AI facial recognition and biometric detection: balancing consumer rights and corporate interests

Dr Felipe Romero-Moreno, *Hertfordshire Law School, University of Hertfordshire, Hatfield, AL10 9EU, UK*
f.romero-moreno@herts.ac.uk

Abstract*— The purpose of this study is two-fold. Firstly, to critically assess the extent to which corporate actors can lawfully use artificial intelligence (AI) technology for real-time facial recognition biometric detection. Secondly, to suggest and appraise some procedural safeguards to make the use of these systems by private actors compatible with consumers' right to protection of their personal data under the General Data Protection Regulation (GDPR). This study seeks to fill an existing gap in the literature. It concludes that unless, the three variables suggested in the study are considered, that is, 'whether', 'when' and 'how' corporate actors can legally use AI for real-time facial recognition biometric detection, the use of this technology will violate consumers' data protection rights.*

Keywords*— Artificial Intelligence, Facial Recognition, Biometric Detection*

I. INTRODUCTION

Facial recognition technology permits the automatic detection of a person by matching at least two faces from electronic images. The first step is to identify and measure multiple facial features, taking out these from the image, and, secondly, contrasting them with characteristics extracted from different faces [1]. Within the private sector, facial recognition systems are currently being deployed for numerous purposes. Among other things, for marketing and advertising such as, profiling consumers to guess their product preferences based on their emotions [2]; using this technology to detect individuals who have been banned from football stadiums [3]; assessing facial expressions of job applicants in interviews [4]; and automatically tagging pictures based on identified faces [5]. However, the rise of artificial intelligence (AI) data-driven facial recognition systems extends beyond the private sector as this technology is also used for public administration, for example, including border management control and law enforcement purposes. Whilst the US currently provides the biggest market for face recognition opportunities, China has shown the highest growth rate and it is committed to becoming a global leader in AI by 2030 [6]. On the other hand, the EU ambitions are huge as the recently published draft of the Artificial Intelligence Act - which is the first piece of legislation in the world regulating AI issues - has as main objective the Union leading the way in the development of trustworthy, ethical and secure AI.

II. RATIONALE FOR THE STUDY

As the General Data Protection Regulation (GDPR), which requires businesses to protect EU consumers' personal data and privacy, the Artificial Intelligence Act is bound to have global repercussions. The latter legislation includes specific provisions on the deployment of AI technology for 'real-time' facial recognition biometric detection in public spaces for the purpose of law enforcement [6]. However, it remains a matter of concern that the use of these systems for purposes other than law enforcement such as, private sector deployment has not been the subject of much debate. A growing body of research has investigated whether, relying on human rights as a benchmark, facial recognition technology could be lawfully implemented [7]. Surprisingly, however, little research has been conducted on the use of AI technology for real-time facial recognition biometric detection by the private sector. Thus, to contribute to the policy discussion concerning the use of this technology beyond law enforcement and fill the gap in the literature, the purpose of this study is two-fold. First, to critically assess the extent to which companies could use AI technology for real-time facial recognition biometric detection. Second, to suggest and appraise some procedural safeguards to make the use of these systems by private actors GDPR compliant.

The remainder of the study is structured as follows. Section 3 discusses AI, machine learning, deep learning and how facial recognition technology works. Section 4 considers facial images as biometric data. Section 5 examines AI automated decision-making and profiling under the GDPR. A summary of the study findings and conclusion are presented in Section 6.

III. UNDERSTADING AI POWERED FACIAL RECOGNITION

A. AI Powered facial recognition and deep learning

There appear to be a lot of definitions of AI, but a commonly used definition is *"the capability of a machine to imitate intelligent human behaviour"*[8]. AI has numerous applications, which increase in depth and breadth of capability. One of the key features of AI is machine learning. This is the examination of statistical models and algorithms that allow computers to predict outcomes and make decisions without being expressly designed to do so. Currently, the most important development of machine learning is the creation of deep neural networks for deep learning, where an AI system can learn from data [9]. For instance, deep learning holds the key to facial recognition identification, facial match, facial tracking and real-time translating conversation. Moreover, artificial neural network algorithms also help facial recognition to become a more accurate technology [10].

B. How does facial recognition technology work?

Technically speaking, a significant difference is whether facial recognition is deployed for authentication, identification or categorisation. Firstly, authentication or verification is commonly known as one-to-one matching. This allows the contrast of two biometric templates, generally supposed to refer to the same person. Two biometric templates are contrasted to

978-1-6654-9988-0/21/$31.00

establish if the individual identified on the two images is the same individual. For instance, this process is used at e-gates by people who travel with an e-passport at border crossing points. Secondly, identification or so-called one-to-many comparison means that the template of an individual's face is contrasted with numerous other templates kept in a database to identify if the face image is kept there. The system returns a percentage for every contrast specifying the likelihood that two images suggest the same individual. This is often referred to automated facial recognition systems. In this context, of relevance here is the Artificial Intelligence Act. It makes a distinction between, on one hand, 'real time' systems where the gathering, contrast and identification of biometric data takes place all immediately or near-immediately (e.g. using 'live' or 'near-'live' video footage created by a camera or the like); and on the other, 'post' systems where the biometric data have already been gathered and the contrast and identification take place just after a significant delay (e.g. video footages or pictures created by CCTV cameras or private devices) [11]. Thirdly, facial recognition systems are also deployed to gather data about a person's traits. This is known as categorization or so-called 'face analysis'. Thus, this technology can also be used for profiling people, which entails classifying them based on their individual traits. Examples of features, which are usually inferred from facial images include sexual orientation, emotions, sex, ethnicity, age and disability [12].

IV. AI Powered Facial Recognition Technology as Biometric Data under the GDPR

Article 4(14) GDPR defines 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''*. Recital 51 GDPR also differentiates between both, 'photographs' and biometric 'facial images'. Thus, an individual's facial image constitutes biometric data, which due to its sensitive nature is a special category of personal data. As a rule, the GDPR prohibits the processing of biometric data such as, a person's facial image unless such individual can rely on one of the ten explicitly set out exceptions included in Article 9(2) GDPR. To lawfully use AI technology for real-time facial recognition biometric detection the only two relevant and possible exceptions to the processing prohibition would be for companies to have: firstly, the individual's explicit consent; and/or secondly, substantial public interest reasons. However, as will be seen, both exceptions are the same to the ones explicitly set out in Article 22(1) GDPR, which regulates automated decision-making and individual profiling. Therefore, these two specific exceptions will be considered in more detail below.

Note here that, pursuant to Article 3 of the GDPR, non-EU established companies (e.g. Clearview AI) would also be subject to the GDPR if they process personal data of individuals within Europe such as, gathering, contrasting and identifying facial images. Thus, effectively Article 3 enables the GDPR to have global reach.

V. AI Automated Facial Recognition Decision Making and Individual Profiling under the GDPR

For the use of AI for real-time facial recognition biometric detection to be legitimate, it would require considering three different variables. Specifically, *whether*, *when* and *how* private actors could lawfully use this technology.

Whether+ When+ How = Lawful corporate facial recognition

A. Whether

The first variable that needs to be examined is *whether* companies could use AI technology for real-time facial recognition biometric detection. As noted above, a key difference is if facial recognition is used for authentication, identification or categorization. Because identification or one-to-many comparison means that corporate actors would have to rely on automated facial recognition, and categorisation or 'face analysis', would involve classifying an individual based on his or her individual traits, it is important to consider here the GDPR provisions regulating both, automated individual decision-making and profiling. As it would be the case with identification, pursuant to Article 22(1) GDPR, automated individual decision-making means to make a decision based solely on automated means without any human involvement. On the other hand, as it would also be the case when analyzing face images or performing 'face analysis', under Article 4(4) GDPR, profiling entails any form of automated personal data processing. It involves the use of data such as, biometric data to assess individual aspects. But profiling can often be part of an automated decision-making process. To be lawful under the GDPR, the use of facial recognition systems requires that appropriate safeguards be in place concerning data processing operations of companies. Firstly, as the Artificial Intelligence Act acknowledges, technical inaccuracies of AI designed to perform biometric detection of natural persons can result in biased outcomes and lead to discrimination in terms of sex, ethnic origin, age, or disabilities. Therefore, this kind of technology should be developed, so that it is subject to intrinsic operational constraints, which cannot be disallowed by the AI itself, it responds to the human operator, and the natural person providing human oversight has the required training, authority and competence to perform that role [13]. Moreover, according to Article 35 GDPR, if identification or categorization of individuals is likely to lead to 'high risk' - as would be the case in the current situation - corporate actors should additionally carry out a Data Protection Impact Assessment before selling or deploying such systems, and publish the identified risks and related mitigation strategies.

B. When

The second variable that needs to be considered is *when* the private sector could rely on AI technology for real-time facial recognition biometric detection. Article 22(4) of the GDPR provides an extra layer of protection for biometric data such as, facial images. As noted above, to legally deploy this technology, data controllers such as, corporate actors could

only perform the processing indicated in Article 22(1) of the GDPR if: firstly, an individual's has explicitly consented to the use of facial recognition; or secondly, the processing of facial images is necessary for reasons of substantial public interest.

In terms of consent, the Court of Justice of the EU case-law stresses that, under Article 4(11) of the GDPR, the consumer's consent must be 'freely given, specific, informed and unambiguous'. For instance, consent would be invalid if the consumer was silent, inactive or pre-ticked boxed were displayed to them. Moreover, consent would also be invalid if the contractual terms misled the consumer such as, making consent compulsory subject to the conclusion of a contract. Therefore, asking consumers to indicate in writing that they do not consent to the gathering and retention of their personal data would negatively impact upon their right to object to it. Furthermore, businesses as data controllers, must also show that consumers actively provide their consent to data processing, and are informed of the consequences of giving consent in plain, clear language, and easily accessible and intelligible form [13]. In this context, applying this guidance to AI technology for real-time facial recognition biometric detection, it would be possible at the point when a smart device wants to perform identification or categorization to give the user the opportunity to provide freely given, specific, informed and unambiguous consent. For example, through 'just in time' pop-up notifications. Moreover, considering smart devices and sensors in big data, further research needs to be undertaken on different kinds of practical and usable consumer affirmative actions, which would constitute valid consent such as, gesture, motions, and behavioral and spatial patterns [14].

In addition to the consent exception, under Article 22(1) of the GDPR, corporate actors can also perform the processing of facial images if it is necessary for substantial public interest reasons. This is in line with Article 9(g) of the GDPR, which states that the processing of biometric data is prohibited, unless this is required on substantial public interest grounds, based on either EU or Member State law. In other words, while the concept of substantial public interest is not expressly defined in the GDPR, this is left for Member States to decide. Thus, for instance, taking the UK as a case study, the UK Data Protection Act 2018, which is the piece of legislation incorporating the GDPR into UK law, in Schedule 1 Part 2 sets out twenty-three substantial public interest conditions. Arguably, following this specific list of conditions, the only relevant exceptions to the processing prohibition, would be for corporate actors to specifically target the use of AI technology for real-time facial recognition biometric identification to three situations. Firstly, the prevention and detection of unlawful acts; secondly, the prevention of fraud; and lastly, when there exists suspicion of terrorist financing or money laundering. In terms of the relevant threshold to be followed, it would seem appropriate here to rely once more on the proposal included in the Artificial Intelligence Act. It suggests that the detection, localisation, one-to-many comparison or prosecution of offenders or alleged offenders of criminal offences are subject to the Council Framework Decision 2002/584/JHA38. In other words, such types of criminal offences must be prosecuted in the Member State affected by a detention order or a custodial sentence for a maximum of at least three years, which is to be defined by Member State law. The Artificial Intelligence Act also notes that this narrowly defined threshold guarantees that the offence is serious enough to allow the deployment of such systems. However, it also explains that the use of real-time facial recognition biometric identification must also be subject to adequate limits in space and time and the reference database of registered individuals (i.e face images) must also be proportionate. Thus, notably, it further underlines the fact that, except in duly justified urgent cases, each use of a real-time facial recognition biometric identification technology must additionally be subject to a prior and explicit authorisation by a Member State court or an independent administrative authority [15].

C. How

Having assessed whether and when under the GDPR private actors could use AI technology for real-time facial recognition biometric detection, the third variable to be examined in this paper is *how* companies could legally implement such systems. Mechanisms to guarantee values-by-design offer explicit and precise links between the basic principles that AI technology must observe and the implementation decisions. The notion that compliance with regulation can be incorporated into the design of the AI technology is fundamental to this approach. Corporate actors are accountable for recognizing the effect of their AI systems from the very outset, along with the benchmark their AI technology must satisfy to prevent negative effects. In this context, it is important to consider the different 'by-design' approaches, which are currently used, for instance, both, privacy-by-design, and security-by-design [16].

- *Implementing 'data protection by design and default'*

Firstly, in terms of 'privacy-by-design', Article 25 of the GDPR, requires that data controllers such as, companies must adopt adequate organizational and technical measures, both at the design stage of biometric data processing and its deployment, to effectively incorporate data protection safeguards and protect individuals' fundamental rights. The GDPR explains that such measures must be determined considering the state of the art, the adoption cost and the scope, context, purposes and nature of the processing, along with the risks for individuals rights and freedoms. Article 25 also recognizes that, by default, just personal data, which is necessary for each specific processing purpose can be processed. It adds that approved certification mechanisms can be employed to prove compliance with these rules [17]. In a nutshell, to be legitimate under the GDPR, the use of real-time facial recognition biometric identification should be subject to the following data protection principles and procedural safeguards.

- *transparency* (corporate actors must give consumers meaningful information that is, consumers must understand why gathering, use and sharing of their biometric data occurs e.g. through 'just in time' notices);

- *lawfulness* (there should be a valid basis for processing i.e. GDPR automated decision-making and profiling);
- *fairness* (corporate actors must provide qualified human intervention to address bias due to automated decision-making and profiling i.e. 'fair algorithms');
- *purpose limitation* (biometric data processing must be specifically targeted to the prevention and detection of unlawful acts, prevention of fraud, and when there is suspicion of terrorist financing or money laundering);
- *data minimisation* (corporate actors must only process data which is adequate, relevant and limited to prevent and detect unlawful acts, and prevent fraud, terrorist financing or money laundering - corporate actors must provide consumers meaningful information about the main parameters to determine which processing is allowed);
- *accuracy* (corporate actors must ensure biometric data is adequate and up to date that is, inaccurate data must be deleted or rectified without delay);
- *storage limitation* (corporate actors must not retain biometric data, which is no longer necessary to prevent and detect unlawful acts, and prevent fraud, terrorist financing or money laundering that is, stored unnecessary data must be deleted);
- *integrity and confidentiality* (corporate actors must prevent data breaches and have in place security measures) [18]

Moreover, as noted above, as well as complying with the above principles, any use of profiling or automated decision-making, which affects subjects of facial recognition biometric identification, should additionally satisfy the following procedural safeguards. First, corporate actors should also carry out regular assessments on the datasets they process to discover any bias and design ways to address any detrimental characteristics such as, overdependence on correlations. Further useful measures should also include the auditing of algorithms and regular reviews of the relevance and accuracy of profiling and automated decision-making. Additionally, corporate actors should also adopt adequate processes to avoid discrimination, mistakes or inaccuracies based on biometric data. Taken together, all these measures should additionally be deployed on a regular basis, not just at the design phase, but also, as the profiling is carried out on individual faces [19].

➢ *Implementing 'security by default'*

Secondly, in terms of 'security-by-design', it is interesting to note that there are numerous ways one can limit the use of real-time facial recognition biometric identification. Thus, perhaps unsurprisingly, evidence shows how the industry is currently working on anti-spoofing measures to avoid this. For example, computer vision dazzle is an open source project, which enables individuals to learn how trends can be used as camouflage to conceal faces. Since facial recognition software searches for certain shapes when it scans images, blocking these shapes means blocking the software's ability to identify people. There are also things one can try such as, creating asymmetry, applying make-up which contrasts with the skin colour in strange directions, using hair to disguise part of the face like the nose bridge and applying face jewels. Additionally, using infrared LEDs wired to caps and masks, or in fact printing face patterns onto anything, which is wearable close to one's face [20].

Therefore, in view of above, to gain trust, the use of AI real-time facial recognition biometric identification systems should also be secure in outcomes, procedures and data and should be developed to be resilient to adversarial data and attacks. In this context, cybersecurity also plays a key role in guaranteeing that the technology is robust against attempts to modify AI performance, behaviour, use or indeed endanger their security properties by adversarial third parties. For instance, cyber-attacks against AI technologies can leverage AI specific assets, such as trained models (e.g. adversarial attacks), or training datasets (e.g. data poisoning), as well as taking advantage of the technology's vulnerabilities. Thus, to ensure a level of cybersecurity, which is adequate to the risks, appropriate mechanisms should lastly be adopted by high-risk AI's providers, considering the AI technology's digital assets and the basic ICT infrastructure [21].

VI. CONCLUSION

The purpose of this study was two-fold. First, to critically examine to what extent the private sector can lawfully use AI technology for real-time facial recognition biometric detection. Second, to suggest and appraise some procedural safeguards to make the use of these systems by corporate actors compatible with the GDPR. This study has sought to fill an existing gap in the literature. It concludes that unless, the three variables suggested in the study are considered, that is, *whether*, *when* and *how* corporate actors can legally use AI for real-time facial recognition biometric detection, the use of this technology will violate consumer GDPR data protection rights.

The main shortcoming of this study is that the corporate use of AI for real-time facial recognition biometric detection is just an in-depth investigation into a small part of a much bigger problem, namely, the impact of the rise of technology on our society. For instance, the draft of the Artificial Intelligence Act warns that, other than data protection issues, the deployment of AI with its intrinsic features such as, complexity, autonomous behavior, opacity and reliance on data, will almost inevitably lead to human rights abuses. Indeed, there seems no end to the plethora of potentially human rights at stake here, including but not limited to the right to human dignity, non-discrimination, equality between men and women, freedom of expression, freedom of assembly, an effective remedy and a fair trial, defense and presumption of innocence [22]. Thus, caution should be taken, as the findings of this study may not be applicable to the whole scenario concerning the corporate use of AI. For example, in addition to the above issues, further research needs to be undertaken on the compatibility of biometric technologies such as, emotion, gesture, body movement, and odour recognition with human rights.

REFERENCES

[1] Eurpean Union Agency for Fundamental Rights, “Facial recogntion technology fundamental righs considerations: in the context of law enforcement,’’ EU FRA.Viena, pp. 1–34, Nov 2019.

[2] Garante per la protezione dei dati personali, ‘‘Installazione di apparati promozionali del tipo “digital signage” (definiti anche Totem) presso una stazione ferroviaria,’’ Italy. December 2017.

[3] European Digital Rights, “Danish DPA approves Automated Facial Recognition,” EDRi. Berlin, June 2019.

[4] C. Hymas, “AI used for first time in job interviews in UK to find best applicants,” The Telegraph. London, September 2019.

[5] T. Simonite, “Facebook can now find your face, even when it’s not tagged,” Wired. San Francisco, December 2017.

[6] European Commission, ‘‘Proposal for a regulation on the European Parliament and of the Council layding down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts,’’ EC. Brussels, pp. 1-118, April 2021.

[7] Eurpean Union Agency for Fundamental Rights, “Facial recogntion technology fundamental righs considerations: in the context of law enforcement,’’ EU FRA.Viena, pp. 1–34, Nov 2019.

[8] Merriam-Webster dictionary, ‘‘Definition of artificial intelligence’’.

[9] Cambridge Consultants, ‘‘Use of AI in online content moderation,’’ Ofcom. London, pp.1-84, July 2019.

[10] Thales Group, ‘‘Face recogntion – fascinating and intriguing.’’ Thales. Paris, April 2021.

[11] European Commission, ‘‘Proposal for a regulation on the European Parliament and of the Council layding down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts,’’ EC. Brussels, pp. 1-118, April 2021.

[12] Eurpean Union Agency for Fundamental Rights, “Facial recogntion technology fundamental righs considerations: in the context of law enforcement,’’ EU FRA.Viena, pp. 1–34, Nov 2019.

[13] Case C-61/19 Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) [2020] EUECJ (11 November 2020)

[14] E. Denham, ‘‘Big data, artificial intelligence, machine learning and data protection,’’ ICO. UK, pp. 1-114, March 2017.

[15] European Commission, ‘‘Proposal for a regulation on the European Parliament and of the Council layding down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts,’’ EC. Brussels, pp. 1-118, April 2021.

[16] European Commission, ‘‘Ethics guidelines for trustworthy AI,’’ EC. Brussels, pp. 1-41, April 2019.

[17] Eurpean Data Protection Supervisor, ‘‘Opinion 5/2018 preliminary Opinion of privacy by design,’’ EDPS. Brussels, pp. 1-34, May 2018.

[18] European Data Protection Board, ‘‘Guidelines 4/2019 on Article 25 Data protection by design and by default,’’ EDPB. Brussels, pp. 1-27, Nov 2019.

[19] Eurpean Data Protection Supervisor, ‘‘Opinion 1/2021 on the proposal for a Digital Service Act,’’ EDPS. Brussels, pp. 1-28, February 2021.

[20] Thales Group, ‘‘Face recogntion – fascinating and intriguing.’’ Thales. Paris, April 2021.

[21] European Commission, ‘‘Ethics guidelines for trustworthy AI,’’ EC. Brussels, pp. 1-41, April 2019.

[22] European Commission, ‘‘Proposal for a regulation on the European Parliament and of the Council layding down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts,’’ EC. Brussels, pp. 1-118, April 2021.