European Journal on Criminal Policy and Research (2023) 29:515–533
https://doi.org/10.1007/s10610-022-09512-y

The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal

Vera Lúcia Raposo[1,2]

Accepted: 9 May 2022 / Published online: 1 June 2022

Abstract
The European legal framework is not devoid of norms that are directly or indirectly applicable to facial recognition technology for identification purposes within law enforcement. However, these various norms, which have different targets and are from multiple sources, create a kind of legal patchwork that could undermine the lawful use of this technology in criminal investigations. This paper advocates the creation of a specific law on the use of facial recognition technology for identification in law enforcement, based on existing regulations, to specifically address the pressing issues arising in this domain. The ultimate aim is to allow its use under certain conditions and to protect the rights of the people involved, but also to provide law enforcement authorities with the necessary tools to combat serious crimes.

Keywords Facial recognition technology · Identification · Law enforcement · Personal data · Artificial intelligence · Algorithm accuracy

Introduction

Police and investigation activities have been shaped, in recent years, by new technologies (Bowling & Iyer, 2019), encouraging innovative and more aggressive ways of policing, that have been labelled as 'new policing' (Fagan et al., 2016). Facial recognition technology (FRT) is one of those digital tools.

The use of FRT for identification purposes within law enforcement has come under attack from all sides, and its legality seems doomed. First, it raises considerable privacy concerns due to the risk of building up an Orwellian society, where a Big Brother State

✉ Vera Lúcia Raposo
vera@fd.uc.pt

[1] University of Coimbra, Coimbra, Portugal

[2] Faculdade de Direito da Universidade de Coimbra, Pátio da Universidade, 3004-528 Coimbra, Portugal

knows everything about its citizens and uses that knowledge to control them. In addition, the protection of personal data (European Data Protection Board and European Data Protection Supervisor, 2021) is also a pressing topic in the European Union (EU) and abroad.[1] Privacy issues arise because FRT deals with a particularly sensitive type of personal data, so-called biometric data, which is subject to a particularly protective legal order, as this paper will highlight. Its effectiveness is also being challenged and some studies have argued that surveillance does not deter crime (Surveillance Studies Center, n.d.). The fact that FRT uses artificial intelligence (AI) is an additional source of concern. There are still many things we do not know about AI (Aroyo & Paritosh, 2021), and the precautionary principle (Raposo, 2021b) has led to what may be an excessively cautious approach to AI in general and to FRT in particular, as demonstrated by the draft regulation proposed by the European Commission (EC) in April 2021 ('the AI Proposal') (European Commission, 2021a). Despite all these legal difficulties, FRT is on the rise, leading to the creation of new paradigms in criminal policy (Fussey et al., 2021).

Objectives and Methods

There are several possible uses of FRT within law enforcement. This paper will solely focus on identification purposes,[2] that is, the use of FRT to identify individuals (both suspects and victims) using photos and/or facial recognition cameras, whether in real-time or not. Identification uses refer to one-to-one authentication, involving a comparison between a template (belonging to the individual claiming to be a particular person) with a previous template from the person whose identity is being claimed; and one-to-many identification, where the template of an individual is compared with templates gathered from a database. The latter involves higher risks, namely due to the existence of a database, but it is the most common use of FRT in law enforcement (MacCarthy, 2021).

This study does not discuss the admissibility of FRT in law enforcement under existing regulations but instead considers a prospective legal framework for EU countries that still lack proper legal standards.[3] The paper recommends a specific legal framework for the use of FRT in this domain, based on existing regulations, which this paper will analyse.

The paper will depart from the existing regulations in force in Europe – not only issued by the EU but also by the Council of Europe – to suggest a draft regulation for the use of FRT in law enforcement. In the analysis of such rules, the paper will rely upon, not only the legal text itself, but also case law, legal opinions and recommendations from competent institutions, and in academic texts.

Because the EU has already established relevant boundaries in this regard, which this paper highlights, national legislatures must keep national laws within these boundaries (moreover, they must consider the relevant norms issued by the Council of Europe). The

[1] In 2013, the Electronic Frontier Foundation (a non-profit digital rights group) filed a lawsuit to compel the FBI to reveal its activities using FRT (Foundation v U.S. Dep't of Justice, 739 F.3d 1 (D.C. Cir. 2014).

[2] Other possible uses include something as simple as to detect a human face in a picture, the so-called face detection (Hasan et al., 2021), or as complex as to detect lies during the interrogation of a suspect, which is known as emotion recognition (Ousmane et al., 2019). None of these uses will be analysed in this paper.

[3] Some EU member states have FRT mechanisms already in place in criminal investigations, but they still lack a specific legal framework. For instance, in France, this is carried out under Article R40-26(3) of the French Code of Criminal Procedure, which is clearly insufficient to address the many issues involved (Sénat, 2021).

paper lists the features to be considered by any FRT regulation in law enforcement within the EU in order to comply with the legal requirements already in place and to guarantee the proper and legitimate use of FRT for law enforcement. We must avoid the so-called 'techno-optimism' (Hayward & Maas, 2021, p. 210) and acknowledge that technology can be used for unlawful means. The aim of this paper is precisely to highlight those illegitimate uses.

A Law to Regulate FRT in Law Enforcement

Valid legal grounds are a common requirement for any restriction on fundamental rights, as in Article 52/1 of the European Charter of Fundamental Rights (ECFR) and Articles 8 to 11 of the ECHR. Specifically in this area, the Law Enforcement Directive (LED) requires a legal base for the processing of personal data within law enforcement.[4] Notably, and unlike in its sister regulation, the General Data Protection Regulation (GDPR),[5] consent cannot be legal grounds for data processing under the LED, which leaves only the option of legal authorisation. The legal basis for data processing must be accessible to the public, clear and precise to provide 'sufficient guarantees against the risk of abuse and arbitrariness' (Recital 33 and Article 8 LED) and to allow people to foresee how will it be applicable (EDRI, 2020). In addition, a specific regulation is required to ensure clarity in the solutions provided, as 'the use of AI in the area of police and law enforcement requires area-specific, precise, foreseeable and proportionate rules' (EDPB-EDPS, 2021, p. 11). Some regulations are already in place, others are still in draft form and are expected to be in force soon. They condition - or will condition - the use of FRT by regulating either data processing (the LED) or artificial intelligence (the AI Proposal). Nonetheless, a clearer legal framework on the use of FRT for law enforcement purposes would be desirable in order to avoid grey zones and potential liabilities.

The law that this paper advocates could be directly issued by the EU or by national member states in compliance with existing EU norms, the latter of which is a better option. Although the EU has the competence to regulate many issues related to this question (and has indeed exercised these regulatory powers), the fight against terrorism and the protection of national security remain competencies of national member states (European Parliamentary Research Service, 2021), and in spite of the Title V of the TFUE ('Area of Freedom, Security and Justice'), most law enforcement activities and criminal justice in general are regulated by national states (Csonka & Landwehr, 2019).

Legal Definition of the Scenarios in Which FRT can be Used

A future legal regulation must impose clear rules regarding to whom, when and under which conditions FRT can be applied. The AI Proposal provides a general limitation in this regard, by banning 'the use of 'real-time' remote biometric identification systems in

[4] At the Council of Europe level, Article 6(1) of the Convention 108 + imposes the same requirement on the processing of special categories of data, including biometric data.

[5] The GDPR provides the general framework for personal data processing in Europe, with the exception of some very specific domains, such as law enforcement, that are regulated by the LED under very similar principles. On consent under the GDPR see Raposo 2022a.

publicly accessible spaces for the purpose of law enforcement' (Article 5/1/d of the AI Proposal), unless under the conditions set forth in this regulation.

However, the AI Proposal is silent regarding other modalities of facial recognition technology for law enforcement purposes, such as when this technology does not take place in real-time or it is not performed in public spaces, or when it is used for other purposes besides identification (Raposo, 2022a). All these possibilities must, therefore, be considered admissible.[6] In the Draft Act they are considered high-risk AI systems (Article 6 of the AI Proposal), or in some cases low risks AI systems (Article 52/2 of the AI Proposal), and thus allowed, provided that certain requirements are met. However, these requirements are imposed mostly on AI developers, manufacturers and importers, whereas the obligations of AI users are limited to issues of product safety (Article 29 of the AI Proposal). Apart from cases described in Article 5/1/d, the Proposal is silent regarding the specific scenarios in which FRT can be used by law enforcement authorities and under which requirements.[7]

Clarity of indications is, however, crucial, as the lack of proper legal guidance has been a hurdle for FRT. Paradigmatically, in a recent decision on FRT in law enforcement, the Court of Appeal of England and Wales found that although the use of FRT in the case was proportionate, the absence of clear guidelines on where and when to apply it was not. In the Court's words, 'AFR Locate fails to satisfy the requirements of Article 8(2), and in particular the 'in accordance with the law" requirement, because it involves two impermissibly wide areas of discretion:[8] the selection of those on watchlists, especially the "persons where intelligence is required" category, and the locations where AFR may be deployed'.[9]

Lawful Uses of FRT for Law Enforcement

In law enforcement, FRT can be used for preventive aims, such as to prevent a previously identified perpetrator from committing another crime ('pre-emptively to identify and manage', Mann & Smith, 2017, p. 124), or for repressive aims, such as to identify a person who is wanted for a crime.

FRT can also be used to scan every person in certain situations (such as crossing a street under FRT surveillance) or to target specific individuals. This reasoning can also be found in the LED, which in Article 6 encourages a 'distinction between personal data of different categories of data subjects'. Moreover, Article 6(a) autonomizes 'persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence', concluding that what is acceptable for data subjects under such conditions is not (or might not be) acceptable for any other person (EDRI, 2020). 'What is publicly acceptable for law enforcement to use when detaining known criminals or investigating crimes may not be tolerable for those situations where police are conducting broad

[6] Moreover, it does not ban FRT for use by other public entities not related to law enforcement and for use by private individuals and companies (Reinhold & Mülle, 2021; Raposo, 2021a).

[7] Note, however, that this cannot be taken as a legal void, as this matter is outside the scope of the Proposal. In detail about this Proposal, see Raposo 2022b.

[8] Technology may limit the way police discretion is exercised, but it does not annul it. Cf. Fussey et al. 2021.

[9] The Queen (on the application of Edward Bridges) (Appellant) v The Chief Constable of South Wales Police (Respondent) & others [2020] EWCA Civ 1058 On appeal from: [2019] EWHC 2341 (Admin), par. 152.

surveillance, or routinely patrolling neighbourhoods' (IJIS Institute and International Association of Chiefs of Police, 2019, p. 7).

Unlawful Uses of FRT Within Law Enforcement

The framework law must establish that the use of FRT is restricted to criminal investigations and ban its use for any external purposes. Especially objectionable purposes should be expressly banned – for example, using FRT for the sole purpose of determining features that historically are connoted with discrimination, such as gender, ethnic origin, skin colour and sexual orientation (Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention 108, 2021; Najibi, 2020).

Sometimes, hidden purposes for mass surveillance (Douglas & Welsh, 2022) underlie the allegations of a criminal investigation. Mass surveillance actions 'rely on watching [the public] indiscriminately, without reasonable suspicion, sufficient possibilities for them to have knowledge of what is happening, ability to consent, nor the genuine and free choice to opt in or out' (EDRI, 2020, p. 10).

Mass surveillance has been used as a tool of control and repression (such as in the case of China's notorious Social Credit System) (Wong & Dobson, 2019), to target certain groups of people (for example, to control the Uighur people in China) (Asher-Schapiro, 2021) and to pursue political aims, such as suppressing political opponents (as occurred during the Hong Kong protests, when authorities used FRT to identify protesters and suppress freedom of expression and assembly) (Doffman, 2019). Such uses of FRT are not restricted to authoritarian states, as they can also be found in liberal democracies (in the US, FRT is sometimes used in black neighbourhoods) (Najibi, 2020), allegedly to maintain law and order.

With mass indiscriminate surveillance, everyone is watched constantly, and there is no anonymity in public spaces (Article 19, 2016; Commission Nationale de l'Informatique et des Libertés, 2019). Every person can become a suspect (EDRI, 2020), and even casual behaviours (such as wearing big sunglasses, hiding one's face or looking at the ground) might be considered suspicious (Commission Nationale de l'Informatique et des Libertés, 2019). For these reasons, privacy intrusions deemed to be (or to have the potential to develop into) mass surveillance have been repeatedly rejected within the EU.[10]

EDRI (a European network aimed to the defence of rights and liberties online) summarised the many dangers of mass surveillance in this way (EDRI, 2020, pp. 21–22):

[10] In the case Digital Rights Ireland and Seitlinger and Others, the European Court of Justice (ECJ) ruled that Directive 2006/24/EC (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/E) was invalid because it allowed the retention of data for all types of electronic communications and thus it might create in people's mind the 'feeling that their private lives are the subject of constant surveillance' (C-293/12, Digital Rights Ireland and Seitlinger and Others, GC, 8 April 2014, ECLI:EU:C:2014:238, par. 37).

In Schrems I, a case arising from a complaint about the transference of personal data from Facebook Ireland Ltd. to Facebook US, the parent company, and subsequent access of the data by US state security agencies, the ECJ ruled again against the perils of State surveillance. The ECJ considered that 'the law and practices in force in the third country [the US, where such type of State surveillance is allowed] do not ensure an adequate level of protection' (Case C-362/14, Schrems v Data Protection Commissioner, GC, 6 October 2015, ECLI:EU:C:2015:650, par. 107).

> A measure allowing for constant, real-time surveillance, especially involving the processing of sensitive, special-category data such as facial biometric data, in a blanket or indiscriminate manner, would per se violate the essence of fundamental rights such as privacy, dignity, freedom of expression and freedom of association and would thus be incompatible with EU law (…) Mass surveillance by its very nature is a fundamental breach of fundamental rights: it impinges on the very essence of privacy, data protection and other rights.

Legitimate Purpose and Necessity

Definition of the scenarios in which FRT can be used (e.g., which persons, under what conditions, to pursue which crimes) must be done in light of two main criteria: the legitimate purpose principle and the necessity principle (European Data Protection Board, 2022).

The legitimate purpose principle is recognised in Article 4/1/b LED, Article 8/2 ECFR, Article 6 of the Convention 108 + and Article 5/1/b of the GDPR. Under this principle, FRT, as with any technology restrictive of fundamental rights, particularly privacy rights, must be used for a purpose considered lawful and relevant by the legal order.

The principle of proportionality *lato sensu*, with its sub-dimensions of proportionality *stricto sensu*, necessity and effectiveness (European Data Protection Supervisor, 2019), is the guiding principle for determining limitations on fundamental rights (Alexy, 2014). In the domain of protection of personal data for law enforcement purposes, Article 10(1) of the LED established that the use of FRT must be 'strictly necessary'. According to the Article 29 Working Party[11] (A29WP), the expression is 'foresee precise and particularly solid justifications for the processing of such data' (Article 29 Data Protection Working Party, 2017, p. 8). The A29WP underlined the distinction between the requirements of necessity, as imposed in Article 8(1) of the LED for the processing of any data (Article 29 Data Protection Working Party, Opinion on some key issues, pp. 7–8) ('processing is necessary'), and the requisite of strict necessity, as set forth in Article 10 of the LED ('where strictly necessary')[12] for the processing of sensitive data, such as biometric data. Under the latter, it should be demonstrated that the purpose of processing such sensitive data – in our case, the investigation of crimes and the application of criminal law – cannot be met by less intrusive measures from a fundamental rights perspective.

Even disregarding law enforcement, the collection and processing of biometric data has been considered excessive in some scenarios. For instance, in a 2008 ruling, S. and Marper v UK, the European Court of Human Rights (ECtHR) declared that 'the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded

[11] Before the creation of the European Data Protection Board (EDPB), the A29WP was the data protection supervisory entity at the European level.

[12] On the interpretation of this expression, see C-293/12, Digital Rights Ireland and Seitlinger and Others, GC, 8 April 2014, ECLI:EU:C:2014:238, par. 92.

as necessary in a democratic society'.[13] Moreover, in 2018, the European Data Protection Supervisor released an opinion in which it advised against the use of processing facial images and (two) fingerprints in ID cards and residence documents (European Data Protection Supervisor, 2018).

The assessment of necessity is uncontroversial. Its interpretation, however, has varied, even if only restricted to the processing of personal data in law enforcement.[14] Necessity should be understood in terms of whether the aim is sufficiently important to deploy FRT and whether a less intrusive measure would be equally suitable in order to achieve the aim. However, the 'necessity' criterion cannot be taken in such a way as to exclude FRT when the aim is likely to be achieved using any other mechanism because, in a sense, there is always a different way to achieve the aim (even if it is less efficient, less accurate or slower) (Renaissance Numerique, 2020). Proportionality is also a dimension of necessity: FRT should only be chosen if the aim cannot reasonably be achieved by other means deemed less intrusive to the fundamental rights and freedoms of the subject. Ultimately, there must be a fair balance between individual rights and the target aim. Necessity also encompasses an assessment of effectiveness. The British Information Commissioner's Office (ICO) sheds some light on this matter.[15] According to ICO, the effectiveness of FRT is dependent not on the number of people arrested using this technology but on the benefit to society. If those who are arrested have not actually committed serious offences (so if, for example, they have been caught pickpocketing on the subway or shoplifting) there is no real benefit; however, the assessment is different for more severe crimes such as terrorism, child abduction or child pornography (Information Commissioner's Office, 2019).

The Special Case of Real-Time Remote Biometric Identification Systems in Publicly Accessible Spaces

As stated, the AI Proposal includes an explicit prohibition on 'the use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement' (Article 5(1)(d) of the Proposal). However, the EC has also recognised the utility of this type of FRT in some cases, and, therefore, in that same law, the EC has allowed its use when 'strictly necessary' (the principle of necessity) for the following purposes: searching for crime victims, including missing children; 'specific, substantial and imminent threat to the life or physical safety of natural persons, or of a terrorist attack'; and detection, localisation, identification or prosecution of a perpetrator or suspect for certain crimes. Regarding the latter exception, crimes must be listed in Article 2(2) of Council Framework Decision 2002/584/JHA (European Council, 2002) and be punishable by the domestic law in question with a custodial sentence or a detention order for a maximum period of at least three years.

[13] S. and Marper v the United Kingdom, 4 December 2008, applications nos. 30,562/04 and 30,566/04, ECtHR [GC], par 125.

[14] Kindt, for instance, presents a three-step test to assess proportionality: legal base (rule of law), legitimate aim and necessity in a democratic society. For necessity, the guiding criterion is the existence of a 'pressing social need' (Kindt, 2013).

[15] Even though the UK is not an EU member state, its norms on data processing are still basically equivalent to EU norms, and for this reason, its opinions are relevant to understanding and applying European legal standards.

The use of FRT in the above-mentioned scenarios is supposed to be an exception allowed under strict requirements (Article 5(2) and (3) of the Proposal) (Christakis, 2021). Such requirements include (i) a previous assessment of the likelihood and severity of harm to citizens and the possible consequences of using FRT on citizens' rights and freedoms; (ii) strict respect for the principles of necessity and proportionality; and (iii) prior authorisation 'granted by a judicial authority or by an independent administrative authority of the Member State' (most likely, the national data protection authority).

However, the exceptional nature of this endorsement is largely theoretical, as the Proposal has some loopholes and, in the end, the restrictive admission of real-time biometric identification in public spaces is not that restrictive. Some of the crimes listed in Article 2/2 of Council Framework Decision 2002/584/JHA are not particularly serious in the sense that they do not affect people's lives or physical integrity (e.g., corruption or fraud) (Raposo, 2021a, 2022b).

Suggested Solution

All this considered, this paper concludes that the use of FRT should be limited not only in terms of the types of crimes but also the types of individuals who are scanned. Regarding crime, FRT should only be used for particularly grievous crimes, namely those presenting severe threats to national security (e.g., national or external terrorism), public health (e.g., the propagation of infectious diseases, for which FRT can be used to identify people not complying with an isolation order following a positive COVID-19 diagnostic, as long as such conduct is criminal under domestic legislation) or unprotected groups (e.g., children, racial/ethnic minorities). The EU has already lists of 'serious crimes' (Paoli et al., 2017) that could be used to define the objective scope of FRT in criminal investigation. In addition to what has already been mentioned in Article 2(2) of the Framework Decision 2002/584/JHA, see, for instance, Article 83(1) of the Treaty on the Functioning of the European Union and Annex I of Regulation (EU) 2018/1727.[16] Regarding the subjective scope, this paper argues that FRT must only involve persons of interest – that is, individuals particularly suspected by police authorities (EDRI, 2020) – unless the circumstances of the criminal investigation impose a wider target, which must be properly justified in each situation by the competent authorities.

Legal Definition of the Source of the Images Used

Any future regulation must define the conditions under which images submitted to FRT can be captured, as in how and why, and whether consent is required (IJIS Institute and International Association of Chiefs of Police, 2019). The latter issue has already been answered in the LED, as consent is not required to collect data, even sensitive data (Article 29 Data Protection Working Party, 2017); however, the other criteria require further clarification.

[16] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Images that are not provided by the data subject can have various sources, whether directly related to law enforcement (such as a previous photograph from a suspect or convicted individual in a police database) or not (e.g., pictures from the national identification database). The use of images found on the internet, especially on social media, is an obvious concern.

The Australian based company Clearview AI made headlines due to their 'legally unclear' business: to collect photos from the internet, namely from social media, and use them to create a huge database that the company sells to interested parties, including police forces worldwide (Sobel, 2021). European law enforcement agencies were also seduced by this easy means of having access to biometric templates (EDRI, 2021a), forcing the European Data Protection Board (EDPB) to make a stand up and issue an alert against the potentially unlawful data processing in place. The most recent public statement in this regard in Europe came from the French data protection authority – the Commission Nationale de l'Informatique et des Libertés - which ordered Clearview AI to stop collecting photos and to delete those in its possession (Commission Nationale de l'Informatique et des Libertés, 2021), in line with other statements from data protection authorities worldwide (Gunning et al., 2021). A future FRT regulation could clarify whether templates can be created from photos taken from social media, eventually following the position of the A29WP, which back in 2017 analysed this issue: 'registering for a social network might include the acceptance of certain data protection rules which provide that all the partners of the provider (including national police authorities) have access to personal data' and '[i]n case of doubt, a narrow interpretation should be applied, as the assumption is that the data subject has voluntarily given up the special protection for sensitive data by making them available to the public including authorities' (Article 29 Data Protection Working Party, 2017, p. 10).[17]

The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention 108 ('Consultative Committee') has suggested that the use of images taken from the internet and, in general, the use of any database created for a different purpose can only take place 'when it is for overriding legitimate purposes and it is provided by law and strictly necessary and proportionate for these purposes (for instance law enforcement or medical purposes)' (Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention 108, 2021, p. 6). In any case, the use of images not collected for law enforcement purposes must be specifically authorised in the regulation on FRT under requisites to be legally established, such as situations of urgency or other pressing reasons properly justified by law enforcement authorities.

Exchange of information between national databases is not a novelty in Europe. The 'Prüm' framework is the umbrella mechanism under which it can take place.[18] Recent European proposals intend to update this mechanism. Both the Proposal for a Directive on information exchange between law enforcement authorities (European Parliament and Council, 2021a) and the Proposal for a Regulation on automated data exchange for police cooperation (European Parliament and Council, 2021b) aim to include face data on the set

[17] This same approach was adopted by the EDPB on its guidelines regarding the use of data gathered from social media under the GDPR (European Data Protection Board, 2020b). In 2022, the European Data Protection Board release some guidelines on the use of FRT in law enforcement (European Data Protection Board, 2022), but the collection of photos from social media was very superficially analysed.

[18] The so called 'Prüm framework' refers to a mechanism of automated data exchange between Member State, involving DNA, dactyloscopic and vehicle registration data saved on the Member States' national databases (Caruana, 2019).

of data to be exchanged. The European Commission (2021b) has guaranteed that '[t]here is also no envisaged use of artificial intelligence for the comparison of facial images under the proposed Regulation'. Still, concerns have been expressed on how reliable this guarantee is, because 'facial image databases can pave the way for biometric mass surveillance practices' (EDRI, 2021b).[19]

The law regulating FRT in law enforcement should clarify this issue, by allowing the exchange of face data between member states and the use of FRT on those data regarding the specific crimes for which FRT is allowed (see the previous sections). The creation of a European database of biometric templates would be a more complex procedure, but provided that adequate precautions are in place it could be a useful measure for fighting crime, especially cross border criminality. The precautions to consider include measures to protect sensitive personal data (regarding access to that data, storage its period, and subsequent data uses), its use being restricted to specific types of crimes and their recording on the database being restricted to individuals convicted of those specific crimes.

Legal Definition of the Image Retention Period

The law must clearly state how long the image will be stored (IJIS Institute and International Association of Chiefs of Police, 2019).[20] According to the recommendation of the A29WP, when deciding the maximum storage period, the principles of necessity and proportionality should be considered, following their interpretation by the ECHR[21] and the EU institutions (Article 29 Data Protection Working Party, 2017).

The definition of the storage period must consider the types of individuals concerned and the results obtained, as different types of data subjects might lead to different solutions. Following Article 5 of the LED, which establishes the need to impose time limits, Article 6 differentiates between data subjects, including victims, suspects, persons convicted of a criminal offence, witnesses, experts and other persons involved. A possible interpretation is that different timeframes should be established for these different types of data. The Consultative Committee puts forth the matching outcome as a criterion to establish different timeframes for storing templates resulting from public surveillance (the so-called uncontrolled environment). According to this criterion, if there is no match, the biometric templates of people passing by should be automatically destroyed upon a negative result; in contrast, if there is a match, the biometric template can be stored for the period strictly necessary to conduct the relevant police investigation (Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention 108, 2021).[22] In any case, note that biometric and personal information must be strictly separated.

[19] Some leaked documents seem to confirm this suspicion (Campbell & Jones, 2020), but the documents were 'disclosed' in 2020, whereas the note where the Commission guarantees that FRT will not be used is from December 2021, so it might be the case that there was a change of heart.

[20] A different issue is how biometric templates should be stored. Despite the potential privacy-related consequences, this matter is more technical than legal and thus is not further explored in this paper.

[21] See, for instance, the ruling of the ECtHR in Gaughran v The United Kingdom 2020, 13 February 2020, application no. 45,245/15, ECtHR, par. 70, where the court concluded that the 'the retention of the applicant's DNA profile, fingerprints and photograph amounted to an interference with his private life'.

[22] If there is no matching the biometric template of the person being screened must be immediately deleted.

When the time limit is reached (regardless of how long it is and how it is calculated), the data should be automatically deleted or at least anonymised. Thus, a model is necessary in which there are periodic reviews in place, after which the data must be deleted (Article 29 Data Protection Working Party, 2017). In its opinion on data processing for law enforcement, the British ICO stated that images should be deleted from the system 'as soon as practicable' (Information Commissioner's Office, 2019, p. 15), but because the opinion does not clarify 'practicable' in this context, it remains an open question.

Protection of the Rights of the People Subject to FRT

The act regulating the use of FRT in law enforcement must provide proper protection against the threats posed by FRT to people's rights following existing regulations, especially as regards privacy (European Data Protection Board, 2022).

Among the many rights at stake, the right to be informed about the use of FRT is foundational, as it allows the subsequent exercise of all other rights.[23] Under Article 13 of the LED (see also Article 5/1 of the GDPR and Recital 26 of LED), authorities have the duty to inform citizens that they are subject to FRT and of the consequent risks (European Data Protection Board, 2020a). Under the LED, the consent of the data subject is not proper legal grounds for the processing of sensitive data (such as biometric data), but certain information must be provided, even if it is not done so for informed consent.[24] This information includes the identity and contact details of the controller, the purpose of the data processing, the retention time and the rights to which the person is entitled. The right to be informed is a prerequisite for the exercise of other rights, such as the right to request access to stored data (Articles 8/3 EUCFR and 14 LED), the right to demand its erasure or rectification (Articles 8/3 EUCFR and 16 LED) and the right to lodge a complaint with a supervisory authority and receive an effective remedy (Article 47 EUCFR). The latter must be exercised in front of a tribunal, as defending rights before administrative authorities, such as data supervisory authorities (Art. 52 LED; GDPR, Art. 77), are not sufficient (European Union Agency for Fundamental Rights, 2019).

In light of the right to be informed, the individuals being tracked by FRT should be alerted to the use of FRT and the specific places where cameras are located. If this is not possible – due to, for example, the secrecy required in some criminal investigations – the individuals should be informed *ex post facto* (Vogiatzoglou et al., 2021). Regarding compliance with the duty to inform, the law should distinguish between *ex ante* and *ex post* information, with more stringent requirements for the latter. Likewise, the law should differentiate between information to be provided to the public and information directed to individuals targeted by FRT, with a wider scope for the latter,[25] which should cover not

[23] Under the case law of the ECJ, see joined Cases C-141/12 and C-372/12, YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S, 17 July 2014, EU:C:2014:2081, par. 57 and Case C434/16, Peter Nowak v Data Protection Commissioner, 20 December 2017, ECLI:EU:C:2017:994, par. 57.

[24] EDRI (2020) suggests that all individuals whose biometric data are captured should be notified of the occurrence, even if (and especially so if) legal proceedings against them are not initiated.

[25] A distinction of this kind, although not entirely coincident with the one in the text, can be found in Vogiatzoglou et al., 2021.

only the fact that personal data is being processed but also the purposes of the processing, the specific data involved and the people who have access to it (Vogiatzoglou et al., 2021).

To safeguard ongoing investigations, mechanisms should be put in place to restrict the right to be informed in certain scenarios, as law enforcement authorities sometimes need to develop their work in secrecy to preserve criminal evidence.[26] This possibility has already been recognised by Article 13/3 of the LED to achieve the purposes stated therein, including the preservation of criminal investigations. Likewise, Article 15 of the LED allows for the invocation of relevant interests – some of which regard investigation procedures, collective/public interests or third-party interests – to fully or partially restrict this right. The norm is formulated in such broad terms that it may be able to cover a wide set of scenarios (Vogiatzoglou et al., 2021). However, there is a mechanism of control for such discretionary powers, as data controllers must provide in writing their reasons for preventing the right to access. However, in such a case, the data supervisory authority might still exercise the right to access as a kind of proxy for the data subject. A similar model of access and restriction to access could be included in a future law regulation FRT in law enforcement.

In addition to the general set of rights that apply to everyone, there are those particular to vulnerable groups.[27] Regarding FRT, this protection is justified by the fact that they might present themselves in ways that might distort their facial features (LGBT); that they have particular facial features (ethnic minorities); or that their features change substantially over time (children) (Government of Scotland, 2018), which affects the accuracy of FRT (Dushi, 2020; European Union Agency for Fundamental Rights, 2018). One might think that children are not an issue in this discussion, as children do not commit crimes, especially the sorts of serious crimes that FRT should target. However, FRT is not only directed at perpetrators but also at victims, and children are frequent victims of the kind of serious crimes that are investigated using FRT, such as international abduction or human trafficking. Therefore, the processing of their biometric data cannot be totally banned.

Compliance and the Rule of Law

The law regulating FRT in law enforcement must implement proper measures to guarantee compliance with its requisites and thus with the rule of law. Transparency and public scrutiny are the cornerstones of compliance. These require strict control of the algorithms used and a record of how they are programmed, which data was used to train them and what training methodologies are in place. For this to occur, frequent audits must be carried out.

From a privacy perspective, a Data Protection Impact Assessment (DPIA) (Recitals 53 and 58 and Article 27 of the LED) and a consultation with the supervisory authority (Recital 96 and Article 28 of the LED) are required. Moreover, according to Article 15/e of the Convention 108+ '[t]he competent supervisory authorities shall be consulted on proposals for any legislative or administrative measures which provide for the processing of personal data'.[28]

[26] Dowsett v The United Kingdom, 24 September 2003, application no. 39,482/98, ECtHR, par. 42.

[27] The European Network Against Racism (2019) highlights that over-policed communities are more prone to be subject to FRT.

[28] Modernised convention for the protection of individuals with regard to the processing of personal data, 2018, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

A mechanism of checks and balances on the use of FRT should be put in place. Such a mechanism might, for instance, require approval before putting in place especially tricky facial recognition processes (such as general surveillance in public spaces), and subsequently constant monitoring. The Proposal for the EC on the uses of AI has some interesting suggestions in this regard (European Commission, 2021a). Article 5(3) of the Proposal states that FRT in public spaces for law enforcement purposes can only be done with prior authorisation from a judicial authority or an independent administrative authority, which are only supposed to authorise such actions based on the proportionality and necessity of FRT use in light of the targeted aims (although the Proposal very reasonably allows this requisite to be waived in situations of urgency).

The law must clearly state law enforcement authorities' accountability in the use of FRT. 'For citizens to accept and consent to certain forms of surveillance, that is to say its positive face, the state should be accountable for its actions' (Taylor, 2002, p. 66). According to the ECFR (articles 41–44, 47–50), citizens have the right to demand respect for due process and the rule of law, including the respect for proportionality *lato sensu*, transparency and the granting of proper compensation in case of harm. Nevertheless, a specific provision for the use of FRT in law enforcement would have to make it clear that in cases of misuse (which must be properly defined in the law – see "Objectives and Methods" section of this paper), the perpetrators would be legally responsible.

Mechanisms to Guarantee Accuracy of FRT

Facial recognition technology algorithms never provide definitive results (yes or no), only probabilities (European Union Agency for Fundamental Rights and Council of Europe, 2018). That is, the software can never determine that two templates belong to the same person (i.e., exact matches), but only how likely they are to belong to the same person (Commission Nationale de l'Informatique et des Libertés, 2019; IJIS Institute and International Association of Chiefs of Police, 2019). From a comparison of the templates, the software will indicate the level of probability that the two templates coincide. Exceeding a threshold previously established by the system will confirm a match (Commission Nationale de l'Informatique et des Libertés, 2019). These probabilities are based on how accurate the software is.

Accuracy closely depends on the technique used, which must be state of the art (European Union Agency for Fundamental Rights, 2019). The accuracy of the algorithm is measured according to the number of false positives and false negatives. The algorithm is considered inaccurate above a given threshold.

The accuracy of FRT depends on several factors, some of which are more easily controllable than others. Even though this is more a technical issue than a legal one, a law on the use of FRT in law enforcement must establish some standard of accuracy, as a mistake derived from a lack of accuracy risks legal consequences for everyone involved (police forces and individuals). FRT failures might lead to false positives (e.g., erroneous matches in which someone is wrongly identified as a wanted person, such as inaccurate placement on a watchlist) and false negatives (e.g., a person goes undetected even though he/she is on a watchlist) (European Union Agency for Fundamental Rights, 2019). The level of certainty in the matching of images is crucial in law enforcement. An error in facial recognition regarding a person allowed to use a smartphone that works by means of facial biometric identification is troubling, but an error in the identification of a criminal is much more

concerning and can lead to outcomes such as detention (which, in the case of erroneous identification, would be unlawful) and public disclosure of the person's identity, leading to social discredit and reputation damage.

Specific concerns involve eventual biased results, derived from the use of incomplete and/or erroneous data, that systematically harm people from ethnic minorities (Haddad, 2021). The so-called 'black data' problem (Ferguson, 2017, p. 131) refers to data on minorities who tend to have more contact with the police than the general population (Crutchfield et al., 2012; McGlynn-Wright et al., 2022) and thus are overrepresented in police databases (Murphy & Tong, 2020).[29] This phenomenon ends up creating more stigmas against this already fragile section of the population, aggravating their situation regarding police forces and feeding discrimination.

The data used to train the algorithms must be accurate and up to date, as stated in Article 5(1)(d) of the LED, Article 5(1)(d) of the GDPR and Article 5/3/d of the Convention 108+ (principle of accuracy).[30] In FRT, the data is the images used to train the algorithm, and it must be of high variety and quality. FRT is 'trained' to recognise faces based on a set of facial images. If a certain group is under-represented in such images, people from that group may be wrongly identified. The law must provide that the images used for training be diverse and of a reasonable number, and that they be updated periodically, because '[s]hould its reliability deteriorate, it will be necessary to renew the training photos and therefore ask more recent photos to be provided' (Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention 10, 2021, p. 9). Only good-quality images should be used. Different scenarios involve images of differing quality, which, in turn, conditions accuracy. In a controlled environment in which a person is set up in a particular place and under the proper light to be 'identified', such as a police station or airport, *ex post facto* identification is typically used. In contrast, in a non-controlled environment (public or semi-public spaces), random images from CCTV cameras are often used, especially images of people passing on a street, and surveillance occurs in real-time (Harwell, 2019). The law must establish different legal effects for these two types of matching, such as by demanding additional methods of identification for the latter – namely, other forms of biometric identification (fingerprints, DNA) – before any police measures are taken (Renaissance Numerique, 2020).

Prohibition of Automated Decision Making

The law regulating FRT in law enforcement should ban decisions that are made automatically based on facial recognition results. Article 11 of the LED generally forbids automated decision making, meaning any 'decision based solely on automated processing, including profiling, which produces legal effects concerning [an individual] or similarly significantly affects him or her'. A positive result cannot lead to an automatic arrest, based solely on this technology (Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 2021). Any potential match must

[29] The study refers to over-representation in genetic databases, but the same will be valid for face databases.

[30] In its opinion on data processing for law enforcement, the British ICO listed some requisites for the lawfulness of FRT, among them that the images used must be clear and verifiable (Information Commissioner's Office, 2019).

be subsequently confirmed by a human operator to prevent false positives (see the section on FRT accuracy) (IJIS Institute and International Association of Chiefs of Police, 2019). Human intervention must be an autonomous assessment and not a blind confirmation of results provided by the software (which is likely to happen when the match confirms the biases of the human operator) (European Union Agency for Fundamental Rights, 2019).

Exceptions to the prohibition of automated decision making should only take place under circumstances listed by the law, which must also provide appropriate safeguards for the rights and freedoms of the data subject.[31] Such exceptions must apply 'only where strictly necessary' (as stated in Article 11 LED) and be based on solid arguments, whose existence must be demonstrated.

Discussion and Conclusions

Mainstream scholars object to the use of FRT in law enforcement. European institutions are also not favourable to its use.[32] Paradigmatically, Wojciech Wiewiórowski, the European Data Protection Supervisor, claimed some time ago that 'It seems that facial recognition is being promoted as a solution for a problem that does not exist' (Wiewiórowski, 2019). This statement, however, seems to be based on the utopian belief that crime is under control. Criminals are always advancing their methods, and they are often one step ahead of law enforcement authorities, who are bound by existing law. The use of FRT might be an important tool for identifying criminals and thus reducing crime (Dushi, 2020), which is by all standards solid grounds for the restriction of rights and liberties, as it fills the 'necessary in a democratic society' test (Articles 8 to 11 of the ECHR on the restriction of human rights) (Council of Europe/European Court of Human Rights, 2020). However, limits must be set to avoid a shift in the surveillance paradigm from the targeted surveillance of specific individuals to, potentially, mass surveillance of everyone. The goal is to build up a legal framework where the risk of an Orwellian Big Brother is definitively excluded.

Regulation is therefore crucial. Depending on the situation, the absence of a clear legal framework could either restrict the use of this technology or lead to abuses. Neither of these outcomes is desirable.

Funding This work was supported by a research grant from the Instituto Jurídico, Faculty of Law of Coimbra University.

Declarations

The author has no financial, personal, academic, or other conflicts of interest in the subject matter discussed in this manuscript.

References

Alexy, R. (2014). Constitutional rights and proportionality. *Revus - Journal for Constitutional Theory and Philosophy of Law, 22,* 51–65

[31] C-293/12, Digital Rights Ireland and Seitlinger and Others, GC, 8 April 2014, ECLI:EU:C:2014:238, pars. 54 and 55.

[32] In October 2021 the European Parliament voted in favour of a permanent ban on the automated recognition of individuals in public spaces (European Parliament, 2021).

Aroyo, L., & Paritosh, P. (2021). Uncovering unknown unknowns in machine learning. *Google AI Blog*, February 11, 2021. https://ai.googleblog.com/2021/02/uncovering-unknown-unknowns-in-machine.html. Accessed 13 May 2021

Article 19 (2016). *The right to protest principles: Background paper*. https://www.article19.org/resources/the-right-to-protest-principles-on-the-protection-of-human-rights-in-protests/. Accessed 26 Mar 2021

Article 29 Data Protection Working Party (2017). *Opinion on some key issues of the law enforcement directive (EU 2016/680), 17/EN WP 258, adopted on 29 November 2017*. https://ec.europa.eu/newsroom/article29/items/610178. Accessed 13 June 2021

Asher-Schapiro, A. (2021). China found using surveillance firms to help write ethnic-tracking specs. *Reuters*, March 30, 2021. https://www.reuters.com/article/us-china-tech-surveillance-trfn-idUSKBN2BM1EE. Accessed 10 May 2021

Bowling, B., & Iyer, S. (2019). Automated policing: The case of body-worn video. *International Journal of Law in Context, 15*(2), 140–161. https://doi.org/10.1017/S1744552319000089

Campbell, Z., & Jones, C. (2020). Leaked reports show EU police are planning a pan-european network of facial recognition databases. *The Intercept*, February 21, 2020. https://theintercept.com/2020/02/21/eu-facial-recognition-database/. Accessed 6 Feb 2021

Caruana, M. M. (2019). The reform of the EU data protection framework in the context of the police and criminal justice sector: Harmonisation, scope, oversight and enforcement, international review of law. *Computers & Technology, 33*(3), 249–270. https://doi.org/10.1080/13600869.2017.1370224

Christakis, T. (2021). *Facial recognition in the draft European AI regulation: Final report on the high-level workshop held on, April 26, 2021, May 27 2021*. https://ai-regulation.com/facial-recognition-in-the-draft-european-ai-regulation-final-report-on-the-high-level-workshop-held-on-april-26-2021/. Accessed 23 June 2021

Commission Nationale de l'Informatique et des Libertés (CNIL) (2019). *Reconnaissance Faciale - Pour Un Debat À La Hauteur des Enjeux, 15 Novembre 2019*. https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux. Accessed 3 Mar 2021

Commission Nationale de l'Informatique et des Libertés (CNIL) (2021). *Reconnaissance Faciale: La CNIL Met en Demeure CLEARVIEW AI de Cesser la Réutilisation de Photographies Accessibles sur Internet, 16 Décembre 2021*. https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-met-en-demeure-clearview-ai-de-cesser-la-reutilisation-de#:~:text=accessibles%20sur%20internet-,Reconnaissance%20faciale%20%3A%20la%20CNIL%20met%20en%20demeure%20CLEARVIEW%20AI%20de,de%20photographies%20accessibles%20sur%20internet&text=En%20mai%202021%2C%20l'association,la%20CNIL%20sur%20cette%20pratique. Accessed 3 Feb 2021

Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Convention 108 (2021). *Guidelines on facial recognition, T-PD(2020)03rev4, 28 January 2021*. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. Accessed 10 May 2021

Council of Europe/European Court of Human Rights (2020). *Guide on Article 18 of the Convention – Limitation on Use of Restrictions on Rights, 2020*. https://www.echr.coe.int/Documents/Guide_Art_18_ENG.pdf. Accessed 10 May 2021

Crutchfield, R. D., Skinner, M. L., Haggerty, K. P., McGlynn, A., & Catalano, R. F. (2012). Racial disparity in police contacts. *Race and Justice*, *2*(3). https://doi.org/10.1177/2153368712448063

Csonka, P., & Landwehr, O. (2019). 10 Years after Lisbon – How 'Lisbonised' is the Substantive Criminal Law in the EU? *Eucrim, 4,* 261–267. https://doi.org/10.30709/eucrim-2019-023

Doffman, Z. (2019). Hong kong exposes both sides of China's relentless facial recognition machine. *Forbes*, August 26, 2019. https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/?sh=57e4856342b7. Accessed 28 Mar 2021

Douglas, S., & Welsh, B. C. (2022). There has to be a better way: Place managers for crime prevention in a surveillance society. *International Journal of Comparative and Applied Criminal Justice, 46*(1), 67–80. https://doi.org/10.1080/01924036.2020.1788960

Dushi, D. (2020). The use of facial recognition technology in EU Law Enforcement: Fundamental rights implications. *Global Campus South East Europe, 2020*. https://repository.gchumanrights.org/handle/20.500.11825/1625. Accessed 23 May 2021

EDRI (2020). *Ban Biometric Mass Surveillance (A set of fundamental rights demands for the European Commission and EU Member States), 13 May 2020*. https://edri.org/our-work/blog-ban-biometric-mass-surveillance/. Accessed 13 May 2021

EDRI (2021a). *Challenge against Clearview AI in Europe', June 2 2021*. https://edri.org/our-work/challenge-against-clearview-ai-in-europe/. Accessed 1 Jan 2022

EDRI (2021b). *Press release: European commission jumps the gun with proposal to add facial recognition to EU-wide police database, December 8, 2021*. https://edri.org/our-work/press-release-ec-jumps-the-gun-on-prum/. Accessed 6 Feb 2022

European Commission (2021a). *Proposal for a regulation of the european parliament and of the council laying down Harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, COM/2021/206 final, Brussels, 21.4.2021*. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206. Accessed 21 Mar 2021

European Commission (2021b). *Police cooperation code: Questions and answers, 8 December 2021b*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_6646. Accessed 8 Feb 2022

European Council (2002). *Council framework decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33167. Accessed 14 May 2021

European Data Protection Board (2020a). *Guidelines 3/2019 on processing of personal data through video devices, version2.0, adopted on 29 January 2020*. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf. Accessed 5 May 2021

European Data Protection Board (2020b). *Guidelines 8/2020 on the targeting of social media users, version 1.0, adopted on 2 September 2020*. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf?fbclid=IwAR19D57q1MkR2DrDZvUpDuFFHzc-VHloVTEONOowE6yEjoiUXyDdVVNA3Oc. Accessed 10 Feb 2022

European Data Protection Board - European Data Protection Supervisor (2021). *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down Harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021*. https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en. Accessed 4 July 2021

European Data Protection Supervisor (2018). *EDPS Opinion 7/2018 on the proposal for a regulation strengthening the security of identity cards of union citizens and other documents, 10 August 2018*. https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en_0.pdf. Accessed 14 May 2021

European Data Protection Supervisor (2019). *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*. edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf. Accessed 17 Apr 2021

European Data Protection Board, Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement, Version 1.0, adopted on 12 May 2022, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_hu. Accessed 18 May 2022

European Network Against Racism (2019). *Data-driven policing: The hardwiring of discriminatory policing practices across Europe*. https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf. Accessed 23 Mar 2021

European Parliament (2021). *Use of artificial intelligence by the police: MEPs oppose mass surveillance, 6 October 2021*. https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance. Accessed 3 Feb 2022

European Parliament and Council (2021a). *Proposal for a Directive of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A782%3AFIN&qid=1639141440697. Accessed 5 Feb 2021

European Parliament and Council (2021b). *Proposal for a Directive of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A784%3AFIN&qid=1639141496518. Accessed 5 Feb 2021

European Parliamentary Research Service, Understanding EU counter-terrorism policy, January 2021. https://www.statewatch.org/media/1746/ep-briefing-eu-counter-terror-policy.pdf. Assessed 4 Jan 2022

European Union Agency for Fundamental Rights. (2018). *#BigData. Discrimination in Data-Supported Decision Making*. Publications Office

European Union Agency for Fundamental Rights (2019). *Facial recognition technology: Fundamental rights considerations in the context of law enforcement, 21 November 2019*. https://fra.europa.eu/

en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law. Accessed 18 Mar 2021
European Union Agency for Fundamental Rights and Council of Europe. (2018). *Handbook on European Data Protection Law*. Publications Office of the European Union
Government of Scotland (2018). *Code of practice on the acquisition, use, retention and disposal of biometric data for justice and community safety purposes in Scotland (Draft for Public Consultation), 22 March 2018*. https://www.gov.scot/binaries/content/documents/govscot/publications/consultation-paper/2018/07/consultation-enhanced-oversight-biometric-data-justice-community-safety-purposes/documents/00538315-pdf/00538315-pdf/govscot%3Adocument/00538315.pdf. Accessed 20 May 2021
Fagan, J., Braga, A. A., Brunson, R. K., & Pattavina, A. (2016). Stops and Stares: Street Stops, Surveillance, and Race in the New Policing. *Fordham Urban Law Journal, 43*(3), 539–614
Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race and the Future of Law Enforcement*. New York University Press, New York
Fussey, P., Davies, B., & Innes, M. (2021). 'Assisted' Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing. *The British Journal of Criminology, 61*(2), 325–344. https://doi.org/10.1093/bjc/azaa068
Gunning, P., Murphy, L., & Christodoulou, C. (2021). Are Clearview users in the Privacy Commissioner's Sights? *Financial Review*, Nov 14, 2021. https://www.afr.com/technology/are-clearview-users-in-the-privacy-commissioner-s-sights-20211112-p598gr, Accessed 2 Feb 2022
Haddad, G. M. (2021). Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom. *Vanderbilt Journal of Entertainment and Technology Law, 23,* 891–918
Harwell, D. (2019). A face-scanning algorithm increasingly decides whether you deserve the job. *The Washington Post*, November 7, 2019. https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/. Accessed 3 Mar 2021
Hasan, M. K., Ahsan, M. S., Abdullah-Al-Mamun, et al. (2021). Human Face Detection Techniques: A Comprehensive Review and Future Research Directions. *Electronics, 10*(19), 2354. https://doi.org/10.3390/electronics10192354
Hayward, K. J., & Maas, M. M. (2021). Artificial Intelligence and Crime: A Primer for Criminologists. *Crime Media Culture, 17*(2), 209–233. https://doi.org/10.1177/1741659020917434
IJIS Institute and International Association of Chiefs of Police (IACP) (2019). *Law enforcement - Facial recognition use case catalog, 2019*. https://www.theiacp.org/resources/document/law-enforcement-facial-recognition-use-case-catalog. Accessed 11 Jan 2021
Information Commissioner's Office (2019). *Information commissioner's opinion: The use of live facial recognition technology by law enforcement in public places, 2019/01, 31 October 2019*. https://jerseyoic.org/media/moqjayy1/live-frt-law-enforcement-opinion-20191031.pdf. Accessed 13 May 2021
Kindt, E. J. (2013). *Privacy and Data Protection Issues of Biometric Applications. Dordrecht, Heidelberg*. Springer
MacCarthy, M. (2021). *Mandating fairness and accuracy assessments for law enforcement facial recognition systems, TECHTANK, May 26, 2021*. https://www.brookings.edu/blog/techtank/2021/05/26/mandating-fairness-and-accuracy-assessments-for-law-enforcement-facial-recognition-systems/. Accessed 3 Feb 2022
Mann, M., & Smith, M. (2017). Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight. *UNSW Law Journal, 40*(1), 121–145
McGlynn-Wright, A., Crutchfield, R. D., Skinner, M. L., & Haggerty, K. P. (2022). The Usual, Racialized, Suspects: The Consequence of Police Contacts with Black and White Youth on Adult Arrest. *Social Problems, 69*(2), 299–315. https://doi.org/10.1093/socpro/spaa042
Murphy, E., & Tong, J. H. (2020). The Racial Composition of Forensic DNA Databases. *California Law Review, 108,* 1847–1911. https://doi.org/10.15779/Z381G0HV8M
Najibi, A. (2020). *Racial discrimination in face recognition technology, blog science policy, Special Edition: Science policy and social justice, October 24, 2020*. https://sitn.hms.harvard.edu/category/flash/science-policy/. Accessed 19 Mar 2021
Ousmane, A. M., Djara, T., Zoumarou, W., et al. (2019). Automatic Recognition System of Emotions Expressed through the Face Using Machine Learning: Application to Police Interrogation Simulation, *2019 3rd International Conference on Bio-engineering for Smart Technologies (BioSMART)*, 1–4. Doi:https://doi.org/10.1109/BIOSMART.2019.8734245

Paoli, L., Adriaenssen, A., Greenfield, V. A., et al. (2017). Exploring Definitions of Serious Crime in EU Policy Documents and Academic Publications: A Content Analysis and Policy Implications. *European Journal on Criminal Policy and Research, 23,* 269–285. https://doi.org/10.1007/s10610-016-9333-y

Raposo, V. L. (2021a). May i have some artificial intelligence with my human rights? *About the recent european commission's proposal on a regulation for artificial intelligence, KSLR EU Law Blog, May 24 2021*. https://blogs.kcl.ac.uk/kslreuropeanlawblog/?p=1569. Accessed 12 June 2021

Raposo, V. L. (2021b). Quarantines: Between Precaution and Necessity. A Look at COVID-19. *Public Health Ethics, 14*(1), 35–46. https://doi.org/10.1093/phe/phaa037

Raposo, V. L. (2022a). (Do Not) Remember My Face: Uses of Facial Recognition Technology in Light of the General Data Protection Regulation. *Information and Communication Technology Law*. https://doi.org/10.1080/13600834.2022.2054076

Raposo, V. L. (2022b). Ex Machina: Preliminary Critical Assessment of the European Draft Act on Artificial Intelligence. *International Journal of Law and Information Technology*, eaac007. https://doi.org/10.1093/ijlit/eaac007

Reinhold, F., & Mülle, A. (2021). AlgorithmWatch's Response to the European Commission's proposed regulation on artificial intelligence – A major step with major gaps, *Algorith Watch*, 22 April 2021. https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/. Accessed 10 May 2021

Renaissance Numerique (2020). *Facial recognition: Embodying European values, June 2020*. https://www.renaissancenumerique.org/publications/facial-recognition-embodying-european-values. Accessed 9 Feb 2021

Sénat (2021). *Biométrie: Mettre la Technologie au Service des Citoyens, 9 Juillet 2021*. https://www.senat.fr/rap/r15-788/r15-7885.html. Accessed 26 May 2021

Sobel, B. L. W. (2021). A New Common Law of Web Scraping. *Lewis & Clark Law Review, 25*(1), 147–207

Surveillance Studies Center (n.d.). *FAQS*. https://www.sscqueens.org/projects/scan/faqs. Accessed 22 May 2021

Taylor, N. (2002). State Surveillance and the Right to Privacy. *Surveillance & Society, 1*(1), 66–85

Vogiatzoglou, P., Quezada Tavárez, K., Fantin, S., Directives, P. N. R., et al. (2021). *JIPITEC, 11*, https://www.jipitec.eu/issues/jipitec-11-3-2020/5191/vogiatzoglou%2C_jipitec%20-11_3_2020_.pdf. Accessed 5 Feb 2021

Wiewiórowski, W. (2019). Facial recognition: A solution in search of a problem?, *European Data Protection Supervisor, Monday, 28 October, 2019*. https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en. Accessed 12 May 2021

Wong, K. L. X., & Dobson, A. S. (2019). We're Just Data: Exploring China's Social Credit System in Relation to Digital Platform Ratings Cultures in Westernised Democracies. *Global Media and China, 4*(2), 220–232. https://doi.org/10.1177/2059436419856090