INTERNET POLICY REVIEW
Journal on internet regulation

Volume 12 **Issue** 1

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Your face is not new to me – Regulating the surveillance power of facial recognition technologies

Giuseppe Mobilio *University of Florence* giuseppe.mobilio@unifi.it

DOI: https://doi.org/10.14763/2023.1.1699

Published: 31 March 2023
Received: 13 September 2022 **Accepted:** 5 December 2022

Funding: The research is supported by the project "SE.CO.R.E. TECH: Self- and Co-Regulation for Emerging Technologies: Towards a Technological Rule of Law", funded by the Italian Ministry for University and Research's (MUR's) "Progetti di Ricerca di Rilevante Interesse Nazionale" (PRIN; Bando 2017 – grant prot. no. 2017SW48EB).
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Mobilio, G. (2023). Your face is not new to me – Regulating the surveillance power of facial recognition technologies. *Internet Policy Review*, *12*(1). https://doi.org/10.14763/2023.1.1699

Keywords: Smart cities, Facial recognition software, Law enforcement, Surveillance, Fundamental rights, Human rights

Abstract: Facial recognition technologies (FRTs) represent one of the cutting-edge applications of artificial intelligence and big data for surveillance purposes. The uses of these biometric technologies are widespread in our cities. However, they may result in serious abuses against the rights of people and minorities, or even in new kinds of mass surveillance. The article focuses on "real-time" and "live" use by law enforcement authorities, one of the most discussed deployments of FRTs. The analysis addresses, from a constitutional point of view, whether banning these technologies is inevitable, or whether it is possible to regulate them in a way that allows their use while protecting the fundamental rights at stake and preserving democratic order and the rule of law. The principle of proportionality is the standard for defining appropriate regulatory measures. The article starts off by providing an overview of how FRTs work and some of the consequent ethical, technical, societal and legal concerns that arise. It then provides a critical analysis of EU data protection legislation and the AI Act proposal to examine their strengths and shortcomings in addressing the proportionate use of FRTs.

This paper is part of **Future-proofing the city: A human rights-based approach to governing algorithmic, biometric and smart city technologies**, a special issue of *Internet Policy Review* guest-edited by Alina Wernick and Anna Artyushina.

Introduction

Facial recognition technologies (FRTs) are one of the next frontiers for automatic identification of people and their use is now widespread in the smart environments of our cities (AI Now Institute 2019). Smart cities are networked with cameras and sensors embedded with software to automatically collect data from number plate readers, behavioural pattern detectors and facial recognition (FR) systems (Ahmad & Dethy, 2019). Law enforcement authorities (LEAs) are massively leveraging these new information and data-generating sources as automated policing tools (Bowling & Iyer, 2019). Biometrics – seen as the automated recognition of individuals based on their biological and behavioural characteristics (Jasserand, 2016, p. 68) – has given LEAs greater capability to identify people in public spaces. But FRTs are even more invasive than any other biometric technology. Compared to taking fingerprints or DNA samples, capturing the image of a face is much easier because it happens at a distance, without contact, with people in motion, without their awareness or consent. FR systems can also be incorporated in a wide variety of devices, such as CCTV cameras, body cams or drones, making recognition embedded, ubiquitous and low cost (Berle, 2020, pp. 2-5). Not surprisingly, since the outbreak of the COVID-19 pandemic, biometric surveillance has been used for remote symptom tracking, social distance monitoring and contact tracing to address health concerns (Van Natta et al., 2020).

As a result, FRTs are exponentially increasing the surveillance capacity of LEAs, but at the same time their use requires greater caution (Artyushina & Wernick, 2021). FRT deployment is founded on the need to protect public interests, fight crime or find missing vulnerable persons; nevertheless, it may result in serious abuses against the rights of people and minorities, or even in mass surveillance by oppressive regimes (Ferguson, 2017). The question that arises is whether the surveillance power of FRTs can find a place within constitutional systems. Considering some emerging categories, one wonders whether the regulation of these technologies can be reconciled with the perspective offered by views such as the "Human Rights-Based Approach" (Donahoe & Metzger, 2019) or Digital Constitutionalism" (De Gregorio, 2022). The aim of this article is to contribute to answering this question. In particular, the issue will be addressed by examining how the current legis-

lation that more directly affects FRTs – namely the EU data protection law – and the recently proposed AI Act of the EU protect the fundamental rights at stake, preserve the democratic order and the rule of law.

The answer is not straightforward, especially if we consider that several policy-makers have banned FRTs or placed a moratorium on them, as is happening in the USA, where some states and cities have prohibited LEAs from using these surveillance systems (Spivack & Garvie, 2020, pp. 89-94), or in Italy (Mobilio, 2021). Some voices have also been raised at the EU level, where the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), in their joint opinion on the AI Act, likewise called for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces (EDPB & EDPS, 2021). This option can be a last resort, but the real challenge for the regulation of FRTs is to balance risks and benefits (Chan, 2021, p. 307). We must avoid absolutising the concept of risk: rather, the risks must be weighed case by case in relation to concrete circumstances, and then balanced in terms of "optimal precautions" (Vermeule, 2014). So, the task is to try to lay down conditions and limits for the use of FRTs so as to lead them toward constitutional values. Only when this is not possible should they be rejected outright.

This article will focus on the deployment of FRTs by LEAs for policing and public security purposes, a scenario where risks and benefits come closer together. It will more specifically address one of the most pervasive and discussed applications, that is, "real-time" or "live" use in public spaces, where monitoring is constant, the number of people involved is indeterminate and recognition occurs instantaneously. The regulatory landscape is very diversified (Almeida et al., 2021), but the analysis here will mainly deal with Europe, though suggestions from the United States and Asia will not be overlooked, considering that these technologies circulate very easily around the globe. After a brief explanation of the FR procedure, the article will describe the possible uses of FRTs by LEAs. This will allow us to highlight the consequent ethical, technical and societal concerns that arise, as well as the risks to fundamental rights. Next, the analysis will consider how regulation – namely EU primary law and the data protection law – addresses these risks by implementing the principles of necessity and proportionality, which are considered to be the guiding principles for determining whether to ban or not, and possibly setting conditions for the use of FRTs by LEAs. The analysis will then move on to the AI Act to assess the progress and setbacks in addressing these risks in the light of the current legislation, with an emphasis on how the use of FRTs could potentially be allowed, although the restrictions on this arising surveillance power should be

very tight.

Looking at the face of FRT: A glance at how they are used

For centuries faces have been used by LEAs to identify people and read states of mind. Today, machines are able to do this automatically by harnessing algorithms and AI (Urquhart & Miranda, 2022). To grasp the implications of this automation, however, it is necessary to clarify how FRTs work. Recognition basically entails a procedure with several steps. *Firstly*, after an image (or footage) of a person has been captured, an algorithm detects the face in the picture. *Secondly*, the algorithms extract the facial features to create a biometric template that is a numerical representation that uniquely distinguishes that person. *Thirdly*, the algorithms compare the single template extracted with the facial images enrolled in a dataset called a "gallery" or "watchlist", in search of a match. People on the watchlist have been already identified and linked to salient information, so that a match allows the person of interest to be recognised. Matching is a *probabilistic process*, as the system expresses the similarity of the images with a percentage value, called a "similarity score". The higher the score, the higher the probability that the sample image matches the image in the gallery. Furthermore, for the purposes of this article, we will use "recognition" as a synonym for identification and categorisation (Art. 29 WP, 2012). There is *identification* – also called 1-to-many comparison – when the extracted template is compared with a gallery of many images (e.g., mugshots). The *categorisation*, instead, does not aim to identify a specific person, but rather to extract several characteristics from the facial image, such as age, ethnic origins, gender, health status and then classify the individual into one or more categories.

Once these premises are established, in order to facilitate our analysis, it is worth looking at some concrete examples distributed according to table 1, which reports some variables on the possible uses of FRTs. The distinction in columns is based on certain elements that may give rise to the ethical, technical, societal and legal concerns described later in the following paragraph. Those elements are purposes of recognition, targeting people and contexts in which the recognition takes place. In the rows, instead, the distinction is based on an increasing intensity of such concerns. The analysis, as premised, will be focused on "real-time" or "live" use in public spaces of FRTs.

TABLE 1: Variables on the possible uses of FRTs

	PURPOSES	TARGETED PEOPLE	CONTEXTS
+	Repression	Individuals	Controlled
+ +	Investigation	Groups	Quasi-controlled
+ + +	Prevention	Society	Uncontrolled

As regards the *purposes* (Raposo, 2022b, p. 4), LEAs can deploy FRTs for repressive purposes, e.g., to identify a person wanted for a crime or a fugitive. In addition, FRTs can be used for investigative purposes, i.e., to monitor a person's movement in a public space and reconstruct his or her interactions with other people after a crime has been committed, or to find missing vulnerable persons or children who are victims of crime. LEAs can also leverage FRTs for preventive reasons, i.e., to prevent a previously identified perpetrator from committing another crime. In this case no crimes have been committed, so there is also the problem of respecting the presumption of innocence. Another distinction can be made based on the people undergoing surveillance, and in particular the *number of people targeted*. So, FRTs can be used to target specific individuals, to detect specific categories of individuals or to scan every person in a society. Lastly, we need to consider the *context* of use. FRTs can work within controlled environments, that is under optimal conditions (of light, posture, etc.), and with the cooperation of people subject to recognition, as in the case of technology supporting border control (so-called "smart borders"). However, the most common applications of FRTs are in quasi-controlled or uncontrolled environments, also called "in the wild". Here LEAs deploy FRTs on public streets, involving an indeterminate number of people that are potentially unaware of or hostile to these forms of surveillance. The accuracy of recognition can also be influenced by uncontrolled conditions, as the data collected in these contexts – as it will be seen – may not meet sufficient data quality requirements.

Specificities and dangers of FRT: Ethical, technical, societal and legal concerns

FRTs have come a long way since their first appearance at the 1970 World's Fair in Osaka or their commercialisation in the USA during the 1990s, with a rapid expansion after 11/9 (Gates, 2011). Well-documented examples from today reveal how FRTs give LEAs an unprecedented surveillance power, which gives rise to several orders of problems. From an *ethical* standpoint FRTs directly entail many values re-

lated to human beings, such as: autonomy, also in regard to awareness of and consent to FRT use; non-maleficence, seen as avoidance of the risk of erroneous recognition; beneficence, seen as leveraging the benefits of FRTs in protecting security; justice, seen as non-discrimination of specific groups; responsibility, in the sense of accountability or liability for the consequences of FRT uses (Chan, 2021, pp. 323-324). Ultimately, there are immediate implications for human dignity, which requires that individuals are not treated as mere objects. FRTs produce an "informatization of the body" (Van Der Ploeg, 2005), whereby body parts are objectivised and become direct sources of digital information for automated external controls to which the person is subjected.

From a *technical* standpoint, FRTs have to tackle the problem of accuracy. FRTs work on a probabilistic basis and may engender errors in the case of false positives, when the software finds a match with a face in the watchlist that does not actually match (consequently giving rise, for example, to a wrongful arrest), or false negatives, when the software fails to find a match with a face present on the watchlist (thus allowing, for example, a suspected terrorist to pass security checks) (Buolamwini et al., 2020, p. 3). Determining whether FRTs are accurate in recognising a match is very challenging because there are many technical variables to consider and many ways to assess accuracy (Fussey et al., 2021, p. 337). Data also influences accuracy. FRTs are more prone to errors when sample images have poor quality, due to collection in an uncontrolled environment and non-cooperative scenarios; when watchlists are configured with images that are not homogeneous in terms of standard and resolution; or when watchlists contain images of people who closely resemble one another (Grother et al., 2019). Even the quality of datasets used to train ML algorithms is crucial, as we will see.

From a *social* standpoint, the deployment of FRTs divides public opinion and is not easily accepted. In 2020 the EU Agency for Fundamental Rights (FRA) released the results of a survey which revealed that only 17% of people in the EU are willing to share their facial image with the public authorities for identification purposes (Christakis et al., 2020).

All these concerns call for even more attention to be paid to the impact of FRTs on *fundamental rights*. These technologies, indeed, broadly affect a multiplicity of rights (FRA, 2020, pp. 18-32). Limiting the focus to the Charter of Fundamental Rights of the European Union (CFREU) and the European Convention on Human Rights (ECHR), the first rights at stake are respect for private life and protection of personal data (Articles 7-8 CFREU and 8 ECHR). The former includes the right to enjoy a sphere of physical, psychological and relational intimacy, which is strongly

jeopardised by such invasive technologies that allow a person's behaviours or habits to be monitored. The latter includes the right to maintain control over one's own data, even in public spaces. But the use of live FRTs implies collecting, comparing, storing and sharing facial images and biometric templates, greatly reducing such control. Other constitutional principles that interfere with FRTs are equality before the law and non-discrimination (Articles 20-21 CFREU and 14 ECHR). The use of these technologies has a high risk of engendering discrimination based precisely on the grounds cited therein, such as sex, race, ethnic origin, membership of a national minority, disability, age or sexual orientation and genetic features, such as phenotypic traits revealed by the face. On the one hand, it has been argued that FRTs enable LEAs to categorise and distinguish one person from others based on the above-mentioned elements and make decisions about them accordingly. On the other hand – as will be discussed further – FRTs are less accurate as a result of errors and biases. The pervasiveness of FRTs may also lead to interference with other freedoms and constitutional values, directly or indirectly through a chilling effect. Examples include the freedom of expression and freedom of assembly (Articles 11-12 CFREU and 10-11 ECHR).

The fact that this surveillance power is not exclusively in the hands of public authorities raises even greater concerns. It is private companies that develop these technologies and make them available to LEAs; they are primarily driven by profit motives without any regard for the general good or the protection of rights. One need only consider the case of Clearview AI, the notorious start-up that has developed FRT systems sold to over six hundred agencies in the U.S., by scraping images from the internet and social media without the consent of people or platforms (Rezende, 2020). Other Big Tech companies, such as IBM, Microsoft and Amazon, have instead decided to suspend the development or sale of FRTs to US police departments until there is national regulation, given worries about the potential abuses or misuses (Heilweil, 2020).

The right measure in the use of FRT under the current regulation

At this point, the question arises as to whether and under what conditions LEAs can lawfully use FRTs and to what extent their use can be curtailed by regulation. Specifically, at a constitutional level, answering this question entails examining the conditions that the regulation of FRTs must meet in order to be lawful in restricting fundamental rights. The keystone for this analysis is Article 52(1) of the CFREU and, in particular, the principle of proportionality, which provides the crite-

rion for finding the right balance between the objectives pursued and the sacrifice of rights.[1] For the purposes of the analysis, it will first be necessary to examine the need for a legal basis to regulate the use of FRTs, and then to consider the proportionality test, which legislation on these technologies must be subjected to, drawing also on the case law of the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR), particularly regarding data protection, which has provided the necessary coordinates.

In search of a law on FRT

According to Article 52(1) of the CFREU any limitation on the exercise of the data protection right "must be provided for by law". The need for a legal basis has been interpreted by the CJEU to mean that the law must lay down "clear and precise rules" governing "the scope and application of the measure" in question, imposing "minimum safeguards" so that individuals whose data has been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and any unlawful access and use of that data (Digital Rights Ireland, § 54) (Schrems II, § 176). Article 8(2) of the ECHR similarly requires that the interference with the exercise of the right to respect for private life, which includes the protection of personal data, must be grounded "in accordance with the law". Accordingly, the ECtHR has specified the requirements of "foreseeability" and "accessibility", clarifying that the law must be "sufficiently clear" in its terms to give citizens an adequate understanding of the conditions and circumstances under which the authorities will be empowered to resort to secret surveillance and data collection measures (Shimovolos, § 68). In particular, the law must set out minimum safeguards concerning: the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them and the kind of remedy provided by national law (Shimovolos, § 68).

However, there is currently no legislation in Europe that *directly* regulates FRTs, particularly their use for law enforcement purposes. This certainly does not mean that there are no regulations that offer protection of fundamental rights and de-

1. According to the Article 52(1) of the CFREU, all measures limiting fundamental rights are considered lawful if they: are provided for by law; respect the essence of the rights; genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others; and are necessary and proportional to the objectives pursued. Though it is possible to consider policy aims as falling within the objectives of general interest, the assessment of a possible violation of the essence of the rights, understood as a macroscopic interference with those rights, is less clear, since no law has yet been annulled for violating the essence of the right to data protection, and only in the Schrems I case (Schrems I) did the CJEU find a violation of the respect for private life (Article 7 CFREU) and the right to effective judicial protection (Article 47 CFRUE).

mocratic values against this surveillance power. Data protection legislation has become more and more decisive, and its applicability also extends to FRTs. We are referring, at the EU level, to Directive (EU) 2016/680 (Law Enforcement Directive – LED), which applies to the processing of personal data for law enforcement purposes, such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, both by a public authority and any other public or private entity entrusted by law for those purposes (Article 3(7)) (Brewczyńska, 2022).[2] Within the framework of the Council of Europe, we instead consider the Convention for the protection of individuals with regard to the processing of personal data, amended in 2018 (Convention 108+). Moreover, the EDPB (EDPB, 2022), national data protection authorities and the Consultative Committee of the Convention 108+ (Consultative Committee, 2021) have recently investigated how both these pieces of legislation actually regulate FRTs. However, those same regulations emphasise the need for legislation that incorporates the substantive requirements set by the courts. National case law and data protection authority decisions confirm the urgency of filling this gap.

As to the former, it is worth considering the famous case "Bridges v. The Chief Constable of South Wales Police", in which the High Court of Justice of Cardiff (R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police, 2019) and the Court of Appeal of London (R (on the application of Bridges) v Chief Constable of South Wales Police, 2020) took FRTs to the stand to decide on whether police use of live FRTs in public spaces complies with the LED and UK national legislation, but more broadly gave insights into how to interpret data protection rules (Zalnieriute, 2021). Specifically, the Court of Appeal stated that the relevant policies regulating FRTs did not have the "necessary quality of law" (R (on the application of Bridges) v Chief Constable of South Wales Police, 2020, § 86 ff.): consequently, the Court declared that individual police officers should not have too much discretion in deciding who to target for surveillance, i.e., who can be placed on a watchlist and matched with a sample image ('who question'), or the location in public spaces where FRTs can be deployed ('where question'). A similar conclusion was reached by the Italian Data Protection Authority in its opinion on 'Sari Real Time', a real-time live facial recognition system developed for the Ministry of In-

2. Otherwise, the applicable legislation is Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR), which does not apply to the processing of personal data "by competent authorities" and to the same five law enforcement tasks listed by the LED (Article 2(2)(d) GDPR). Despite the attempt to separate the two regimes, GDPR and LED cannot be considered dichotomous, given the importance of national law in defining "criminal offences", the private bodies entrusted with policy tasks, the stages of criminal proceedings, or preventive activities, which thus differ between Member States.

terior, that had not yet been implemented. The Italian Authority established that 'Sari Real Time' was not supported by any legal rules governing FRTs or imposed safeguards against automated processing 'on a large scale' that could also extend to people who were not the subject of 'attention' of LEAs (Garante per la protezione dei dati personali, 2021).

The thorny issue of respecting the proportionality principle

Proportionality is a key instrument of judicial methodology, which enables the Courts to condition state intervention to constitutional rights and values (Tridimas, 2018, p. 243). As said earlier, respect for the proportionality principle is a condition for the legitimacy of a measure limiting fundamental rights. The application of proportionality entails a three-part test: suitability, necessity and *strictu sensu* proportionality (de Búrca, 1993, p. 113) (Barak, 2012, p. 243 ff.) (Dalla Corte, 2022).

The first sub-test of *suitability* assesses whether a measure is appropriate for the achievement of the objectives it pursues. More precisely, the assessment includes the "worth" of the purpose pursued and the "rational connection" between the measure and that purpose (Barak, 2012, pp. 303 ff.). So, the first question is whether the use of FRTs by LEAs is fit for the purpose of fighting crime. In this case the answer can generally be considered affirmative, but in order to justify the "rational connection", the CJEU requires a precise definition of the objectives pursued by a measure, in particular whether it entails a serious interference with the right to personal data protection (Tele2 Sverige AB, § 102) (La Quadrature du Net, § 136). The suitability requirement is therefore entangled with the above-mentioned need for more precise rules, since the vagueness and generality of the definition of the objectives preclude this sub-test.

The suitability test does not seek to determine whether the disadvantages and costs – in terms of restricting fundamental rights – outweigh the benefits. This type of assessment is relevant to the other two sub-tests, where the main concerns are concentrated. These two sub-tests have also been detailed by the courts, although there are not many pronouncements that help to make a clear distinction between them (Dalla Corte, 2022, pp. 270-271). The first one is the *necessity test* (EDPS, 2017), which basically considers whether the restrictive measure is genuinely effective, understood as "essential" for achieving the objective of general interest pursued, and whether it is "the least intrusive" for the rights at stake. So, the second question is whether there are means other than FRTs which are similarly suitable and impose less interference with fundamental rights. On this point, the evaluation must be carried out very carefully, since there are less restrictive tools

for investigating and prosecuting crimes that do not involve such pervasive automated surveillance, ethical concerns and high potential error rates.

The last step is the *strictu sensu proportionality* test, which entails a different kind of assessment. Indeed, this sub-test consists of a broader comparison aimed at finding a balance between the intensity of the interference with rights ("costs") and the importance of the objective to be achieved in a given context ("benefits") (EDPB, 2019). In this case, the assessment of proportionality is always performed on a legislative measure *ex ante*, but the test aims to ascertain *in concreto* the objective pursued and the way in which fundamental rights are affected by envisioning the scenarios where the measures provided by the law would be applied. Again, the assessment is very tricky and involves manifold aspects. Bearing in mind the variables set out in table 1, when the *strictu sensu* proportionality test refers to costs, it considers the impact of FRTs, taking into account the context of surveillance (e.g., open public spaces), the scope (e.g., the number or the age of individuals involved), the level of intrusiveness (e.g., identification, categorisation and profiling of people, and even the rates of errors that may occur) and the fundamental rights of data subjects that may be affected (including the chilling effect). When this sub-test refers to benefits, on the other hand, it considers the needs and importance of the objectives pursued, taking into account the specific purpose (e.g., border security or surveillance of street furniture), or the seriousness of the crime prosecuted (e.g., terrorism or pickpocketing) (EDPB, 2022).

The proportionate use of FRT under data protection regulations

Setting the conditions for the proportionate use of FRTs in legislation is even more complex because the proportionality test, as outlined above, needs to take into account how data protection regulations specifically address the need for proportionality in the use of FRTs. Proportionality, as mentioned, is a cornerstone of Article 52(1) of the CFREU, but its testing is often 'nested' within proportionality in EU data protection law (Dalla Corte, 2022, p. 266) (Guinchard, 2018, p. 440), i.e., it is often subject to consideration of how the principle is articulated in existing data protection law. In order to understand whether legislation on the use of these technologies by LEAs involves a truly proportionate sacrifice of rights, we need to look at how data protection regulations deal with some of the most sensitive issues at stake in the proportionality test and which will have to be assessed when FRTs are actually used. The emerging problematic aspects of the relationship between legislation and proportionality will then be addressed in order to give an

opinion on the AI Act.

The LED adopts a regulatory framework that relies on a broader risk-based approach, in turn based on the proportionality principle (Gellert, 2018). Two aspects of this approach are worth noting for the purposes of this analysis. The first one is the importance of the general *principle of accountability*. Where LEAs use FRTs, they must implement "appropriate technical and organisational measures" in order to comply and be able to demonstrate compliance with data protection rules (Article 19 LED). The stringency of safeguards that LEAs must implement will vary in proportion to the severity of the risk, that is, the likelihood that these rules and rights will be violated (Yeung & Bygrave, 2022, p. 146). As a consequence, LEAs using FRTs must be accountable for the application of the rules outlined here, on the assumption that the issues raised by the application and use of these surveillance technologies have not yet been thoroughly explored (Menéndez González, 2021, pp. 87-88).

Secondly, the main tool for assessing the concrete risks that may arise and for managing the response measures is the *data protection impact assessment* (DPIA), designed as a mechanism to promote accountability (Demetzou, 2019). According to the LED, when a type of processing of personal data is likely to result in "a high risk to the rights and freedoms", the controller, prior to the processing, should provide a DPIA containing (at least) a description of the envisaged processing operations, an assessment of the risks, the measures envisaged to address them, safeguards and mechanisms to ensure the protection of personal data and demonstrate compliance with the LED (Article 27 LED).[3] As a result, the DPIA is a tool for assessing *ex ante* a specific and concrete type of processing by a controller. This kind of assessment, despite the differences, takes account of many factors which are also relevant for the purposes of the above-mentioned proportionality test. In the case of the *strictu sensu* proportionality sub-test, in particular, the assessment of the proportionality of a legislative measure is conducted at a more abstract level, but it could nevertheless be considered as a "DPIA on the law" (EDPS, 2019, p. 22). However, there is a growing demand to adapt this instrument to the impact on rights produced by algorithmic technologies (Janssen, Seng Ah Lee & Singh, 2022), specifically by FRTs (Castelluccia & Le Métayer Inria, 2020).

Having pointed out these two aspects, we must now examine the provisions of data protection regulations that attempt to impose a proportionate use of FRTs and

3. When a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, or involves a high risk to the rights and freedoms of data subjects, the controller must consult the relevant supervisory authority (Article 28 LED).

the difficulties in achieving this objective. The first barrier to a disproportionate use of FRTs lies in the data regime. Indeed, the LED has distinguished between *personal data*, such as simple facial images, and *biometric data*, i.e., data resulting from specific technical processing relating to personal data with the aim of uniquely identifying a person (Articles 3(13) and similarly 6(1) Convention 108+) (Kindt, 2018, p. 527). The biometric templates processed by ML algorithms fall into the latter category and their processing in any case constitutes a serious interference in itself, regardless of the results of the recognition, e.g., a positive match (EDPB, 2022, p. 3). Consequently, there is a more restrictive regime for FRTs, as LEAs are allowed to process biometric templates – it is important to stress here – only if a double requirement is met: "where strictly necessary" and "where authorised by Union or Member State law" (Article 10(1)(a) LED).[4]

Strict necessity echoes the requirement of necessity – as we have seen – also laid down at the primary level in terms of "essentiality" and "least restrictiveness" for fundamental rights. But the LED sets a very stringent requirement, namely that the restriction must be limited to what is "absolutely necessary" (EDPB, 2022, p. 19). Drawing inspiration from Article 29 Working Party opinions (Art. 29 WP, 2017), CJEU case law (Digital Rights Ireland, §§ 57-62) and the variables in table 1, appropriate safeguards against the disproportionate use of FRTs can be conceived on a number of grounds. On the legal side, it is possible to limit the purpose of the processing (e.g., allowing their use for investigating only certain categories of serious crime, or excluding their use for preventive purposes) or their actual deployment (e.g., restricting the interference to personal data pertaining to a particular time period, geographical area or categories of persons). On the technical and organisational side, it is possible to impose additional data security measures to ensure the confidentiality or integrity of data (e.g. through encryption). On the procedural side, it is possible to consider the prior authorisation of a court or another independent body for the specific use of FRTs, or human intervention in order to verify the match between the sample image and the images in the watchlist to exclude false positives (Article 11(1) LED). *Authorisation by law*, on the other hand, echoes another requirement laid down at the primary level, namely "provision by the law". However, as mentioned above, the lack of specific legislation directly regulating FRTs means that there is no regulation for the lawful restriction of fundamental rights that meets the characteristics of "necessary quality of law", including in

4. Alternative to the latter, biometric data may be processed to protect the vital interests of a person, or if it is "manifestly made public by the data subject". In the latter case, it is not sufficient to make public a facial photo, e.g., on a social network, but the data subject must have deliberately made public the biometric template.

terms of "foreseeability" and "accessibility" as clarified by the CJEU and ECtHR. Moreover, this absence of legislation means that there is no legal basis for the processing of biometric data either, according to Article 10 of the LED. In conclusion, we need clear rules detailing the appropriate legal, technical, organisational and procedural measures just mentioned for the use of FRTs by LEAs.

Other provisions that attempt to address the use of FRTs in a proportionate way are the purpose limitation and data minimisation principles. *Purpose limitation* requires that images be collected for "specified, explicit and legitimate purposes" and not further processed "in a manner that is incompatible with those purposes" (Articles 4(1)(b) LED and 5(4)(b) Convention 108+). For this reason, the legislation also defines the boundaries of the possible legitimate re-use of images (so-called secondary processing) for other purposes. Here the LED again requires explicit authorisation by law and that "processing is necessary and proportionate to that other purpose" (Article 4(2) LED). Therefore, law enforcement purposes will not legitimise *per se* the re-use of data. Data collected for one crime may also be used for solving another crime, provided that compatibility is "assessed on a case-by-case basis and subject to a legal basis including clear and explicit safeguards" (Art.29WP, 2015, p. 6). In concrete terms, a facial recognition match obtained in one investigation may not be re-used in another investigation and accessed by different authorities unless it is verified as indispensable, in accordance with the principle of proportionality, for the identification of a specific suspect, victim or witness, and not for the identification of people unrelated to the crime or for generic categorisation purposes.[5]

According to the *data minimisation* principle, on the other hand, the processing of images must be "adequate, relevant and not excessive" in relation to the legitimate purpose pursued (Articles 4(1)(c) LED and 5(4)(c) Convention 108+). This principle is also relevant for FRTs considering that they require an enormous number of images in order to be trained and to build watchlists. As will be better explained later, the use of highly differentiated images to train ML algorithms will lead to more accurate recognition. Moreover, as the UK Information Commissioner's Office (ICO) pointed out, LEAs can follow very different practices in building watchlists, using images of people who are "in the focus of police attention" specifically targeted by police operations to be carried out (e.g., sporting events, specific crimes) or indiscriminately expanding the number of images to be compared (ICO, 2019, pp. 14-18).

5. This is why Article 6 of LED requires a clear distinction be made between the personal data of different categories of people, such as suspects of a crime, victims or people convicted.

These two principles, however, risk proving an inability to guide a proportionate use of FRTs. As big data analytics teaches, alongside a primary use of images there is a secondary use that reveals the "optional value" of this data, the entity of which cannot be predicted (Mayer-Schönberger & Padova, 2016, pp. 317-320). The cases of re-use of data, the training datasets and watchlist building are illustrative of how images acquire value when processed in other activities or for other purposes. From the perspective of LEAs, this represents a "practical convenience" (Simoncini & Longo, 2021) in the use of data and FRTs that they hardly want to relinquish. Therefore, strong legislation is needed to counteract this tendency of LEAs: to unduly exploit data and technologies on practical grounds and, by encouraging the proportionate use of FRTs, prevent regulators and users from abusing surveillance power.

The mentioned principles operate in continuity with the *storage limitation* principle, under which personal data must be stored in a form that allows the identification of data subjects for a period of time no longer than is necessary to achieve the legitimate purposes (Article 4(1)(e) LED and 5(1)(e) Convention 108+). As stated by the CJEU, data retention must "meet objective criteria, that establish a connection between the data to be retained and the objective pursued" (Tele2 Sverige AB, § 110): when this connection is broken and there is no further legal basis for processing, data must be erased or made anonymous. Thus, with respect to LEAs' activities, the retention period should vary, for instance, in light of the conclusion of a particular inquiry or the passing of a final judicial decision. In the case of FRTs, we must also consider the results of the recognition: if there is no match, facial images and biometric templates cannot be retained and have to be automatically deleted; if there is a match, the data (and matching reports) can be retained for a strictly limited time provided by law with necessary safeguards (Consultative Committee, 2021, p. 12). Thus, national law may provide for a mixed system combining general maximum time limits with a periodic review of the need to store data for a further period, which should be assessed in terms of necessity and proportionality (Art. 29 WP, 2017, p. 4). In this respect, the retention of data for intelligence or preventive purposes is unlikely to pass a strict proportionality test, since in these cases images are stored, especially on watchlists, without any specific crime to be prosecuted and thus without any point of closure. The storage limitation principle is thus a paradigmatic example of how legal rules should support the proportionality test by placing a final limit on data processing and FRT use, which can only be overcome based on a rigorous assessment.

The principle of proportionality also comes to the fore in respect of other core

rights enshrined in data protection legislation, namely the right to be informed about facial recognition and the other rights that flow from it. Indeed, LEAs must make available to the public various types of *information* about the use of FRTs, such as the proceeding authority, the purposes of recognition and the existence of other rights (Articles 13 LED and 8 Convention 108+).[6] The right to be informed is also a prerequisite for the exercise of *other rights*, such as the right to request access to stored data, or the right to rectification and erasure, especially in case of inaccuracy (e.g., low quality) or unlawful use of images (Articles 14 and 16 LED). In 2019 the importance of those rights was stressed by the Hamburg Commissioner for Data Protection when he ordered the police to delete the database of video surveillance FRT material that was created to prosecute the violent protesters at the June 2017 G20 Summit (Hamburg DPA, 2019). The Hamburg Commissioner criticised the fact that people involved were not aware of such legal interference and therefore could not exercise their rights or even lodge an appeal against it (Raab, 2019).

However, such rights face limits in proportion to the need to protect public interests. National legislation can limit those rights in order to not prejudice inquiries, the prevention or prosecution of criminal offences or the protection of public security (Articles 13(3), 15 and 18 LED, and 9(2) Convention 108+). However, by referring to national law, European legislation leaves too much discretion to the States. The LED does not specify any minimum requirements for national legislation, apart from implicitly referring to the proportionality principle. Thus, each State can autonomously compare the interests at stake, define the purposes or crimes that can justify such limitations, the information that can be withheld and thus determine the level of awareness of the population subjected to FRTs. However, it is precisely the non-transparent use of these technologies by LEAs and the perception of exposure to such controversial forms of surveillance that may help to explain concerns and protests such as those that have erupted in the US over the use of FRTs against Afro-Americans (Williams, 2020). The case of the rights in question therefore illustrates the need for detailed state legislation to not hollow out the guarantees provided to citizens subject to FRTs.

Finally, there is an aspect to consider when assessing proportionality, which is also linked to the protests just mentioned, and which is perhaps the greatest source of concern about the use of FRTs. This is the issue of *bias* (Friedman & Nissenbaum,

6. Unlike the GDPR, the LED does not consider the principle of transparency. Other information, such as the legal basis for the processing, or the storage period, must be provided to the data subjects in "specific cases" (Article 13(2) LED), which refers to situations where the data subjects need to be made aware of the processing in order to effectively exercise their rights.

1996). Bias can lead to errors and inaccuracies in recognition, and consequently to racial, ethnic and gender discrimination. These risks need to be weighed as a cost of using FRTs in the proportionality test. Many forms of bias can afflict these systems (Veale & Binns, 2017) (Barocas & Selbst, 2016), but here it is sufficient to focus on those occurring within the training dataset used for ML algorithms. ML models can indeed embed discrimination due to model construction choices and, in particular, the data models under consideration (Kroll et al., 2017, p. 681). This is the case, for instance, when labels are used to classify images and sort them into categories. The aim is to help ML systems recognise newly captured unlabeled images. But labels simplify the world in order to "capture" it in data, and consequently bias can arise both in the choice of class labels and in the labelling activity (Borgesius, 2018, p. 15). Labels may cover names (for identification purposes), or racial and national identities, emotions, or other physical and behavioural features (for categorisation purposes), but the results can be very problematic (Crawford & Paglen, 2021). Moreover, bias can also occur when ML algorithms are trained on biassed data or learn from a biassed sample (Borgesius, 2018, p. 17). The accuracy of algorithms that automatically perform identification will be compromised if training data reflect implicit biases (Leslie, 2020). So, the greater the "pluralism" of the data used in relation to sex, age and ethnic origin, the greater the system's ability to identify people. Recent studies, however, show that dark-skinned people and women are heavily underrepresented in these datasets (Cook et al., 2019) (Merler et al., 2019). Thus, dark-skinned women are associated with higher facial recognition error rates than light-skinned men of Caucasian origin, especially in the case of uncontrolled environments such as public streets (Buolamwini & Gebru, 2017) (Grother et al., 2019).

Other people who may experience discrimination as a result of the lower accuracy of FRTs include children, the elderly and people with disabilities. In relation to age, due attention must be paid to the temporal alteration of the physical elements used for recognition (FRA, 2019, p. 90). With respect to disabilities, in addition, it is necessary to consider the consequences resulting from accidents or specific syndromes that can alter the morphological and behavioural state of a person (Byrne-Haber, 2019).

Data protection regulations have tackled bias where it states that personal data, also when used to train FRTs, should be "accurate and, where necessary, kept up to date" (Article 4(1)(d) LED). For this reason, LEAs wishing to employ FRTs must be able to demonstrate that there are no biases in these systems. As the "Bridges" case also shows, LEAs should make an evaluation of the demographic composition

of each algorithm training dataset, either directly or through independent verification, to determine that the dataset is not biassed towards any particular demographic group. No reasons of commercial confidentiality given by the manufacturer of the system can justify an LEA's failure to make this assessment (R (on the application of Bridges) v Chief Constable of South Wales Police, 2020, § 199). Otherwise, smart policing instruments are legally and ethically unacceptable. However, this goal is not readily achievable. On the legal side, detecting bias or discrimination is not a specifically mentioned justification for processing sensitive personal data. Therefore, it may currently be unclear to what extent such processing is lawful in view of data protection legislation (FRA, 2022, p. 26). In addition, it is very difficult to prove that a person has suffered from discrimination precisely because of the poor quality of the training dataset. Moreover, the widespread use of FRTs trained on unrepresentative data makes it difficult to replace or correct systems currently in use. It is clear, therefore, why legislation regulating FRTs must be very cautious in assessing the potential benefits against possible, serious drawbacks.

The future of FRT regulation: The AI Act

An attempt to adopt a regulation that would set more stringent conditions for proportionate use of FRTs is offered by the proposal for a Regulation "laying down harmonised rules on artificial intelligence" (so-called *AI Act*), which is still being negotiated at the time of writing this article (Council of the European Union, 2022). EU Institutions have prepared the ground with several documents, such as the "Ethics Guidelines for Trustworthy AI", produced by the High-level Expert Group on AI in 2019, or the White paper on AI published in 2021 by the European Commission, which laid down the foundations for a "human-centric" approach (Floridi, 2021). The aim is, on the one hand, to implement a trustworthy AI and, on the other, to facilitate the development of a Digital Single Market in the EU.

The AI Act employs a *risk-based approach* (De Gregorio & Dunn, 2022), distinguishing between uses of AI that create "unacceptable risks", "high risks" and "low" or "minimal risk", each associated with different redlines. Within the first category, the proposal bans "the use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes" (Article 5(1)(d)). This applies to the 'particularly intrusive' FRTs discussed thus far (Recital 18). However, the AI Act provides such broad exceptions to this ban that "it barely deserves to be called a 'prohibition'" (Smuha et al., 2021, p. 25).

Firstly, LEAs can deploy FRTs when "strictly necessary" for the *objectives* of: searching for crime victims; preventing a "specific, substantial and imminent threat" to

the life of people, a critical infrastructure or a terrorist attack; and prosecuting perpetrators or suspects for crimes sentenced with a certain punishment referred to in the Decision on the European Arrest Warrant[7], or in the law of Member States. The *actual deployment* of FRTs, therefore, must take into account several elements: the nature of the situation giving rise to the possible use and the consequences for rights and freedoms. LEAs should comply "with necessary and proportionate safeguards and conditions", as regards "the temporal, geographic and personal limitations" (Article 5(2)). Moreover, each individual use must be *authorised* by a national judicial authority or independent administrative authority (except in urgent cases, where validation must be requested "without undue delay during use of the AI system"), on the basis of "objective evidence" and "clear indications" in terms of "necessity for and proportionality to" the objectives (Article 5(3)). *Member States* will have to specify the rules for such authorisation and may also provide for the option of restricting the use of FRTs in relation to the offences to be prosecuted (Article 5(4)). National rules are indispensable, because the future AI Act cannot be invoked as a sufficient legal basis under the provisions of the LED (Recital 23). Finally, FRTs are also expressly subject to the conditions set by the second category of *high risk* uses of AI (Annex III(1)). The new regime is inspired by that of the New Legislative Framework and imposes numerous burdens on all value chain participants. Providers, in particular, before they can place technology on the market, must demonstrate compliance with all the obligations by undergoing a "conformity assessment", as an internal control check that once passed allows the CE mark to be affixed to high-risk AI systems.[8]

As a result, FRTs empowered by AU will be regulated by dedicated legislations, and their employment will be governed by the principles of proportionality and necessity, under the supervision of an independent (possibly judicial) public authority. With reference to the distinction made in table 1, LEAs will only be empowered to use FRTs to search for certain individuals and for purposes of investigation and repression of a crime, since it is very difficult for other cases to meet these stringent requirements. However, the overall framework raises some concerns. The problems can be divided into three groups, depending on whether they relate to (i) the formulation of the rules just mentioned, (ii) to what is missing in these rules or (iii) to the relationship of these rules with existing data protection legislation.

7. Council Framework Decision 2002/584/JHA of June 13, 2002.

8. With the exception of remote biometric identification systems, which are subject to a third-party conformity assessment (Art. 43(1)). The latter can in turn be excluded if the provider demonstrates that the system complies with the "harmonised standards" (Art. 40) or with the "common specifications" (Art. 41).

With regard to the first set of problems, i.e., *exceptions to the prohibition* of the "real-time" use of FRTs by LEAs, we must first look at the *objectives* set. Here there is an attempt to limit the use of FRTs to the most serious cases and "narrowly defined situations" (Recital 19), but some of the crimes listed as exceptions in the European Arrest Warrant Decision are not particularly serious (e.g., corruption or fraud) (Raposo, 2022a, p. 96); the mention of critical infrastructure similarly risks leaving LEAs with too wide a margin of discretion in the use of FRTs. Even the reference to national law, although limited to offences punishable by a sentence of at least five years, seems to be too broad. Consequently, there is a risk that the legislation will allow a disproportionate use of these technologies.

Looking at the *actual deployment* of FRTs, what is essentially required is a case-by-case assessment, not left up to LEAs, and based on the principle of proportionality. This is undoubtedly a step forward compared to the currently existing rules. But even here it would be necessary to look closely at the national implementing legislation, which risks, on the one hand, not providing sufficient guarantees for citizens regarding the intervention of the judicial or independent administrative authority and, on the other hand, falling short in terms of regulation, because the Proposal does not require Member States to adopt rules on other aspects of the use of these systems that should be regulated, although CJEU and ECtHR case law has emphasised the importance of having clear, precise and accessible rules governing the scope and application of mass surveillance measures (Barkane, 2022, p. 155). As mentioned, data protection regulation clearly shows that these rules should support the proportionality assessment, also in contrast to considerations regarding the practical convenience of using FRTs. In addition, the authorities that should authorise the use of FRTs (and LEAs as well) lack a tool similar to the DPIA to help them assess the risks and countermeasures to be taken in specific situations. Therefore, the AI Act should not miss the opportunity to introduce impact assessments that would require users to identify and assess the impact of AI systems on fundamental rights, as well as on society and democratic values (EDRI, 2021, p. 35).

The second set of problems relates to what *the AI Act does not regulate*, or does not regulate adequately. Primarily, the ban *does not cover* all possible uses of FRTs by LEAs, including some that are not considered in this analysis, even when there is a serious threat to rights and freedoms (Christakis et al., 2021). This may be seen in the case of "ex post" use, or use to detect a person's emotional state, or to assess their personality traits and characteristics, or to profile individuals for the purpose of detecting, investigating or prosecuting criminal offences. AI systems used for

such purposes are considered "high risk" (Article 6(3) and Annex III draft AI Act). There is legitimate concern as to whether these cases should also be prohibited or further restricted, as the proposal potentially leaves room for a disproportionate use of FRTs. In particular, it has been questioned whether "ex post" use – where the biometric data have already been captured, and the comparison and identification occur only "after a significant delay" (Recital 8 draft AI Act) – can actually be considered less dangerous than "real time" use (Schröder, 2022). The distinction is justified by the fact that "ex post" use is "likely to have a minor impact on fundamental rights" compared to "real time" use "which may be used for the processing of the biometric data of a large number of persons" (Recital 8). However, we cannot exclude the possibility that the former would not be less intrusive than the latter, since the intrusiveness does not necessarily depend on the length of time within which the biometric data is processed, and a mass identification system is able to identify thousands of individuals in only a few hours (EDPB & EDPS, 2021, §31). Nevertheless, it is worth noting that the French Conseil d'Etat recently ruled that the "ex post" use of FRTs meets the requirements of "absolute necessity" set by the LED and French data protection law solely because it allows for police officers to be able to effectively compare images to identify suspects and support criminal investigations with a high degree of reliability (Christakis & Lodie, 2022).

In addition, biometric categorisation systems and emotion recognition systems *are not necessarily regarded as high-risk*, even when used by LEAs (Article 52). But categorising people based on their physical characteristics, such as visible gender, race or age, opens the door for serious risks of discrimination against minorities such as those with religious, racial or LGBTQI+ identities. Moreover, the claim of being able to read emotions from the images of human bodies is far from being scientifically and objectively corroborated. Studies show that the way people communicate apparently clear emotions varies considerably between cultures, situations and even between individuals in different circumstances. At the same time, similar configurations of facial expressions may express one or more complex emotions (Barrett et al., 2019). So, these uses may also be disproportionate and deserve to be banned or severely restricted.

The third set of problems relates to the aforementioned provisions of the AI Act and their *relationship with the existing data protection legislation*. Some aspects of the LED and the AI Act, such as the definition of biometric data, are expressly related (Recital 7 draft AI Act). In other parts, by contrast, the two are not related and the rules of the AI Act regarding the "real time" use of FRTs by LEAs apply as a *lex specialis* in relation to the LED (Recital 23 draft AI Act). Thus, the former should

prevail over the latter. However, we need to assess whether the new Proposal might lead to a backward step in the protection of rights compared to the existing data protection law. In any event, the EDPB and the EDPS have also stressed that it is crucial to ensure clarity concerning the relationship between the Proposal and existing legislation (EDPB & EDPS, 2021, §15).

In some parts, the Proposal *does not overlap* with data protection regulation, as in the case of the purpose limitation and data minimisation principles, or the storage limitation principle. Here the latter should continue to apply. In other parts, however, there is an *overlap,* and it is necessary to determine which regulation should apply. We can find an example of overlap and a *backward step* in the protection of fundamental rights in the case of information. The AI Act also requires the provision of information as a form of transparency (Veale & Borgesius, 2021, p. 13). However, unlike data protection regulation, the information will not be given directly to people, but only recorded in a public database (Article 60 Proposal AI Act). Furthermore, as stated by the EDPB & EDPS, the transparency obligation does not apply to AI systems used for law enforcement and it is too broad of an exception: a "distinction must be made between AI systems that are used to detect or prevent and AI systems that aim to investigate or help the prosecution of criminal offenses. Safeguards for prevention and detection have to be stronger because of the presumption of innocence" (EDPB & EDPS 2021, §70). Therefore, the proportionality test must take into account people's lower awareness of the use of FRTs in order to determine whether these instruments are the least restrictive measure, and to weigh the costs against the benefits.

On the other hand, an important *step forward* compared to the existing regulations appears to have been made in the case of data quality and bias. The Proposal recognises that the technical inaccuracies of FRTs "can lead to biased results and entail discriminatory effects" (Recital 33). Consequently, training, validation and testing data sets should be subject to "appropriate data governance and management practices", to ensure that they are "relevant, representative, free of errors and complete" (Article 10(3)). Datasets will consider the "specific geographical, behavioural or functional setting" within which FRTs will be used (Article 10(4)). Bias monitoring, detection and correction will be separate justifications for the processing of sensitive categories of personal data as part of the quality standards for high-risk AI systems (Article 10(5)). Unlike the generic provisions of the LED, the requirements set forth by the Proposal are more precise and aimed at preventing market placement of non-compliant FRTs. They call for pluralistic training datasets and watchlists. Moreover, the data processed by FRTs should be chosen in relation

to the concrete use of the system.[9] However, we should not forget that the enforcement of the new rules is left up to providers, leaving too much discretion to providers in the assessment of "adequacy" (Smuha et al., 2021, p. 24). Furthermore, it is wishful thinking to believe that datasets can be "complete" and "free of errors", especially in the case of systems that are already in place, also given the high costs of correcting datasets or building new ones (Hacker, 2018, p. 1150). Again, particular care must be taken to identify the actual costs and benefits of using FRTs.

Conclusion

FRTs are biometric means that enhance the surveillance powers of LEAs. The debate on whether these technologies should be banned in whole or in part is very heated, especially following discussion on the proposed AI Act. Using the conceptual tools of constitutional law, this paper seeks to contribute insights regarding the legal question of whether a ban is an inevitable solution. We argue that it is possible to regulate FRTs in a way that balances the benefits of this surveillance power with the protection of fundamental rights, the preservation of the democratic order and the rule of law. Our analysis has focused on the 'real-time' use of FRTs, one of the most worrying applications of these biometric technologies. We have offered a taxonomy of the most widespread uses of FRTs, distinguishing between different purposes, targeted people and contexts. For each of these, a number of variables have been made explicit which, in ascending order, increase the level of concern for different reasons. On the ethical side, the deployment of FRTs may lead to the undermining of various human values, which can be essentially related to dignity. On the technical side, the risk of inaccuracy increases due to many factors, mainly related to image quality. On the social side, public opinion shows widespread disagreement with the use of these technologies by LEAs. Finally, in terms of the protection of fundamental rights, we are dealing with technologies that can simultaneously restrict a number of rights, either directly or through chilling effects. In consideration of these dangers, the analysis has focused on the legal conditions under which LEAs are allowed to use FRTs. The answer lies in the requirements set by the CFREU and ECHR, as detailed by the CJEU and the ECtHR, in terms of legal basis and proportionality between the objectives pursued and the sacrifice of fundamental rights. The proportionality test thus established must therefore be read in conjunction with data protection legislation, which seeks to set the conditions for the proportionate use of FRTs. Data protection regulation

9. In addition, the AI Act also guarantees human supervision, as the intervention of two natural persons is required to confirm any match based on facial recognition (Article 14(5)).

confirms that without clear rules laying down strict conditions or safeguards (as in the case of biometric data) and addressing the practical convenience of using these technologies (as in the case of the limitation and minimisation principles), the use of FRTs by LEAs is unlikely to pass the proportionality test. Accordingly, there is a need for legislation that supports the proportionality assessment (as in the case of maximum data retention periods), without leaving too much discretion to the Member States (as in the case of the right to information and other related rights), but rather requiring them to consider and weigh all the relevant factors (as in the case of bias). With these considerations in mind, it has been possible to express an opinion on the recently proposed AI Act, which, not surprisingly, includes among the prohibited AI practices the precise use by LEAs of 'real-time' remote biometric identification systems, such as FRTs, in publicly accessible spaces. Despite the advances in terms of regulation that explicitly address these technologies, the proposal reveals several problematic aspects. One of the most important is the excessive reference to national legislation, which leaves too much room for manoeuvre in the regulation of these technologies, opening up the possibility of disproportionate use. The AI Act also fails to regulate with due care all possible uses of FRTs by LEAs, leaving the door open to possible uses that could prove equally dangerous to fundamental rights. Finally, the draft shows little connection with existing data protection legislation, and while in some respects it appears to enhance the protection of rights, in others it seems to set it back. Thus, the European legislator's decision to regulate these technologies without banning them outright appears to be the right one in the abstract, but the concrete conditions imposed suggest that perhaps the time is not yet ripe to put this surveillance power fully in the hands of LEAs.

References

All internet sources were last accessed on 20 January 2023.

Ahmad, W., & Dethy, E. (2019). Preventing surveillance cities: Developing a set of fundamental privacy provisions. *Journal of Science Policy & Governance*, *15*(1), 1–11. http://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/ahmad_dethy_jspg_v15.pdf

AI Now Institute. (2019). *AI Now Report 2019* [Report]. AI Now Institute. https://ainowinstitute.org/AI_Now_2019_Report.pdf

Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, *2*(3), 377–387. https://doi.org/10.1007/s43681-021-00077-w

Article 29 Data Protection Working Party. (2012). *Opinion 02/2012 on facial recognition in online and mobile services* [WP 192]. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

Article 29 Data Protection Working Party. (2015). *Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data* (WP 233). https://ec.europa.eu/newsroom/article29/items/640460/en

Article 29 Data Protection Working Party. (2017). *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680* (WP 258). https://ec.europa.eu/newsroom/article29/items/610178

Artyushina, A., & Wernick, A. (2021, November 8). Smart city in a post-pandemic world: Small-scale, green, and over-policed. *Spacing*. https://spacing.ca/toronto/2021/11/08/smart-city-tech-post-pandemic-small-scale-green-over-policed/

Barak, A. (2012). *Proportionality: Constitutional rights and their limitations*. Cambridge University Press. https://doi.org/10.1017/CBO9781139035293

Barcoas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, *104*(3), 671–732. https://doi.org/10.15779/Z38BG31

Barrett, L. F., Adolphs, R., Marsella, S., Martinez, A. M., & Pollak, S. D. (2019). Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements. *Psychological Science in the Public Interest*, *20*(1), 1–68. https://doi.org/10.1177/1529100619832930

Berle, I. (2020). *Face recognition technology: Compulsory visibility and its impact on privacy and the confidentiality of personal identifiable images* (Vol. 41). Springer International Publishing. https://doi.org/10.1007/978-3-030-36887-6

Borgesius, F. Z. (2018). *Discrimination, artificial intelligence, and algorithmic decision-making* [Study]. Council of Europe. https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73

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

Brewczyńska, M. (2022). A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation. In E. Kosta, R. Leenes, & I. Kamara (Eds.), *Research handbook on EU data protection law* (pp. 91–114). Edward Elgar.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, *81*, 77–91. http://proceedings.mlr.press/v81/buolamwini18a.html

Buolamwini, J., Ordóñez, V., Morgenstern, J., & Learned-Miller, E. (2020). *Facial recognition technologies in the wild: A primer* [Report]. Algorithmic Justice League. https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf

Byrne-Haber, S. (2019, July 11). *Disability and AI-bias* [Medium post]. https://sheribyrnehaber.medium.com/disability-and-ai-bias-cced271bd533

Case of Shimovolos v. Russia, Application no. 30194/09 (European Court of Human Rights 21 June 2011). https://hudoc.echr.coe.int/fre?i=001-105217

Castelluccia, C., & Le Métayer Inria, D. (2020). *Impact analysis of facial recognition: Towards a rigorous methodology* (hal-02480647). HAL Inria. https://hal.inria.fr/hal-02480647/document

Chan, G. K. Y. (2022). Towards a calibrated trust-based approach to the use of facial recognition technology. *International Journal of Law and Information Technology*, *29*(4), 305–331. https://doi.org/10.1093/ijlit/eaab011

Christakis, T. (2020, March 3). *EU citizens reluctant to share their biometric data with public authorities finds FRA, Ai-Regulation.Com*. AI-Regulation.Com. https://ai-regulation.com/eu-citizens-reluctant-to-share-their-biometric-data-with-public-authorities-finds-fra/

Christakis, T., Becuywe, M., & AI-Regulation Team. (2021). *Facial recognition in the draft European AI Regulation: Final report on the high-level workshop held on April 26, 2021* [Report]. AI-Regulation.com. https://ai-regulation.com/facial-recognition-in-the-draft-european-ai-regulation-final-report-on-the-high-level-workshop-held-on-april-26-2021/

Christakis, T., & Lodie, A. (forthcoming). The French Supreme Administrative Court finds the use of facial recognition by law enforcement agencies to support criminal investigations 'strictly necessary' and proportional. *European Review of Digital Administration & Law*.

Consultative Committee of the Convention 108. (2019). *Guidelines on artificial intelligence and data protection* (T-PD(2019)01). Council of Europe, Directorate General of Human Rights and Rule of Law. https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

Consultative Committee of the Convention 108. (2021). *Guidelines on facial recognition* (T-PD(2020)03rev4). Council of Europe, Directorate General of Human Rights and Rule of Law. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

Cook, C. M., Howard, J. J., Sirotin, Y. B., Tipton, J. L., & Vemury, A. R. (2019). Demographic effects in facial recognition and their dependence on image acquisition: An evaluation of eleven commercial systems. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *1*(1), 32–41. https://doi.org/10.1109/TBIOM.2019.2897801

Council of the European Union. (2022). *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—General approach*. https://artificialintelligenceact.eu/wp-content/uploads/2022/12/AIA-%E2%80%93-CZ-%E2%80%93-General-Approach-25-Nov-22.pdf

Crawford, K., & Paglen, T. (2021). Excavating AI: The politics of images in machine learning training sets. *AI & SOCIETY*. https://doi.org/10.1007/s00146-021-01162-8

Dalla Corte, L. (2022). On proportionality in the data protection jurisprudence of the CJEU. *International Data Privacy Law*, *12*(4), 259–275. https://doi.org/10.1093/idpl/ipac014

Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18 (Court of Justice of the European Union 16 July 2020). https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1666781

de Búrca, G. (1993). The principle of proportionality and its application in EC law. *Yearbook of European Law*, *13*(1), 105–150. https://doi.org/10.1093/yel/13.1.105

De Gregorio, G. (2022). *Digital constitutionalism in Europe. Reframing rights and powers in the algorithmic society*. Cambridge University Press. https://doi.org/10.1017/9781009071215

De Gregorio, G., & Dunn, P. (2022). The European risk-based approaches: Connecting constitutional

dots in the digital age. *Common Market Law Review*, *59*(2), 473–500. https://doi.org/10.54648/COLA2022032

Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation. *Computer Law & Security Review*, *35*(6), 105342. https://doi.org/10.1016/j.clsr.2019.105342

Donahoe, E., & Metzger, M. (2019). Artificial intelligence and human rights. *Journal of Democracy*, *30*(2), 115–126. https://doi.org/10.1353/jod.2019.0029

Erratum to papers published in Information Polity – Volume 27, issue 2. (2022). *Information Polity*, *27*(3), 417–418. https://doi.org/10.3233/IP-229012

European Data Protection Board. (2020). *Guidelines 3/2019 on processing of personal data through video devices* (Guidelines 3/2019 Version 2.0). European Data Protection Board. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

European Data Protection Board. (2022). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement* (Guidelines 05/2022 Version 1.0). European Data Protection Board. https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf

European Data Protection Board (EDPB) & European Data Protection Supervisor (EDPS). (2021). *EDPB-EDPS 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)*. https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

European Data Protection Supervisor. (2017). *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*. https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf

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*. https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

European Digital Rights. (2021). *European Commission adoption consultation: Artificial Intelligence Act*. European Digital Rights, EDRi. https://edri.org/wp-content/uploads/2021/08/European-Digital-Rights-EDRi-submission-to-European-Commission-adoption-consultation-on-the-Artificial-Intelligence-Act-August-2021.pdf

European Union Agency for Fundamental Rights. (2020). *Facial recognition technology: Fundamental rights considerations in the context of law enforcement* (FRA Focus) [Focus paper]. European Union Agency for Fundamental Rights; Publications Office of the European Union. https://doi.org/10.2811/524628

European Union Agency for Fundamental Rights (FRA). (2022). *Bias in algorithms – Artificial intelligence and discrimination* [Report]. European Union Agency for Fundamental Rights; Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/c5bdd489-7cf4-11ed-9887-01aa75ed71a1

Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race and the future of law enforcement*. New York University Press.

Floridi, L. (2021). The European legislation on AI: A brief analysis of its philosophical approach. *Philosophy & Technology*, *34*(2), 215–222. https://doi.org/10.1007/s13347-021-00460-9

Friedman, B., & Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions on Information Systems*, *14*(3), 330–347. https://doi.org/10.1145/230538.230561

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

Garante per la protezione dei dati personali. (2021). *Parere sul sistema Sari Real Time* (doc. web). Italian data protection authority. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575877

Gates, K. A. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance*. NYU Press. https://doi.org/10.18574/nyu/9780814732090.001.0001

Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, *34*(2), 279–288. https://doi.org/10.1016/j.clsr.2017.12.003

Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face recognition vendor test part 3: Demographic effects* (NIST IR 8280; p. NIST IR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

Guinchard, A. (2018). Taking proportionality seriously: The use of contextual integrity for a more informed and transparent analysis in EU data protection law. *European Law Journal*, *24*(6), 434–457. https://doi.org/10.1111/eulj.12273

Hacker, P. (2018). Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law. *Common Market Law Review*, *55*(4), 1143–1185. https://doi.org/10.54648/COLA2018095

Hamburg DPA. (2018). *Anordnung "Einsatz der Gesichtserkennungssoftware „Videmo 360" durch die Polizei Hamburg zur Aufklärung von Straftaten im Zusammenhang mit dem in Hamburg stattgefundenen G20-Gipfel"*. https://datenschutz-hamburg.de/assets/pdf/Anordnung_HmbBfDI_2018-12-18.pdf

Heilweil, R. (2020, June 11). Big tech companies back away from selling facial recognition technology to police. That's progress. *Vox*. https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

Information Commissioner's Office. (2019). *ICO investigation into how the police use facial recognition technology in public places* [Report]. Information Commissioner's Office. https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

Janssen, H., Seng Ah Lee, M., & Singh, J. (2022). Practical fundamental rights impact assessments. *International Journal of Law and Information Technology*, *30*(2), 200–232. https://doi.org/10.1093/ijlit/eaac018

Jasserand, C. A. (2015). Avoiding terminological confusion between the notions of 'biometrics' and 'biometric data': An investigation into the meanings of the terms from a European data protection and a scientific perspective. *International Data Privacy Law*, ipv020. https://doi.org/10.1093/idpl/ipv020

Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB (C-203/15) v Post- och telestyrelsen, and Secretary of State for the Home Department (C 698/15) v Tom Watson, Peter Brice, Geoffrey Lewis (Tele2 Sverige AB), ECLI:EU:C:2016:970 (Court of Justice of the European Union 21 December 2016). https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1663267

Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (Digital Rights Ireland), ECLI:EU:C:2020:791 (Court of Justice of the European Union 6 October 2020). https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:62012CJ0293

Joined Cases C-511/18 and C-512/18, La Quadrature du Net (C-511/18 and C-512/18) v Premier ministre, and Ordre des barreaux francophones et germanophone v Conseil des ministres (La Quadrature du Net), ECLI:EU:C:2020:791 (Court of Justice of the European Union 6 October 2020). https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1659829

Kindt, E. J. (2018). Having yes, using no? About the new legal regime for biometric data. *Computer Law & Security Review*, *34*(3), 523–538. https://doi.org/10.1016/j.clsr.2017.11.004

Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2016). Accountable algorithms. *University of Pennsylvania Law Review*, *165*, 633–705.

Leslie, David. (2020). *Understanding bias in facial recognition technologies*. Zenodo. https://doi.org/10.5281/ZENODO.4050457

Bridges, R (On Application of) v The Chief Constable of South Wales Police, [2019] EWHC 2341 (Admin). Case No: CO/4085/2018 (England and Wales High Court (Administrative Court) 4 September 2019). https://www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html

Maximillian Schrems v Data Protection Commissioner, C-362/14 (Court of Justice of the European Union 6 October 2015). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62014CJ0362&from=IT

Mayer-Schönberger, V., & Padova, Y. (2016). Regime change? *Science and Technology Law Review*, *17*(2). https://doi.org/10.7916/STLR.V17I2.4007

Menéndez González, N. (2021). Development or dystopia? An introduction to the accountability challenges of data processing by facial recognition technology. *Communications Law*, *26*(2), 81–96. https://www.bloomsburyprofessional.com/journal/communications-law-17467616/

Merler, M., Ratha, N., Feris, R. S., & Smith, J. R. (2019). *Diversity in faces* (arXiv:1901.10436). arXiv. http://arxiv.org/abs/1901.10436

Mobilio, G. (2021). *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*. Editoriale Scientifica.

Raab, T. (2019). Germany, Video surveillance and face recognition: Current developments. *European Data Protection Law Review*, *5*(4), 544–547. https://doi.org/10.21552/edpl/2019/4/14

Raposo, V. L. (2022a). Ex machina: Preliminary critical assessment of the European Draft Act on artificial intelligence. *International Journal of Law and Information Technology*, *30*(1), 88–109. https://doi.org/10.1093/ijlit/eaac007

Raposo, V. L. (2022b). The use of facial recognition technology by law enforcement in Europe: A non-Orwellian draft proposal. *European Journal on Criminal Policy and Research*. https://doi.org/10.1007/s10610-022-09512-y

Rezende, I. N. (2020). Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective. *New Journal of European Criminal Law*, *11*(3), 375–389. https://doi.org/10.1177/2032284420948161

Schröder, A. (2022, October 14). Real-time' versus 'post' remote biometric identification systems under the AI Act. *ALTI Forum*. https://alti.amsterdam/schroder-biometric/

Simoncini, A., & Longo, E. (2021). Fundamental rights and the rule of law in the algorithmic society. In H.-W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, & G. D. Gregorio (Eds.), *Constitutional challenges in the algorithmic society* (pp. 27–41). Cambridge University Press. https://doi.org/10.1017/9781108914857.003

Smuha, N. A., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., & Yeung, K. (2021). How the EU can achieve legally trustworthy AI: A response to the European Commission's Proposal for an Artificial Intelligence Act. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3899991

Spivack, J., & Garvie, C. (2020). A taxonomy of legislative approaches to face recognition in the United States. In A. Kak (Ed.), *Regulating biometrics: Global approaches and urgent questions* (pp. 86–95). AI Now Institute. https://ainowinstitute.org/regulatingbiometrics-spivack-garvie.pdf

Bridges, R (On the Application Of) v South Wales Police, [2020] EWCA Civ 1058. Case No: C1/2019/2670 (England and Wales Court of Appeal (Civil Division) 11 August 2020). https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html

Tridimas, T. (2018). The principle of proportionality. In R. Schütze & T. Tridimas (Eds.), *Oxford Principles of European Union Law: The European Union Legal Order* (Vol. 1, pp. 243–264). Oxford University Press. https://doi.org/10.1093/oso/9780199533770.003.0010

Urquhart, L., & Miranda, D. (2022). Policing faces: The present and future of intelligent facial surveillance. *Information & Communications Technology Law*, *31*(2), 194–219. https://doi.org/10.1080/13600834.2021.1994220

van der Ploeg, I. (2005). *Biometric identification technologies: Ethical implications of the informatization of the body* (Policy Paper No. 1; BITE). Biometric Technology & Ethics. https://www.academia.edu/6039558/Biometric_Identification_Technologies_Ethical_Implications_of_the_Informatization_of_the_Body

Van Natta, M., Chen, P., Herbek, S., Jain, R., Kastelic, N., Katz, E., Struble, M., Vanam, V., & Vattikonda, N. (2020). The rise and regulation of thermal facial recognition technology during the covid-19 pandemic. *Journal of Law and the Biosciences*, *7*(1), lsaa038. https://doi.org/10.1093/jlb/lsaa038

Veale, M., & Binns, R. (2017). Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. *Big Data & Society*, *4*(2), 205395171774353. https://doi.org/10.1177/2053951717743530

Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, *22*(4), 97–112. https://doi.org/10.9785/cri-2021-220402

Vermeule, A. (2014). *The constitution of risk*. Cambridge University Press. https://doi.org/10.1017/CBO9781107338906

Williams, D. (2020). Fitting the description: Historical and sociotechnical elements of facial recognition and anti-black surveillance. *Journal of Responsible Innovation*, *7*(1), 74–83.

Yeung, K., & Bygrave, L. A. (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance*, *16*(1), 137–155. https://doi.org/10.1111/rego.12401

Zalnieriute, M. (2021). Burning bridges: The automated facial recognition technology and public

space surveillance in the modern state. *Science and Technology Law Review*, *22*(2), 284–307. https://doi.org/10.52214/stlr.v22i2.8666

Published by

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

in cooperation with

UNIVERSITY OF TARTU
Johan Skytte Institute of
Political Studies