Regulating facial recognition in the EU

INNOVATIVE TECHNOLOGIES
Lorem ibsum dolor on ibsum dolorlorem and ipsum dolor ipsumlorem dolor

IN-DEPTH ANALYSIS

EPRS | European Parliamentary Research Service

Authors: Tambiama Madiega and Hendrik Mildebrath
Members' Research Service

PE 698.021 – September 2021

EN

Artificial intelligence has powered the use of biometric technologies, including facial recognition applications, which are increasingly used for verification, identification and categorisation purposes. This paper: (1) provides an overview of the technologies, economics and different uses of facial recognition technologies; (2) highlights concerns arising from the technology's specific characteristics and from its potential impacts on people's fundamental rights; (3) takes stock of the legal framework, especially the data protection and non-discrimination rules currently applicable to facial recognition in the European Union (EU); and (4) examines the recent proposal for an EU artificial intelligence act, regulating facial recognition technologies. Finally, (5) the paper briefly looks at the approaches taken to facial recognition regulation outside the EU and at an international level.

AUTHOR(S)

Tambiama Madiega and Hendrik Mildebrath, Members' Research Service, EPRS (with research support from Fabiana Fracanzino)

This paper has been drawn up by the Members' Research Service, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

To contact the authors, please email: eprs@ep.europa.eu

LINGUISTIC VERSIONS

Original: EN

Translations: DE, FR

Manuscript completed in September 2021.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Photo credits: © LuckyStep / Adobe Stock.

PE 698.021
ISBN: 978-92-846-8503-5
DOI:10.2861/140928
QA-01-21-197-EN-N

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

Executive summary

Artificial intelligence (AI) powers the use of biometric technologies, including facial recognition applications, which are used for verification, identification and categorisation purposes by private or public actors. While facial recognition markets are poised to grow substantially in the coming years, the increasing use of facial recognition technologies (FRTs) has emerged as a salient issue in the worldwide public debate on biometric surveillance.

While there are real benefits to using facial recognition systems for public safety and security, their pervasiveness and intrusiveness, as well as their susceptibility to error, give rise to a number of fundamental rights concerns with regard, for instance, to discrimination against certain segments of the population and violations of the right to data protection and privacy. To address such effects, the EU has already put strict rules in place under the Charter of Fundamental Rights, the General Data Protection Regulation, the Law Enforcement Directive and the EU framework on non-discrimination, which also apply to FRT-related processes and activities. However, various actors question the effectiveness of the current EU framework in adequately addressing the FRT-induced fundamental rights concerns. Even if courts attempted to close gaps in protection through an extensive interpretation of the pre-existing legal framework, legal uncertainties and complexities would remain.

Against this backdrop, the draft EU artificial intelligence (AI) act, unveiled in April 2021, aims to limit the use of biometric identification systems including facial recognition that could lead to ubiquitous surveillance. In addition to the existing applicable legislation (e.g. data protection and non-discrimination), the draft AI act proposes to introduce new rules governing the use of FRTs in the EU and to differentiate them according to their 'high-risk' or 'low-risk' usage characteristics. A large number of FRTs would be considered 'high risk' systems which would be prohibited or need to comply with strict requirements. The use of real-time facial recognition systems in publicly accessible spaces for the purpose of law enforcement would be prohibited, unless Member States choose to authorise them for important public security reasons, and the appropriate judicial or administrative authorisations are granted. A wide range of facial recognition technologies used for purposes other than law enforcement (e.g. border control, market places, public transport and even schools) could be permitted subject to a conformity assessment and compliance with some safety requirements before entering the EU market. Conversely, facial recognition systems used for categorisation purposes would be considered 'low risk' systems and only subject to limited transparency and information requirements. While stakeholders, researchers and regulators seem to agree on a need for regulation, some critics question the proposed distinction between low-risk and high-risk biometric systems, and warn that the proposed legislation would enable a system of standardisation and self-regulation without proper public oversight. They call for amendments to the draft text, including with regard to the Member States' leeway in implementing the new rules. Some strongly support stricter rules – including an outright ban on such technologies.

Looking beyond the EU, there is a global surge in use of facial recognition technologies, whilst concerns about state surveillance are mounting and amplified by the fact that there are, so far, very limited legally binding rules applicable to FRTs even in major jurisdictions such as the United States of America (USA) and China. Policy- and law-makers around the globe have the opportunity to discuss – in a multilateral and possibly in a bilateral context – how to put in place adequate controls on the use of facial recognition systems.

Table of contents

1. Background

1.1. Technologies

1.1.1. Terminology

1.1.1.1. Biometrics

Biometrics technologies are used to identify, verify, or confirm a person's identity based on their physiological (external appearance) or behavioural (how they act) characteristics.[1] **Physiological characteristics** are assessed through morphological identifiers (mainly consisting of fingerprints, the hand's shape, the finger, vein pattern, the eye (iris and retina), and the face's shape) and biological analyses (DNA, blood, saliva, or urine). **Behavioural characteristics** are commonly assessed using voice recognition, signature dynamics (speed of movement of pen, accelerations, pressure exerted, inclination), gait (i.e. individual walking style) or gestures.[2]

Biometrics allows a person to be identified and authenticated based on verifiable unique and specific data. **Biometric identification** consists of determining the identity of a person by capturing an item of their biometric data (e.g. a photograph) and comparing it to the biometric data of several other persons kept in a database, providing an answer to the question 'Who are you?'. **Biometric authentication** compares data on a person's characteristics to their biometric data to determine resemblance and provides an answer to the question 'Are you Mrs or Mr X?'.[3] **Biometric technologies** include 'fingerprint recognition', 'signature recognition', 'DNA matching', 'eyes – iris recognition', 'eyes – retina recognition', 'voice – speaker identification', 'gait', 'hand geometry recognition' or 'face recognition'.[4]

1.1.1.2. Facial recognition

'Facial (or face) recognition' technologies (or FRTs) are a specific type of biometric technologies that refer to a multitude of technologies used for different purposes, ranging from the simple **detection** of the presence of a face in an image, to more complex verification, identification, and categorisation or classification of individuals.[5] **Verification** (one-to-one comparison) enables the comparison of two biometric templates, usually assumed to belong to the same individual. **Identification** (one-to-many comparison) means that the template of a person's facial image is compared to other templates stored in a database to discover if their image is stored there. FRTs are also used to perform a **categorisation** (or classification) of individuals, based on their personal characteristics. In this respect, a wide range of software has been developed to assess the attributes of a person from their face, for the purpose of **'face attribute classification'** (e.g., gender, race, or ethnicity), or for **'face attribute estimation'** (e.g., age). Furthermore, FRTs can be used to **classify facial expressions** (such as a smile), or the emotional state of a person (such as 'happy', 'sad' or 'angry').[6]

[1] See A. Kak, Regulating Biometrics: Global Approaches and Urgent Questions, 2020, p. 6.

[2] See Thales, Biometrics: definition, use cases and latest news, 2021.

[3] Ibid.

[4] See Biometrics Institute, Types of Biometrics, 2021.

[5] See J. Buolamwini, V. Ordóñez, J. Morgenstern, and E. Learned-Miller, Facial Recognition Technologies: A Primer, Algorithmic Justice League, 2020, p. 2-6. See also: European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2020, p. 7-8.

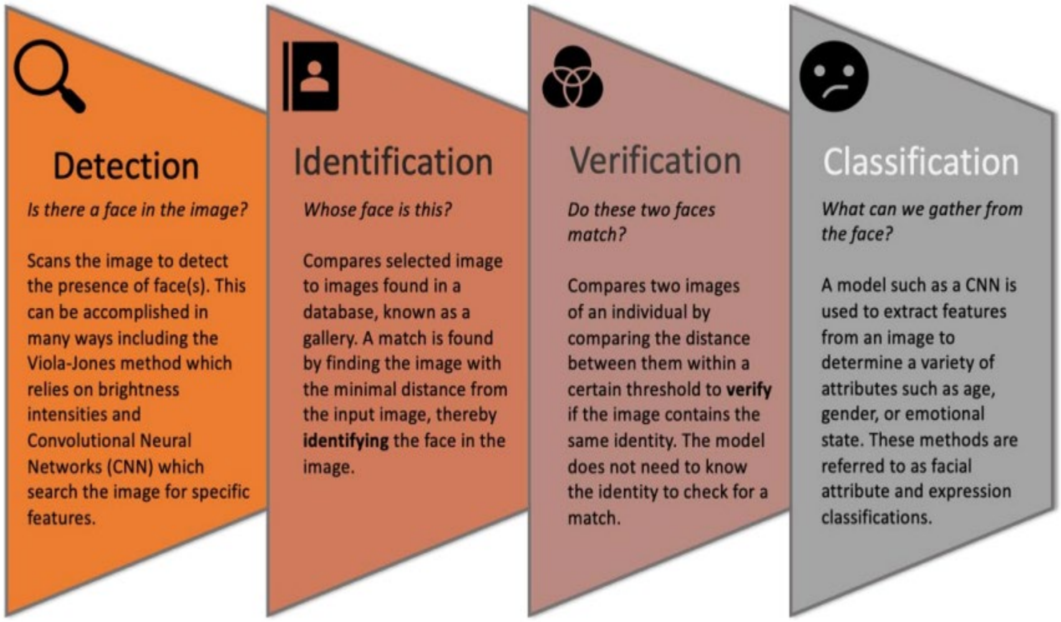
[6] Ibid.

1.1.2. Facial recognition and artificial intelligence technologies

Facial recognition technologies have greatly evolved from their creation in the early 1990s to their early commercialisation powered by the creation of a larger, more substantial datasets in the 2000s and with the integration of deep learning techniques from 2014 onwards.[7]

Today, technologies within the realm of artificial intelligence (AI) such as **machine learning**, including **deep learning** and **computer vision algorithms**, increasingly enable computers to see, collect and process the content of images and videos. Algorithms are routinely trained to learn and extract facial features and properties from large datasets and deep learning is now the dominant approach to facial detection and analysis.[8] Artificial intelligence improves traditional face-recognition systems by allowing, for instance, for faster and more accurate identification (e.g., in cases of poor lighting and obstructed targets). This shift towards **'AI-based' (or 'AI-powered') facial recognition systems** is fostering the emergence of real-world FRT applications.[9] However, at the same time, this 'second wave' biometric technology collects highly sensitive and personal data.[10]

Figure 1 – Facial detection and recognition techniques



Detection

Is there a face in the image?

Scans the image to detect the presence of face(s). This can be accomplished in many ways including the Viola-Jones method which relies on brightness intensities and Convolutional Neural Networks (CNN) which search the image for specific features.

Identification

Whose face is this?

Compares selected image to images found in a database, known as a gallery. A match is found by finding the image with the minimal distance from the input image, thereby **identifying** the face in the image.

Verification

Do these two faces match?

Compares two images of an individual by comparing the distance between them within a certain threshold to **verify** if the image contains the same identity. The model does not need to know the identity to check for a match.

Classification

What can we gather from the face?

A model such as a CNN is used to extract features from an image to determine a variety of attributes such as age, gender, or emotional state. These methods are referred to as facial attribute and expression classifications.

Source: The Alan Turing Institute, 2020.

[7] For an overview of the technological evolution see I. Raji and G. Fried, About Face: A Survey of Facial Recognition Evaluation, 2021.

[8] See D. Leslie, Understanding bias in facial recognition technologies, The Alan Turing Institute, 2020.

[9] See M. Wang and W. Deng, Deep Face Recognition: A Survey, 2020. See also: OECD, Artificial Intelligence in Society, 2019, p. 88.

[10] See European Commission, Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe, 2021, p. 8.

1.2. Usage

Biometric applications are used in everyday private and public life. Facial recognition applications in particular have become very popular among companies, consumers and governments (See Annex 1) and are spreading at a fast rate.[11] Today's uses are diverse and include:

- **Consumer applications**

Information technology (IT) devices such as smartphones, computers or smart doorbells increasingly comprise facial recognition technologies to identify the user. For instance, face verification systems are used to grant access to a computer or a cell phone. Such technologies – used even by children – are increasingly used to **access digital services** such as Snapchat (which is based on computer vision) or Facebook, (which detects human faces present in users' pictures).[12] Car manufacturers are also integrating these technologies to allow drivers to **access cars** and monitor drivers for warning signs of drowsiness or inattentiveness.[13]

- **Business and payment applications**

In the banking sector, facial recognition technologies are decreasing the need for human intervention. Banks are using such systems to authenticate customers' identity as soon as they approach an ATM or open a banking app on a mobile device, as well as to conduct relevant fraud checks.[14] They facilitate **mobile banking** by authenticating users via fingerprint or facial recognition captured by smart phones.[15] Retailers are also integrating face-based payment systems, to assess the demographics of shoppers for marketing purposes or block entry to commercial premises if the system flags a customer as 'suspect'.[16]

- **Surveillance or access control to physical spaces**

Facial recognition technologies that capture people's biometric measurements from a specific distance without interacting with the person are providing vast benefits compared to other biometric security solutions, such as palm prints and fingerprints. For **law enforcement** purposes, facial recognition can help identify a person who has any kind of criminal record or other legal issues.[17] Law enforcement officers can use facial recognition to compare images of suspects in databases in support of investigations. Such FRTs are also already widely used to verify passport identification in airports and ports for **border control** purposes,[18] and could become a key technology in identifying travellers and handling immigration applicants in the future.[19]

[11] See E. Rowe, Regulating Facial Recognition Technology in the Private Sector, *Stanford Technology Law Review*, Vol. 24(1), 2021.

[12] See A. Dirin, J. Suomala and A. Alamäki, AI-based Facial Recognition in Emotional Detection, 2019.

[13] See J. Buolamwini et al., 2020.

[14] See McKinsey, AI-powered decision making for the bank of the future, 2021.

[15] See OECD, 2019, p. 57.

[16] See S. Fourtané, AI Facial Recognition and IP Surveillance for Smart Retail, Banking, and the Enterprise, 2020.

[17] D. Salama AbdELminaam, A deep facial recognition system using computational intelligent algorithms, PLoS ONE, Vol. 15(12), 2020, p. 2.

[18] See C. Dumbrava, Artificial intelligence at EU borders: Overview of applications and key issues, EPRS, European Parliament, July 2021.

[19] See United Kingdom Government, New Plan for Immigration: Legal Migration and Border Control Strategy Statement, 2021. The United Kingdom (UK) plans to install new technologies (including facial biometrics) to ensure that the majority of all arrivals at the main UK ports will pass through some form of contactless corridor or automated gates for identity and security.

In addition, there is a tendency to adopt identification recognition technology in **public spaces**.[20] For instance, public gatherings or protests may be subject to real-time face identification, and entertainment events (e.g. sporting events and concerts) may use face verification for ticketing. Even in the **workplace and education** contexts, facial recognition systems are already deployed. For instance, employers are using face technologies to limit employee access to workspaces and to assess candidates during job interviews, and FRTs are being introduced in schools to take attendance and assess student attentiveness.[21]

Others

There are multiple other applications for FRTs, including for **digital marketing** purposes, in **healthcare** (i.e. patient screening), and in **election organisation** (i.e. e-voting).[22] In addition, in recent years, facial recognition has even become a key technology to enable **sentiment analysis**. Beyond identifying people, new systems are now developed to infer demographic characteristics, emotional states, and personality traits. Such '**emotion recognition technologies**' are increasingly used to analyse facial expressions and other biometric data to track sentimental state and measure human emotion.[23] Emotion recognition has even been framed as a natural next step in the evolution of biometric applications, leading to the integration of emotion recognition in places where facial recognition has already been implemented.[24] Potential uses of such technology cover a wide range of applications, including for customer behaviour analysis and advertising and healthcare (e.g. autism detection).[25] Another remarkable related evolution is the current testing of facial recognition technology to **assess individuals' political orientation.**[26]

1.3. Economics

As facial recognition technologies are quickly entering many aspects of everyday life, the **facial recognition market is poised to grow fast.**[27] Facial recognition is becoming widely used as a key technology for payment authentication. The number of users of software-based facial recognition to secure mobile payments is expected to grow substantially and exceed 1.4 billion globally by 2025, given the relatively low barriers to entry to this market (i.e. need for a front-facing camera and appropriate software), and the implementation of such technology on a large scale by big platforms (e.g. FaceID by Apple).[28] A number of companies are now developing and providing biometric solutions to governments, public authorities and private entities in the fields of civil identity and

[20] See Crawford et al., AI Now Report, 2020, p.11. Public surveillance using facial recognition technology has already been installed in in Hong Kong, Delhi, Detroit and Baltimore.

[21] See J. Buolamwini et al., 2020. See also, Trades Union Congress, Technology managing people - The worker experience, 2021.

[22] See Facial recognition 2020 and beyond – trends and market, i-SCOOP.

[23] See A Dirin et al., 2019. See also Crawford et al., AI Now Report, 2020.

[24] See ARTICLE 19, Emotional Entanglement: China's emotion recognition market and its implications for human rights, London, 2021, p. 18.

[25] See Facial Emotion Recognition, European Data Protection Supervisor website, May 2021.

[26] See M. Kosinski, Facial recognition technology can expose political orientation from naturalistic facial images, *Sci Rep 11*, 100, January 2021.

[27] See i-SCOOP, Facial recognition 2020 and beyond – trends and market, 2020. See also, *Fortune Business Insights*, Facial recognition market, Global Industry Analysis, Insights and Forecast, 2016 2027, 2021. The report found that the global facial recognition market size will grow from US$4.35 billion in 2019 to close to US13.00 billion by 2027.

[28] See Mobile payment authentication: Biometrics, Regulation & forecasts 201-2025, Juniper Research, 2021. See also Press Releases, Facial Recognition for Payments Authentication to Be Used by Over 1.4 Billion People Globally by 2025, Juniper Research, 2021.

public security. They provide services for border checks, public security and law enforcement, including criminal forensics and real-time facial recognition.[29]

As a corollary, investments in face recognition technologies increase as technologies mature. A Stanford study found that, after the autonomous vehicle and health sectors, facial recognition received **the third largest share of global investment devolved to AI** in 2019, with close to US$4.7 billion,.[30] The Covid-19 crisis appears to have accelerated massive investment in facial recognition systems, which are increasingly used in digital healthcare and seen as complementary to other technologies, such as AI, the internet of things (IoT) and 5G.[31]

1.4. Key findings

Significant technological progress has been made in recent years in the field of facial recognition. Artificial intelligence has powered the use of biometric technologies, including facial recognition applications that are increasingly used today to ensure verification and identification of consumers, for business and payment applications and for surveillance by private or public actors. Investment in face recognition technologies is also expected to grow in the coming years, as their usage will surge and diversify and the number of FRT system deployments and experiments is rapidly increasing.

2. Concerns raised by facial recognition

While there are real benefits associated with identity verification in terms of public safety, security and efficiency,[32] the development of facial recognition raises a number of concerns stemming from a combination of the specific characteristics of this technology and from its potential impacts on fundamental rights.

2.1. Technical features and accuracy of facial recognition technology

The fact that facial recognition technology is **pervasive**, while **human control is difficult to implement**, is a primary source of concern. Facial recognition technology records features of the human body that a person cannot change (unlike mobile phone identifiers), a wide number of images are already available (for instance on the internet), and facial images can be captured remotely without a person's knowledge, while an individual's consent is very difficult to obtain when the technology operates in public spaces.[33] In addition, the use of deep learning techniques enables incredibly sensitive information about a very large number of persons to be collected, and makes manual verification and labelling almost impossible, as data sets grow.[34] Furthermore, **security risks**

[29] See, for instance, the services provided by the Thales company.

[30] See Stanford University, The AI Index 2019 Annual Report, 2019.

[31] See i-SCOOP and *Fortune Business Insights*, above.

[32] For an overview of the benefits, see Centre for Data Ethics and Innovation, Facial Recognition Technology, Snapshot Series, p. 21.

[33] See C. Castelluccia and D. Le Métayer Inria, Impact Analysis of Facial Recognition, Centre for Data Ethics and Innovation, 2020, p. 7-8.

[34] K. Haoarchive, This is how we lost control of our faces, *MIT Technology review*, 2021.

posed by the collection and retention of face recognition data, with a risk of breach and misuse of face recognition data, have been highlighted.[35]

Moreover, the **risk of error** has been highlighted. Empirical studies[36] show that the technical performance of most facial recognition systems remains quite limited and that face detection software can make two types of errors. A **false negative** occurs when the FTR software fails to find a face that is present on a picture. A **false positive** occurs when a face detector identifies a non-face structure as a real face.[37] The error rates can be significant particularly when photographs that are compared to one another contain different lighting, shadows, backgrounds, poses, or expressions, when low resolution images are used, and FRT systems are also less accurate when there is large age discrepancies (e.g. between an image of someone in their youth and 10 years later).[38] **Insufficient training data** is another cause of algorithmic bias in facial recognition software.[39] These risks may have very far-reaching consequences for fundamental rights.

Companies withdrawing from the FRT market

The risk of errors has led some companies to decide to withdraw from the FRT market. **Axon**, a leading supplier of police body cameras in the USA decided not to commercialise face-matching technology, given the serious ethical concerns and the technological limitations at stake.[40] Similarly, **Microsoft** and **Amazon** announced moratoria on their production of facial recognition software and services, and **IBM** announced that it will not remain in this business.[41]

2.2. Data protection and privacy concerns

Using facial recognition technologies implies collecting, comparing or storing facial images for identification purposes. The use of AI-powered facial recognition technologies, especially 'second wave' biometrics, deploy more elaborate technologies and algorithms, collecting highly sensitive and personal data.[42] The increasing combination of AI and IoT technologies means that more data, including personal data, are constantly collected and analysed through devices (e.g. surveillance cameras or autonomous vehicles), with the use of improved AI technology (e.g. facial recognition) leading to more invasive outcomes for individual privacy and data protection.[43] Such practices underpin strong concerns regarding the **right to protection of personal data** set out in **Article 8** of the Charter of Fundamental Rights of the European Union (the Charter) and with the **right to private life** under **Article 7** of the Charter (See Section 3 below).[44] Concerns largely relate to the **difficultly to ensure explicit consent** for the use of FRTs. It has been reported that a number of vendors have been scraping publicly available facial images from other websites to build their

[35] See N. Turner Lee, P. Resnick, and G. Barton, Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms, Brookings, 2019. See E. Rowe, 2021, p. 32-34.

[36] See P. Grother et al., Face Recognition Vendor Test (FRVT), 2019.

[37] See J. Buolamwini et al., 2020, p. 3.

[38] See J. Lynch, Face Off: Law Enforcement Use of Face Recognition Technology, Electronic Frontier Foundation, 2020, p. 11-12.

[39] See N. Turner Lee, P. Resnick, and G. Barton, Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms, Brookings, 2019.

[40] See R. Smith, The future of face matching at Axon and AI ethics board report, 2019.

[41] See D. Leslie, 2020, p. 22. See also, R. Smith, The future of face matching at Axon an AI ethics Board report, 2019.

[42] See European Commission, Study supporting the impact assessment of the AI regulation, 2021.

[43] See also, OECD, Artificial Intelligence in Society, 2019, p. 88.

[44] See European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2020.

biometric databases,[45] and even FRT researchers have gradually abandoned asking for people's consent.[46]

2.3. Bias and discrimination concerns

Discrimination refers to a situation when one person is, has been or would be, treated less favourably than another in a comparable situation.[47] Discrimination in algorithmic decision-making can occur during the design, testing and implementation of algorithms used for facial recognition, through bias incorporated in the algorithm itself, or because of the way the results are handed over by the person or authority performing the facial recognition.[48] Facial recognition technology can have very high rates of false positives/false negatives and bias may lead to different types of discrimination against certain categories of populations. **Gender and race biases** have been especially documented, with the accuracy of facial recognition technology varying significantly and being less accurate for women and people of colour than for white men.[49]

Empirical studies show that the risk of discriminatory treatment regarding dark-skinned people/persons of colour is higher in the law enforcement context.[50] The use of training data incorporating sampling bias is a typical issue for numerous facial recognition technologies that perform less well with black people than with white people – and least well with black women. It has been found that, in the USA, the incidence of false-positives disproportionately impacts people of colour and **alters the traditional presumption of innocence** in criminal cases, by placing more of a burden on suspects and defendants to prove they are not who the system identifies them to be.[51] Such outcome interferes with Article 21 of the Charter, which prohibits any discrimination based on grounds such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.[52]

Furthermore, academics have highlighted there are broader implications and moral harms, suffered by people whose lives are directly impacted by the risks of misuse and abuse in using FRTs. There are concerns related to **'distributive injustice'**, e.g. when members of a discriminated-against social group are refused access to benefits, resources or opportunities because of their affiliation with that group. Concerns also relate to **'recognitional injustice',** e.g. when the identity claims of members of a discriminated-against social group are denied or violated in ways that reaffirm and augment their marginalised position.[53]

[45] A. Kak, 'Introduction', in A. Kak, *Regulating Biometrics*, AI now, September 2020, p. 7.

[46] K. Hao, This is how we lost control of our faces, MIT Technology Review, 2021.

[47] See European Union Agency for Fundamental Rights, 2020.

[48] Ibid, p. 27.

[49] See J. Buolamwini and T. Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 2018. See also J. Cavazos et al., Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias?, IEEE Transactions on Biometrics, Behaviour and Identity Science, 2021.

[50] See Amnesty international, Ban dangerous facial recognition technology that amplifies racist policing, 2021. See also L. Hardesty, Study finds gender and skin-type bias in commercial artificial-intelligence systems, MIT News, 2018.

[51] See J. Lynch, Face Off: Law Enforcement Use of Face Recognition Technology, Electronic Frontier Foundation.

[52] See European Union Agency for Fundamental Rights, 2020.

[53] See D. Leslie, 2020, p. 21-25. One example is when an automated system, built with the intended purpose of making an administrative process more efficient, systematically achieves its goals for some privileged social group or groups but does the opposite for marginalised groups (i.e. increases the burden of time and effort needed to complete the same process).

2.4. Mass surveillance and concerns for fundamental rights

Risks related to a possible generalisation of the use of facial recognition technologies have also been pointed out. The possibility of **extending the use of facial recognition systems** beyond their initially authorised and controlled purpose entails some risks in the medium or long-term. Such extensions can take place, for instance, by using data collected on social networks or databases originally set up for different purposes, by using a database beyond its allowed purpose or introducing new functionalities to an existing system (e.g. for example by extending facial recognition used for passport control to payments in an airport and then throughout the whole city).[54] It has been argued that such an extension may constitute part of a deliberate strategy by promoters using facial recognition systems first in contexts where the purpose seems legitimate and then gradually extending their use (i.e. **'slippery slope' argument**).[55]

There is an increasing use of remote biometric identification systems in publicly accessible spaces and face recognition seems to be rapidly becoming the norm in the EU. European Commission investigations show that wherever such a system is in operation, the whereabouts of persons included in the reference database can be followed, thereby impacting their personal data, privacy, autonomy and dignity.[56] Consequently, new social concerns such as the **impossibility of moving in public space anonymously**, or a **conformism** detrimental to free will, could derive from such a mass surveillance system induced by the use of facial recognition systems. In this sense, the Italian Data Protection Authority stated that the automated processing of biometric data for facial recognition could constitute a form of **indiscriminate mass surveillance**.[57]

Furthermore, the use of FRTs raises some concerns with respect to a number of other civil liberties including **religious freedoms**[58] and the **rights of the child** – as vulnerable people deserving a higher standard of protection, especially when used for law enforcement and border management purposes,[59] given the lower accuracy with which the technology detects rapidly-changing young faces.[60] It has also been stressed that using facial recognition technologies to process facial images captured by video cameras in the public space may interfere with a person's **freedom of opinion and expression** and have a negative effect on their **freedom of assembly and of association.**[61] The use of facial recognition technology to identify persons in the context of assemblies has considerable adverse effects on the rights to privacy, freedom of expression and peaceful assembly according to a United Nations Human Rights Council report.[62] Furthermore, the automatic identification and traceability of persons may have strong impact on social and psychological behaviour of citizens and highlight important **ethical questions** raised with the use of such technology[63]. The effect can be even stronger with a risk to see the development of entrench structural racism and threatening of modern democratic forms or life social solidarity because of

[54] See C. Castelluccia and D. Inria, 2020, p. 8-9.

[55] Ibid, p. 17.

[56] See European Commission, Impact assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council, 2021, p. 18.

[57] Mentioned in European Parliament, Question for written answer E-002182/2021.

[58] See E. Rowe, 2021, p. 31.

[59] See European Union Agency for Fundamental Rights, 2020, p. 28-29.

[60] See E. Rowe, 2021, p. 26.

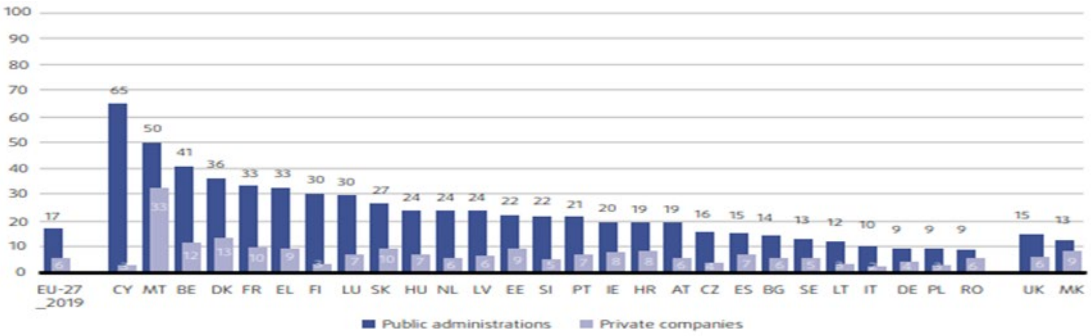
[61] See European Union Agency for Fundamental Rights, 2020, p. 29-30.

[62] See Report of the United Nations High Commissioner for Human Rights, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, 2020.

[63] See High-Level Expert on AI, Ethics guidelines for trustworthy AI, 2019, p. 33.

face surveillance infrastructures.[64] All those concerns translate into a rather cautious approach to facial recognition technology among EU citizens.

Figure 2 – Willingness to share facial images for identity with public authorities and private companies, by country



Source: European Union Agency for Fundamental Rights, Your rights matter: Data protection and privacy, 2020.

Against this backdrop, defining the conditions when AI can be used for automated identification of individuals and differentiating between identification and tracking of an individual and between targeted surveillance and mass surveillance is crucial for setting the right framework (see Section 4 below).[65]

2.5. Key findings

The concerns raised by the development of facial recognition stem from a combination of technical features and the technologies' lack of accuracy, which may lead to serious threats to civil liberties. While there are real benefits to using facial recognition systems in terms of public safety, security and efficiency for identity verification, the risk of algorithmic error is high. Facial recognition technology can have very high rates of false positives and of false negatives and may lead to bias and various types of discrimination against certain populations. A particularly sensitive case is the increasing use of remote biometric identification systems in publicly accessible spaces.

3. Current EU legal framework

3.1. Interplay and functioning of EU multi-level framework

Within the EU legal order, data protection, privacy and non-discrimination rules, as well as the proposed AI regulation, lay down critical parameters for the development and use of facial recognition technology (FRT). The relevant rules are spread over different tiers of the EU legal order. Most notably, the fundamental rights to data protection, privacy and non-discrimination enshrine a set of basic guarantees at the primary level in the Charter of Fundamental Rights (CFR). Although the Charter is addressed to 'EU institutions and to the Member States when implementing Union law' (Article 51(1) CFR), it may also affect relations between private parties ('horizontal effect').[66] Secondary legislation giving effect to fundamental rights and sector-specific regulations, govern the

[64] See D. Leslie, 2020.

[65] See High-Level Expert on AI, 2019, p.33.

[66] See E. Frantziou, The Horizontal Effect of the Charter, *Cambridge Yearbook of European Legal Studies*, Vol 22, 2020.

manufacturing and deployment of emerging technologies in more detail. In this multi-level framework, secondary legislation and its implementation must be consistent with primary law.

3.2. Respect for private life and protection of personal data

Since the use of FRT implies the processing of data for the purpose of identification, its use by public authorities constitutes an interference with the **right to data protection**, as set out in Article 8 CFR and the **right to private life** under Article 7 CFR. More specifically, the initial video-recording, the subsequent retention of the footage, and the comparing of footage with database records for the purpose of identification (matching), all present interferences with or limitations on this right. Any limitation on these fundamental rights must be strictly necessary and proportionate pursuant Article 52(1) CFR.[67]

In practice, however, these fundamental rights are still taking shape[68] and the extent of their application to private relations is not yet settled[69]. In themselves, they hardly provide practical guidance for the use of FRT and often only indirectly contain and resolve conflicts at the interface of data protection and emerging technologies. It is rather their 'expression' in secondary law, which presents a workable framework.[70] Both the **Law Enforcement Directive** (LED) and the **General Data Protection Regulation** (GDPR) apply to automated processing of personal data and to manual processing forming part of a filing system, pursuant to Article 2(1) GDPR and Article 2 LED.[71] However, the LED is a more specific regime than the GDPR (*lex specialis*) and is applicable when public authorities process personal data for the prevention, investigation, detection of prosecution of criminal offences (Recitals 11 and 12 LED and Recital 19 GDPR). Following the main legal principles of data protection (Article 5 GDPR and Article 4 LED), the processing of facial images must be:

- lawful, fair and transparent;
- follow a specific, explicit and legitimate purpose (clearly defined in Member State or Union law);
- comply with the requirements of data minimisation, data accuracy, storage limitation, data security and accountability.

Data controllers (and indirectly manufacturers) should design their intended data processing activities in full respect of the data protection principles ('data protection by design and by default', Article 25 GDPR and Article 20 LED).[72]

[67] As regards data protection, the requirements in Article 8(2) CFR must be fulfilled.

[68] For an introduction, see G. Fuster and H. Hijmans, The EU rights to privacy and personal data protection: 20 years and 10 questions, International Workshop 'Exploring the Privacy and Data Protection connection', 2019.

[69] See Judgement in Case C-131/12, *Google Spain*, CJEU, 13 May 2014.

[70] One commentator goes so far as to say that 'secondary data protection law plays [...] a key role not only for informing the fundamental right to data protection, but also for establishing the conditions and the limitations for its application', see Y. Ivanova, The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World, in D. Hallinan et al., *Data Protection and Privacy*, Vol. 13, 2020, pp. 5-6.

[71] While the LED applies to processing in Schengen Member States, the GDPR applies to processing in the European Economic Area.

[72] See EDPB, Guidelines 3/2019 on processing of personal data through video devices, 2020, p .30; See Council of Europe, Guidelines on Facial Recognition, 2021, p. 15; See EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2020, pp. 17-18.

3.2.1. Lawful, fair and transparent

According to Articles 5(1)(a) GDPR and Article 4(1)(a) LED, as well as Recital 26 LED, any processing of personal data must be lawful, fair and transparent in relation to the natural person concerned.

3.2.1.1. Lawfulness

For processing to be lawful, it must satisfy the requirements of **specific legal bases** (Recital 40 GDPR, Recital 35 LED). Video surveillance may have a legal basis in Article 6 GDPR,[73] or in national transpositions of Article 8 LED, but if it is used to process special categories of data, the processor must (additionally) satisfy the strict requirements under Article 9 GDPR or Article 10 LED.[74] Since FRT usually processes data relating to physical, physiological or behavioural characteristics automatically for the purpose of uniquely identifying a natural person, its use qualifies as processing of biometric data[75] within the meaning of Article 3(13) LED and Article 4(14) GDPR.[76] Consequently, such processing will need to fulfil the strict requirements under Article 9 GDPR and Article 10 LED. Decisions based solely on automated processing may only be taken where the requirements of Article 22(2) and (4) GDPR or Article 11(1) and (2) LED are satisfied. The European Data Protection Board (EDPB) considers that 'the use of video surveillance including biometric recognition functionality installed by private entities for their own purposes (e.g. marketing, statistical, or even security) will, in most cases, require **explicit consent** from all data subjects (Article 9(2)(a) GDPR).'[77] Another legal basis repeatedly brought into play in the FRT context is Article 9(2)(g) GDPR, which permits the processing of personal data based on Union or Member State law if it 'is necessary for reasons of substantial public interest'.[78]

The deployment of biometrics-enabled facial recognition by law enforcement agencies is subject to similar conditions under the LED (Articles 4(1)(a) and 10 LED).[79] Within **law enforcement** contexts, police departments typically invoke criminal procedure codes,[80] or surveillance codes and police laws[81] as their legal bases. Certain trial operations have been based on consent.[82] In a UK case, the

[73] For details, see EDPB Guidelines 3/2019 on processing of personal data through video devices, 2020, pp. 9-14; See also Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, Conference of the German Data Protection Authorities (DSK), 17 July 2020, pp. 7-15.

[74] See EDPB, Guidelines 3/2019 on processing of personal data through video devices, 2020, p. 17. Several commentators consider that Article 9 GDPR overrides Article 6 GDPR, as *lex specialis*, whereas the EDPB assumes their concurrent application.

[75] E. J. Kindt, Having yes, using no? About the new legal regime for biometric data, *Computer Law & Security Review*, Vol. 34(3), 2018.

[76] See EDPB, Guidelines 3/2019 on processing of personal data through video devices, 2020, p. 18-21.

[77] See EDPB, 2020, p. 18. See also Center for Democracy & Technology, CDT response to consultation on EDPB Guidelines 3/2019, 2019, which welcomes this approach. The Centre for Information Policy Leadership (CIPL) suggests that other legal bases should be considered thoroughly (see CIPL response to consultation on EDPB Guidelines 3/2019, 6 September 2019, pp. 10-11). Concerning consent requirements, see EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, 2020. As regards obstacles to consent, see E. Selinger and W. Hartzog, The Inconsentability of Facial Surveillance, *Loyola Law Review*, Vol. 66(1), 2020.

[78] See European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2020, p. 24 and European Data Protection Supervisor, Facial recognition: A solution in search of a problem?, 2019.

[79] See European Union Agency for Fundamental Rights, 2020, p. 24; See Article 29, Working Party Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), 2017, pp. 7-6.

[80] Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg, Hamburg DPA, 31 August 2018, p. 10.

[81] UK Information Commissioner's Office, Opinion on The use of live facial recognition technology by law enforcement in public places, 2019, p. 9.

[82] Bundespolizeipräsidium Potsdam, Abschlussbericht Biometrische Gesichtserkennung, 28 September 2018, pp. 22-23.

Appeals Court overturned a first instance decision, inter alia because the legal framework did not qualify as a legal basis, because it was imprecise and afforded individual police officers too much discretion concerning who could be placed on a watch-list and where FRT could be deployed.[83] In a German case, the Hamburg Data Protection Authority (DPA) considered that indiscriminate video surveillance and subsequent biometric extraction and storage during the 2017 G20 Summit, lacked sufficient legal bases.[84] After the order to delete the police database of biometric templates was overruled by a first instance court judgment, the Hamburg DPA argued at appeal that the lack of a sufficiently determinate legal bases also violated Article 8(2) CFR, Article 4(1)(a) LED and the national transposition thereof.[85] Particular issues also arise where operators scrape public data, or access data collected by third parties, to support their FRT systems.[86]

Box 2 – Principle of proportionality

Both the direct application of the fundamental rights to privacy and data protection[87] as well as a CFR-consistent interpretation of the GDPR and the LED require that data processing related to FRT by EU Institutions and Member States is proportionate.[88] Both the German and UK legal and administrative actions against the deployment of FRT by law enforcement authorities address proportionality concerns. Referring to the CJEU cases *DRI*[89] and *Tele2 Sverige,*[90] the Hamburg Data Protection Authority (DPA) held that the legal basis relied upon by the police, was not sufficiently specific and determinate and thus did not satisfy the requirements of proportionality pursuant Article 8 CFR and the right to informational self-determination under the Basic Law.[91] Even if the legal basis were applicable, the DPA concluded that the practical application of FRT did not satisfy the requirement of strict necessity and proportionality as required by the applicable law.[92] In the UK case, it appears that the Court of Appeals would have considered the deployment of FRT proportionate, had it not been unlawful due to the indeterminate legal bases, the insufficient data protection impact assessment and the failure to assess potential algorithmic discrimination in accordance with the public sector equality duty.[93]

[83] Judgment in Case No. C1/2019/2670, Court of Appeal, 11 August 2020, paras. 90-96.

[84] Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg, Hamburg DPA, 31 August 2018, pp. 9-27.

[85] Antrag auf Zulassung der Berufung §§ 124, 124a VwGO, Hamburg DPA, 13 March 2020, pp. 5-6.

[86] See EDPB, Guidelines 3/2019 on processing of personal data through video devices, 2020, pp. 15-16; EDPB, Response to MEPs inquiry on Clearview AI, 2020; this topic is also broadly discussed among academics.

[87] See European Union Agency for Fundamental Rights, *Handbook Applying the Charter of Fundamental Rights of the EU*, EU Publications Office, 2018, p. 38.

[88] This interpretation is supported by the primacy of Article 7, 8 and 52(1) CFR andthe implicit adherence of the GDRP/LED to the principle of proportionality as reflected by stricter requirements for deeper interferences (see e.g. Articles 6 and 9 GDPR as well as Article 8 and 10 LED) and the principle's fragmented codification throughout the GDPR and LED (e.g. Recital 26, third sentence, LED, Articles 5(1)(c), 6(1)(b)-(f) and 35(7)(b) GDPR, Recital 39, ninth sentence, GDPR). See also the reasoning of the Hamburg DPA in his appeal from 13 March 2020, pp. 5-6 and p. 8. It should be kept in mind that fundamental rights only exceptionally affect relations between private entities; see, however, Judgement in Case C-131/12, *Google Spain*, CJEU, 13 May 2014 and E. Frantziou, The Horizontal Effect of the Charter, *Cambridge Yearbook of European Legal Studies*, Vol 22, 2020.

[89] Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, CJEU, 8 April 2014.

[90] Judgment in Case C-203/15, *Tele2 Sverige*, CJEU, 21 December 2016.

[91] Antrag auf Zulassung der Berufung §§ 124, 124a VwGO, Hamburg DPA, 13 March 2020, p. 8 et seq.

[92] Antrag auf Zulassung der Berufung §§ 124, 124a VwGO, Hamburg DPA, 13 March 2020, pp. 19-20; Order pursuant Sec. 6 HmbRI(EU)2016/680UmsAAG and Sec. 43(1)5 HmbJVollzDSG, Hamburg DPA, 18 December 2018, p. 22.

[93] Judgeent in Case No. C1/2019/2670, Court of Appeal, 11 August 2020, paras. 90-96, 152-153 and 199-202.

3.2.1.2. Transparency

According to the transparency principle (Article 5(1)(a) GDPR), 'it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and **to what extent the personal data are or will be processed**' (Recital 39 GDPR).[94] This does not in itself prevent competent authorities[95] from carrying out activities such as covert investigations or video surveillance (Recital 26 LED). According to Article 13(3) LED, however, Member States may introduce **exceptions**, to avoid obstructing or prejudicing ongoing investigations; or to protect public security and national security. Such exemptions may prove instrumental for law enforcement, since disclosure of FRT to the suspect may undermine their law enforcement efforts. Because this would preclude data subjects from exercising their rights, strong justifications are necessary for the application of such exceptions.[96]

For video surveillance under the GDPR, the European Data Protection Board (EDPB) recommends a two-layered approach in order to comply with transparency requirements.[97] The most important information should be provided through a **warning sign** positioned in a way that the (intended) 'data subject can easily recognise the circumstances of the surveillance before entering the monitored area'. Further mandatory details may be provided by other easily accessible means (e.g. poster and website), which are clearly referred to on the first layer (e.g. QR code or website address). Similarly, the Council of Europe adopts a layered approach in its guidelines to facial recognition.[98] Additionally, regulators, stakeholders and academics are discussing to what extent an individual has a **right to an explanation** of the decision reached after algorithmic assessment, including 'meaningful information about the logic involved' (Articles 13-15 and 22 GDPR and Recital 71 GDPR and Articles 11, 13 and 14 LED and Recital 38 LED).[99] This right may well apply to automated decisions based on FRT, but its implementation remains uncertain.

3.2.1.3. Fairness

The European Data Protection Board held in recent guidelines that 'fairness is an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject'.[100] The principle is subject to ambiguity and some commentators consider it **a catch-all principle**, which may be leveraged in cases where processing would otherwise be permissible, but appears unfair in the case in point.[101] Academics suggest 'that fairness is a corrective tool for rebalancing asymmetric or unbalanced relationships (i.e. situations of induced vulnerabilities) between controllers and

[94] For more information, see Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679, 2016 (endorsed by the EDPB).

[95] Article 3(7) LED.

[96] See European Union Agency for Fundamental Rights, 2020, p. 24.

[97] See EDPB, Guidelines 3/2019 on processing of personal data through video devices, 2020, pp. 26-27.

[98] See Council of Europe, Guidelines on Facial Recognition, T-PD(2020)03rev4, 2021, pp. 11-12.

[99] See B. Goodman and S. Flaxman, 'European Union regulations on algorithmic decision-making and a "right to explanation"', *AI Magazine*, Vol. 38(3), 2017; S. Wachter et al., 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', *International Data Privacy Law*, Vol. 7(2), 2017; and various others.

[100] See EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2020, pp. 17-18.

[101] see P. Kramer, 'Artikel 5 DSGVO', in M. Eßer et al., *Auernhammer DSGVO BDSG*, 2020, para 15; T. Herbst, 'Artikel 5 DS-GVO', in J. Kühling and B. Buchner, *DS-GVO BDSG*, 2018, para. 17.

subjects.'[102] While the definition of this principle remains in flux, commentators propose to rein-in algorithmic discrimination by means of its progressive interpretation.[103] Although it is too soon to draw final conclusions on the principle's normative content, it should be kept in mind as a binding leitmotif by developers when designing FRT and by operators when conceiving implementation plans.

As indicated by the Conference of the German Data Protection Authorities (DSK), discriminatory processing may simultaneously violate the requirement of a legitimate purpose (see details on the principle of purpose limitation below).[104] Similarly, one might argue an interference with the principle of lawfulness (see details above), where the fundamental right to non-discrimination is not sufficiently safeguarded (Article 9(2)(g) GDPR).

3.2.2. Specific, explicit and legitimate purpose

The principle of purpose limitation stipulates that personal data may only be processed for a **precisely defined, explicit and legitimate purpose** and that **downstream repurposing**, i.e. the use of data for a purpose that is incompatible with the designated purpose, is only possible under strict conditions (Article 5(1)(b) GDPR and Article 4(1)(b) LED).[105] The intended purpose must be formulated with sufficient precision that the person concerned may be able to envisage the purpose for which their data will be processed.[106] As FRT bears the considerable risk of 'function creep',[107] related systems and processes should include safeguards, such as a compartmentalised architecture, to prevent their use for unauthorised purposes.[108] Even if the intended access were included in the scope of the legitimate purpose, the principle of proportionality (see Box 2) and data security may further restrict access conditions and require safeguards, such as that reasonable suspicion is established, that searching possibilities are limited, and/or that cascading systems (layering of measures, beginning with the least intrusive) are in place.[109]

[102] See G. Malgieri, The concept of fairness in the GDPR, FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, January 2020. Likewise, T. Herbst, 'Artikel 5 DS-GVO', in J. Kühling and B. Buchner, *DS-GVO BDSG*, 2018, para. 17

[103] See P. Hacker, 'Teaching fairness to artificial intelligence', *Common Market Law Review*, Vol 55(4), 2018, pp. 1172-1173; G. Malgieri, The concept of fairness in the GDPR, 2020, , p. 163; CIPL, Report on Artificial Intelligence and Data Protection: Hard Issues and Practical Solutions, February 2020, pp. 6-12.

[104] See Hambacher Erklärung zur Künstlichen Intelligenz, DSK, 3 April 2019, pp. 3-4; For details on the GDPR as an anti-discrimination law and its limits see P. Hacker, 2018, pp. 11701185; See also F. Zuiderveen Borgesius, Discrimination, artificial intelligence and algorithmic decision-making, Council of Europe, 2018, pp. 21-25.

[105] For details, see EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2020, pp. 19-20; See Article 29 Working Party, Opinion 03/2013 on purpose limitation (not endorsed by the EDPB), and European Union Agency for Fundamental Rights, *Handbook on European data protection Law*, 2018, pp. 12–125.

[106] Advocate-General J. Kokott Opinion in Case C-275/06, *Promusicae*, CJEU, 18 July 2007, para. 53

[107] See L. Houwing, 'Stop the Creep of Biometric Surveillance Technology', *European Data Protection Law Review*, Vol 6(2), 2020; For examples of function creep in law enforcement related contexts, see European Union Agency for Fundamental Rights, Under watchful eyes - biometrics, EU IT-systems and fundamental rights, 2018, pp. 61 and 66.

[108] See European Union Agency for Fundamental Rights, Fundamental rights and the interoperability of EU information systems: borders and security, 2017 pp. 21-23. See also EDPB, Guidelines 3/2019 on processing of personal data through video devices, 2020, p. 21; European Union Agency for Fundamental Rights, Under watchful eyes - biometrics, EU IT-systems and fundamental rights, 2018, pp. 59-62 and p. 66.

[109] See European Union Agency for Fundamental Rights, Under watchful eyes - biometrics, EU IT-systems and fundamental rights, 2018, pp. 64-68 with reference to the judgment in Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, CJEU, 8 April 2014, para. 51.

3.2.3. Data minimisation, data accuracy, storage limitation, data security and accountability

The principle of **data minimisation** is generally interpreted to mean that the quantity of data should be limited (GDPR), or not excessive (LED), to what is necessary for the purpose (Article 5(1)c) GDPR and Article 4(1)(c) LED). According to Data Protection Authorities and commentators, this also includes anonymising data where possible.[110] The French Data Protection Authority, for instance, held that deploying a facial recognition-based access control system at schools violated the principles of proportionality and data minimisation, since the objectives of reducing the duration of controls and securing the entrance could have been achieved with less intrusive means, for instance, through a badge system.[111] The European Data Protection Supervisor (EDPS) notes that FRT systems may not comply with the principle of data minimisation.[112]

Both the GDPR and the LED incorporate the principle of **storage limitation**. The principle stipulates that data should not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed (Article 5(1)(e) GDPR and Article 4(1)(e) LED).[113] Several data protection bodies published opinions on storage limitations concerning data from video recordings under the GDPR. For instance, surveillance footage for the purpose of detecting vandalism should be erased, ideally automatically, after a few days. 'The longer the storage period set (especially when beyond 72 hours), the more argumentation for the legitimacy of the purpose and the necessity of storage has to be provided'.[114] In principle, three days, i.e. 72 hours, suffice to clarify whether captured data needs to be stored longer, while excess material can be deleted.[115] Data may be stored for a longer period, if special surveillance purposes apply.[116] According to the European Data Protection Board, 'data controllers must ensure that data extracted from a digital image to build a template will not be excessive and will only contain the information required for the specified purpose, thereby avoiding any possible further processing'.[117] Also, depending on the purpose, once a facial template has been generated, the underlying raw-data may need to be deleted.[118]

The principle of **data accuracy**, requires that the data is factually and temporally accurate (Article 5(1)(d) GDPR and Article 4(1)(d) LED). This implies certain data must be kept up-to-date. 'The

[110] Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, DSK, 17 July 2020, p. 10; See EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2020, pp. 21-23.

[111] Commission nationale de l'informatique et des libertés, Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position, 2019. In its Decision in Case N° 1901249 from 27 February 2020, the Administrative Tribunal of Marseille annulled the decision of the regional council of Provence-Alpes-Côte d'Azur to the extent that it launched the experimentation of the FRT-powered access control system in the 'Ampère' (Marseille) and 'Les Eucalyptus' (Nice) high schools, on the grounds that the intended processing of biometric data was not covered by the exceptions under Article 9(2) GDPR, rendering the regional council's decision illegal (see para. 13).

[112] EDPS, Facial recognition: A solution in search of a problem?, 2019; For details on tensions between emerging technologies and the principle of data minimisation, see A. Roßnagel, 'Artikel 5 DSGVO', in S. Simits et al., *Datenschutzrecht*, Nomos, 2019, paras. 133-135.

[113] The LED requires that Member States prescribe specific time limits for storage and review (Article 5 LED), see Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), Article 29 Working Party (not endorsed by the EDPB), 29 November 2017, pp. 3-6.

[114] EDPB, Guidelines 3/2019 on processing of personal data through video devices, 2020, p. 28.

[115] DSK, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, 2020, pp. 22-23. See also Videoüberwachung auf Bahnhöfen, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit website.

[116] See DSK, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, 2020, pp. 22-23.

[117] See EDPB, Guidelines 3/2019 on processing of personal data through video devices, 2020, p. 21.

[118] Ibid.

assessment of whether personal data is accurate and complete must be made in the light of the purpose for which that data was collected'.[119] Additionally, certain insignificant errors may not affect its accuracy (e.g. a single faulty data point per million in a sequenced genome which may still serve as a biometric identifier).[120] The EU Agency for Fundamental Rights (FRA) considers that 'accuracy is usually interpreted as correctness of personal data for one individual (e.g. is the age of one person in a database correct), though the term accuracy could be interpreted more widely'.[121] According to the Council of Europe's Guidelines on facial recognition, developers 'will have to avoid mislabelling, thereby sufficiently testing their systems and identifying and eliminating disparities in accuracy, notably with regard to demographic variations in skin colour, age and gender, and thus avoid unintended discrimination'.[122] Data controllers or processors would need to check the quality of images and biometric templates inserted in watch-lists to prevent potential false matches, since low quality images can cause an increase in the number of errors.[123] In its Guidelines on automated individual decision-making and profiling, the Article 29 Working Party appears to suggest that, even where inaccurate inferences are drawn from accurate raw data through the use of artificial intelligence, this may violate the principle of data accuracy (which is arguable).[124] Consequently, this principle would not only require accurate input data,[125] but also that algorithms are trained on representative dataset and contain as little hidden bias as possible.[126] This normative aspect remains unsettled and contestable.

According to the **principle of data security**, data must be processed in a manner that ensures appropriate security for personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Article 5(1)(f) GDPR and Article 4(1)(f) LED). Article 32 GDPR and Article 29 LED (indirectly) prescribe that the controller and processor should implement proportionate technical and organisational measures to prevent that personal data is disclosed to, or accessed by, unauthorised persons or organs. The European Data Protection Board suggests that the controller must adequately protect the system and the data throughout all stages of processing, i.e. during storage, transmission, and processing.[127] To this end, the controller shall take the following measures: compartmentalise data during transmission and storage, store biometric templates and raw data or identity data on distinct databases, encrypt biometric data, notably biometric templates, and define a policy for encryption and key management, integrate an organisational and technical measure for fraud detection, associate an integrity code with the data (for example signature or hash) and prohibit any external access to the biometric data. Such measures will need to evolve with

[119] Judgment in Case C434/16, *Nowak*, CJEU, 20 December 2017, para. 53.

[120] D. Hallinan and F. Borgesius, Opinions can be incorrect (in our opinion)! On data protection law's accuracy principle, *International Data Privacy Law*, Vol. 10(1), 2020.

[121] See European Union Agency for Fundamental Rights, Data quality and artificial intelligence - mitigating bias and error to protect fundamental rights, 2019, p. 9.

[122] Council of Europe, Guidelines on Facial Recognition, 2021, p. 9.

[123] Ibid, pp. 12-13. Additionally, 'in case of false matches, the entities will take all reasonable steps to correct future occurrences and ensure the accuracy of digital images and biometric templates'.

[124] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2018.

[125] As regards proper data management, see European Union Agency for Fundamental Rights, Under watchful eyes - biometrics, EU IT-systems and fundamental rights, 2018, pp. 81-97.

[126] On bias, see M. Hildebrandt, The Issue of Bias. The Framing Powers of Ml, in M. Pelillo and T. Scantamburlo, *Machine Learning and Society: Impact, Trust, Transparency*, MIT Press, 2020; #BigData: Discrimination in data-supported decision making, FRA, 30 May 2018.

[127] See EDPB, Guidelines 3/2019 on processing of personal data through video devices, 2020, pp. 28-32; see also Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, DSK, 17 July 2020, p. 21.

the advancement of technologies.[128] The Council of Europe takes a more high-level approach, but specifically mentions the need for 'measures to prevent technology-specific attacks, including presentation attacks and morphing attacks'.[129]

According to the **principle of accountability**, the data controller shall be responsible for demonstrating compliance with the personal data processing principles (Article 5(2) GDPR and Article 4(4) LED).[130] To this end, the controller must implement appropriate technical and organisational measures (Article 24 and Recital 84 GDPR, as well as Article 19 and Recital 53 LED). Where the controller intends to deploy FRT, a **data protection impact assessment**, including prior consultation with the data protection authority, would most likely[131] be required (Articles 35-36 GDPR and Articles 27-28 LED). This should consist of a comprehensive analysis of the legal permissibility and the risks involved in the FRT implementation.[132] Other accountability measures for controllers include the **recording of processing activities** (Article 30 GDPR and Article 24 LED), the **documentation of data breaches** (Article 33(5) GDPR and Article 30(5) LED) and **the implementation of appropriate technical and organisational measures** (Article 24 GDPR and Article 19 LED). These are important tools for accountability, as they help controllers comply with requirements, but also demonstrate that appropriate measures have been taken to ensure compliance.

3.3. Non-discrimination framework

3.3.1. EU anti-discrimination framework

As demonstrated by several studies, discrimination presents a considerable risk-factor associated with the deployment of FRT (see Section 2 above).[133] Since the EU non-discrimination framework largely applies to public and private operators of AI-powered FRT systems, their implications and fitness require examination. In the EU, the right to non-discrimination is enshrined in primary and secondary law and applies to algorithmic decision-making. Discrimination occurs where a person or group is treated less favourably than another, based on certain personal characteristics, or in other words, based on legally 'protected grounds', which may not provide the basis for differential treatment (e.g. sex, race and disability). Discrimination in algorithmic decision-making may arise inter alia from unrepresentative training data, bias in data labelling schemes and flawed/inadequate mathematical functions.[134]

[128] See EDPB, Guidelines 3/2019 on processing of personal data through video devices, 2020, p. 21.

[129] See Council of Europe, Guidelines on Facial Recognition, 2021, p. 13.

[130] For details, see European Union Agency for Fundamental Rights, *Handbook on European data protection Law*, EU Publications Office, 2018, pp. 135-137.

[131] See European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2019, p. 26; see also Information Commissioner's Office, Opinion on the use of live facial recognition technology by law enforcement in public places, 2019, pp. 13-14; EDPB, Guidelines 3/2019 on processing of personal data through video devices, 2020, p. 33.

[132] Police authorities made substantial efforts when testing FRT, see South Wales Police, DPIA for Automated Facial Recognition, 11 October 2018; Metropolitan Police Service, DPIA for Live Facial Recognition, 01/DPA/20/000467, 10 February 2020. See also Council of Europe, Guidelines on Facial Recognition, above p. 10 and pp. 13-15; C. Castelluccia and D. Inria, 2020; See M. E. Kaminski and G. Malgieri, 'Algorithmic impact assessments under the GDPR: producing multi-layered explanations', *International Data Privacy Law*, 2020.

[133] For an introduction, see D. Leslie, 2020. For examples, see J. Gerards and R. Xenidis, Algorithmic discrimination in Europe, European Commission, 2021, pp. 84, 86, 88 and 114.

[134] See European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2019, p. 27; See European Union Agency for Fundamental Rights, #BigData:

On a **primary law level**, non-discrimination rules are laid down most notably in Articles 2 TEU, 10 TFEU, in Articles 20 and 21 CFR and as a general principle in case law. Article 21 CFR embeds non-discrimination into the framework of substantive norms. Its scope extends beyond the personal and material scope of the secondary non-discrimination legislation, as the provision is sector-neutral and contains a non-exhaustive (theoretically open) list of 'protected grounds'. Where the scope of Article 21 CFR overlaps with that of secondary legislation, the CJEU often refrains[135] from mentioning Article 21 CFR and applies the logic set out in the directives (see below). In other cases, the Court 'anchors its reasoning more strongly in the wording of the Charter'.[136] Due to its open formulation and broad reach, Article 21 CFR seems conceptually fit to tackle cases of **algorithmic discrimination**.

On a **secondary law level**, the most pertinent anti-discrimination laws include the Racial Equality Directive 2000/43/EC, the Employment Equality Directive 2000/78/EC, the Gender Goods and Services Directive 2004/113/EC, and the Gender Equality Directive (recast) 2006/54/EC. The prohibition of discrimination under these directives extends to three policy areas: employment, the welfare system and access to (and supply of) goods and services. However, the grounds protected, are not homogenous – resulting in a 'hierarchy of grounds' and uneven protection.[137] A horizontal anti-discrimination directive, meant to close remaining gaps, is blocked in Council since 2008.[138] Apart from that, the binding secondary legislation largely follows a homogenous logic, which distinguishes between direct and indirect discrimination. The rule or practice in question qualifies as **'direct discrimination'**, where it explicitly makes a distinction based on the 'protected ground' or a non-dissociable factor thereof, and can only be justified under strict conditions.[139] Conversely, an apparently neutral treatment (neutral rule, criterion or practice), which places a group at a significant disadvantage, would qualify as **'indirect discrimination'** and could thus be justified more flexibly.[140] Indirect discrimination mainly differs from direct discrimination in that it moves the focus away from differential treatment to differential effects, and for this reason it can be justified more easily. In machine learning contexts, direct discrimination is predicted to be less prevalent

Discrimination in data-supported decision making, 2018, pp. 3-5; M. Hildebrandt, The Issue of Bias. The Framing Powers of Ml, in M. Pelillo and T. Scantamburlo, *Machine Learning and Society: Impact, Trust, Transparency*, MIT Press, 20, 2019.

[135] See A. Ward, 'The Impact of the EU Charter of Fundamental Rights on Anti-Discrimination Law: More a Whimper than a Bang', *Cambridge Yearbook of European Legal Studies*, Vol. 20, 2018, pp. 42-53; H. Eklund and C. Kilpatrick, 'Article 21', in S. Peers et al., *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing (forthcoming), paras. 21.65-21.69; E. Muir, 'The Essence of the Fundamental Right to Equal Treatment', *German Law Journal*, Vol. 20(6), 2019, pp. 827-829.

[136] See E. Muir, 2019, pp. 833-838 (discussing 'gap cases'). H. Eklund and C. Kilpatrick, 'Article 21', in S. Peers et al., *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing (forthcoming), paras. 21.61-21.64.

[137] For a graphic perspective, see EU anti-discrimination law, Academy of European Law, p. 11; Algorithmic discrimination in Europe, Directorate-General for Justice and Consumers, European Commission, 2021, p. 55; R. Xenidis, Shaking the normative foundations of EU equality law, EUI Working Papers LAW 2017/04, pp. 23-32; R. Algorithmic discrimination in Europe, DG Justice and Consumers, European Commission, 2021, pp. 53-62; P. Hacker, 'Teaching fairness to artificial intelligence', *Common Market Law Review*, Vol 55(4), 2018, p. 1154-1157.

[138] Procedure file 2008/0140(APP), EP Legislative Observatory; for details, see Anti-Discrimination Directive, Legislative Train Schedule, EPRS, European Parliament.

[139] Such acts may be justified based on, for instance, genuine occupational requirements (Article 14(2) Gender Equality Directive (recast) 2006/54/EC, Article 4 Racial Equality Directive 2000/43/EC, Article 4(1) Employment Equality Directive 2000/78/EC), exceptions in relation to religious institutions (Article 4(2) Employment Equality Directive 2000/78/EC), and exceptions particular to age discrimination (Article 6 Employment Equality Directive 2000/78/EC).

[140] Such acts may be justified if they (i) serve a legitimate aim and (ii) effectively promote this legitimate aim, and are (iii) necessary/proportionate.

than indirect discrimination, if not rare.[141] It would appear that, '[i]ndirect discrimination seems fit to capture a large spectrum of apparently neutral but [in fact] discriminatory algorithmic outputs [...]'.[142]

3.3.2. Gaps in the EU anti-discrimination framework

However, many researchers consider that the current EU anti-discrimination framework does not afford sufficient protection from algorithmic discrimination. They assert, for instance, that EU anti-discrimination law suffers from a 'rampant enforcement problem'[143] and that algorithmic discrimination 'exacerbates the weakness of the individual justice approach'.[144] The scope of **secondary legislation** appears inappropriately narrow and certain requirements present inappropriately high thresholds for obtaining protection. Leaving aside intrinsic shortcomings in secondary EU anti-discrimination law,[145] as well as in individual litigation,[146] algorithms may subject new segments of the population to differential treatment that fall outside the pre-existing grounds of EU anti-discrimination directives.[147] Despite being unfair and problematic, such cases would not be prohibited by secondary law. One researcher contends that 'EU anti-discrimination law [...] provides for an easy justification' of certain forms of algorithmic discrimination.[148] While the **fundamental right to non-discrimination** may present a stop-gap,[149] it only applies where the Union institutions, bodies, offices and agencies are acting or EU law is being implemented by the Member States (Article 51 CFR), its applicability to disputes among private entities is uncertain,[150] and drawing on case law, it may prove less elastic and transversal than expected.[151] Additionally,

[141] See European Commission, Algorithmic discrimination in Europe, 2021, pp. 67-73; R. Xenidis and L. Senden, 'EU non-discrimination law in the era of artificial intelligence : mapping the challenges of algorithmic discrimination', in U. Bernitz et al., *General principles of EU law and the EU digital order*, Kluwer Law International, 2020, p. 19; S. Wachter et al., 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI', 3 March 2020, p. 41 and pp. 44-45; P. Hacker, 'Teaching fairness to artificial intelligence', *Common Market Law Review*, Vol. 55(4), 2018, p. 1151.

[142] See R. Xenidis and L. Senden, above at pp. 20-21; See P. Hacker, above pp. 1154-1160 (referring to the material and personal scope of the directives).

[143] P. Hacker, Teaching fairness to artificial intelligence, 2018, p 1167-1168.

[144] R. Xenidis and L. Senden, 2017, p. 26.

[145] Such as 'lack of clarity and ensuing insecurity for claimants' and the uneven level of protection by EU secondary law ('hierarchy of grounds').

[146] R. Xenidis and L. Senden, 2017, p. 25: 'Comparative research on the enforcement of gender equality law in the Member States of the EU reveals a multitude of other, persisting problems that deter people from initiating legal action to protect their right to equality. These range from institutional problems (e.g. length of proceedings, lack of expertise and assistance, lack of trust in the judiciary, lack of sufficient compensation), financial problems (e.g. cost of proceedings, lack of legal aid) to uncertainty about the outcome and fear of victimisation, by the employer, family and society.'

[147] See F. Zuiderveen Borgesius, 2018, p. 36; Similarly, S. Wachter et al., 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI', 3 March 2020, pp. 11-12 and various others.

[148] P. Hacker, 2018, pp. 1164-1165; Opposing this view, see R. Xenidis and L. Senden, 2017, p. 22.

[149] J. Gerards and F. Zuiderveen Borgesius, 'Protected Grounds and the System of Non-Discrimination Law in the Context of Algorithmic Decision-Making and Artificial Intelligence', *Colorado Technology Law Journal*, forthcoming (2021), pp. 12-13.

[150] For details, see Explanations relating to the Charter of Fundamental Rights, Praesidium of the European Convention, 14 December 2007, Explanation on Article 21; A. Ward, 'The Impact of the EU Charter of Fundamental Rights on Anti-Discrimination Law: More a Whimper than a Bang', *Cambridge Yearbook of European Legal Studies*, Vol. 20, 2018, pp. 53-56. On the horizontal effect of the CFR in general see E. Frantziou, 'The Horizontal Effect of the Charter', *Cambridge Yearbook of European Legal Studies*, Vol. 22, 2020. On the horizontal effect of anti-discrimination provisions in Member States' Constitutions, see I. Chopin and C. Germaine, A comparative analysis of non-discrimination law in Europe 2019, European Commission, 2019, p. 11.

[151] A. Ward, 2018, pp. 35-39; See J. Gerards and R. Xenidis, 2017, p. 65.

commentators identified a 'jumble of justifications' and a 'criss-crossing of methods' in case-law and admonish that the lack in coherence 'mutes' the impact of Article 21 CFR and 'is to the detriment of those people [the Charter] sets out to protect'.[152]

Even if the scope of EU anti-discrimination law were extended to span discrimination in various shapes and forms and across the various fields of AI application, it would likely remain ineffective against algorithmic discrimination. Most researchers agree that victims of artificial intelligence discrimination would face profound **challenges to detect and prove (*prima facie*) discrimination**. Absent (comparative) reference points, and due to 'speeds, scale and levels of complexity that defy human understanding', algorithmic decisions may appear legitimate and the victim may not become aware of discrimination in the first place.[153] Even if the victim suspected discrimination, evidence of the algorithmic decisions remains with the operator or provider, and is therefore likely inaccessible to the victim.[154] System controllers may, for instance, invoke their intellectual property rights and trade secrets as grounds for refusal of access.[155] However, it should be noted that courts may take the refusal to provide access into account as one factor in the context 'of establishing facts from which it may be presumed that there has been direct or indirect discrimination'.[156] Nevertheless, without knowledge of at least the algorithmic output, the victim would face particular challenges determining comparator groups, proving statistical disparities and refuting justifications. Finally, even if the victim and their legal counsel were able to obtain access, algorithms are hardly intelligible to non-experts such as victims, judges and legislators.[157] Some artificial intelligence is even generally 'non-decomposable' (**'black box' phenomenon**) and defies common-sense reasoning, thereby precluding the detection of discriminatory decisions or the comprehension of the technical functionality.[158] The resulting enforcement deficits may spiral into lower incentives for compliance.[159]

3.3.3. Options to close gaps in protection

To overcome this lack of transparency and to meet the enforcement challenges, researchers recommend different measures. Some propose statutory innovation, while others rely on leveraging the existing framework through interpretation. Some commentators recommend that 'national legislators should retain or introduce general non-discrimination provisions that can act as a safety net', for cases where differential treatment is not covered by general (Article 21 CFR), or specific anti-discrimination laws, but seems unfair and problematic.[160] Alternatively, sector-specific rules for AI

[152] A. Ward, 2018, pp. 56; See H. Eklund and C. Kilpatrick, 'Article 21', in S. Peers et al., *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing (forthcoming), para. 21.74; E. Muir, 'The Essence of the Fundamental Right to Equal Treatment', *German Law Journal*, Vol. 20(6), 2019, pp. 831-833.

[153] S. Wachter et al., 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI', 3 March 2020, p. 6 and p. 10; P. Hacker, 2018, p. 1169; See J. Gerards and R. Xenidis, 2017, p. 75.

[154] R. Xenidis and L. Senden, '2017, p. 20 and 24 (with reference to the CJEU's *Meister* and *Danfoss* cases). P. Hacker, 2018, pp. 1169-1170; See J. Gerards and R. Xenidis, 2017, p. 75.

[155] S. Wachter et al., 2020, p. 10.

[156] Judgment in Case C-415/10, *Meister*, CJEU, 19 April 2012, para. 47; P. Hacker, 2018, p. 1170 contends 'there is little hope a refusal to grant access to output data will lead to a strong indication of a prima facie case of discrimination. Even if this was different, [...] it only helps to establish a prima facie case, and not to refute the justification of the algorithmic model.' (See preceding paragraph).

[157] See J. Gerards and R. Xenidis, 2017, p. 75.

[158] See S. Wachter et al., 2020, p. 12; J. Gerards and R. Xenidis, 2017, p. 75, consider that 'there is no need to open the algorithmic "black box' but only to provide prima facie evidence'.

[159] See P. Hacker, 2018, p. 1169.

[160] See J. Gerards and F. Zuiderveen Borgesius, (forthcoming), p. 67; See J. Gerards and R. Xenidis, 2021, pp. 141-142.

decision-making may be a viable solution (see Section 4 below).[161] Another researcher mentions viable legislative instruments to fill in the gaps, such as access and information rights, public enforcement, and collective redress, but contends that it is unlikely that the legislator would take action, especially with a view to the horizontal anti-discrimination directive currently stalled in Council.[162] Instead, the researcher advocates leveraging the GDPR, notably data subjects' access rights, data protection impact assessment rules (DPIAs), the principle of fairness and public enforcement instruments.[163] Other commentators developed a statistical tool that enables the identification and assessment of potential discrimination and would thus be of value to judges, claimants and regulators, as well as to operators, providers and manufacturers (e.g. to pre-emptively correct bias).[164] Finally, researchers consider the 'individual justice approach', i.e. individual litigation, as wholly inadequate and favour concentrating on leveraging EU equality and non-discrimination supervisory bodies and the development of an 'equality by design' approach.[165] 'Depending on their mandate, national equality bodies could also play an important role in supporting individual claims, initiating class actions and bringing the issue to the attention of the legislator'.[166] Additionally, impact assessments may be 'further developed as detection and enforcement tools, beyond the area of data protection in the field of equality and non-discrimination' and certification agencies might be promoted.[167] Finally, an integrated approach, combining legal, knowledge-based, and technological solutions may be taken.[168]

3.4. Other relevant legislation

Apart from the above mentioned framework, FRTs need to take account of requirements under EU law protecting the **rights of the child** and of **elderly people**, the **freedom of expression** and **freedom of assembly and of association**, the **right to good administration**, as well as the **right to an effective remedy**.[169] Other concerns raised by the AI components of FRT systems relate to product safety, product liability and consumer protection.[170] Furthermore, a growing body of EU law governing **border controls** must be taken into account in the law enforcement context.

[161] See F. Zuiderveen Borgesius, 2018, pp. 69-70.

[162] See P. Hacker, 2018, pp. 1170-1171.

[163] See P. Hacker, 2018, pp. 1170-1185; On the topic of AI regulation through the GDPR, see Discrimination, artificial intelligence and algorithmic decision-making, Council of Europe Study, 2018, p. 21-25 and G. Mazzini, A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law, in A. De Franceschi and R. Schulze, *Digital Revolution – New challenges for Law*, C.H. Beck and Nomos, 2019, pp. 34-53.

[164] S. Wachter et al., 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI', 3 March 2020, p. 44-72; In fn. 305, they implicitly call for 'data to be collected and held for the purposes of statistical assessment'.

[165] See R. Xenidis and L. Senden, 2020, p. 26-29; See F. Zuiderveen Borgesius, 2018, p. 66, who emphasises the necessity of adequately funding equality bodies and data protection authorities and equipping them with sufficient investigation and enforcement powers: 'Without enforcement, transparency will not necessarily lead to accountability.'

[166] See R. Xenidis and L. Senden, 'above at p. 27; On the powers of equality bodies see E. Lantschner, 'Strategic litigation', *European equality law review*, Vol 2020(1), 2020 and T. Kádár, 'The legal standing of equality bodies', *European equality law review*, Vol 2019(1), 2019.

[167] See R. Xenidis and L. Senden, above at p. 28.

[168] See J. Gerards and R. Xenidis above pp. 140-151.

[169] See European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2019, pp. 28-32.

[170] See European Commission, Impact Assessment accompanying the Proposal for an AI-framework, 2021, pp. 6-9; G. Mazzini, A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law, in A. De Franceschi and R. Schulze, *Digital Revolution – New challenges for Law*, C.H. Beck and Nomos, 2019, pp. 2-34.

Box 3 – AI and border controls

A number of amendments to the different **EU centralised information systems on border controls** are discussed in order to allow the processing of facial recognition technology for the purpose of verification or identification. The integration of automatic face recognition technology in the **EU Schengen Information System** (SIS), the most widely used and largest information sharing system for security and border management in Europe has been proposed. Furthermore, the outstanding proposals for revising the **European dactyloscopy database** (Eurodac), which supports the implementation of EU asylum legislation and the **Visa Information System,** envisage the implementation of face recognition technology.[171]

3.5 Key findings

The processing of biometric data through facial recognition technologies profoundly affects the individual's right to data protection and privacy and its deployment and regulation is subject to the strict rules of the CFR, the GDPR and the LED. Although the specific data protection requirements are still taking shape, the intrusive nature of such technologies and the vocal opposition from a wide range of actors, indicate that developers and operators should not mistake uncertainty for leniency. Ultimately, the EU data *acquis* demands a privacy and data protection-preserving configuration of the entire facial recognition system, including components such as biometric databases, data retention policies, decision-making procedures and algorithms. Additionally, researchers question the effectiveness of the EU non-discrimination framework to tackle algorithmic discrimination associated with FRT systems. Operators of AI-powered FRT systems must take adequate organisational and technical measures to reduce algorithmic discrimination.[172] Conversely, regulators should consider strengthening and extending the EU non-discrimination framework, to ensure that operators do not circumvent the underlying rationale.[173] These fundamental rights issues feature prominently as arguments for an EU regulatory intervention to curb the risks associated with AI applications.[174] According to the European Commission study 'Supporting the Impact Assessment of Regulator Requirements for Artificial Intelligence in Europe', these 'second wave' biometrics bear new and unprecedentedly stark risks for fundamental rights, **most significantly the right to privacy and non-discrimination**.[175]

[171] For an overview, see C. Dumbrava, Artificial intelligence at EU borders, Overview of applications and key issues, IDA, EPRS, European Parliament, July 2021, pp. 13-14.

[172] S. Wachter et al., 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI', 3 March 2020; M. MacCarthy, Fairness in algorithmic decision-making, Brookings, 6 December 2019.

[173] Even if courts attempted to close gaps in protection through an extensive interpretation of the pre-existing legal framework, legal uncertainties and complexities would remain for a considerable period of time. In the medium-term, this could foster a climate in which operators cross the line of what is lawful, while others adopt risk-averse strategies and are dissuaded from lawful business cases. (Similarly, see European Commission, Impact Assessment accompanying the Proposal for an AI-framework, 2021, pp. 23 et seq.).

[174] See European Commission, Impact Assessment accompanying the Proposal for an AI-framework, 2021, p 18-21; See European Commission, Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe, 2021, pp. 22-43.

[175] See Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe, 2021, p. 39

4. Proposed EU artificial intelligence act and facial recognition

4.1. Background

The **European Commission** published a *White Paper on Artificial Intelligence (AI)*[176] in February 2020, highlighting the fundamental rights implications of using remote biometric identification AI systems and especially facial recognition technology in the EU. To prevent fundamental rights violations and to avoid fragmentation of the internal market, the Commission proposes to identify the **specific circumstances**, if any, which might justify such use, as well as **common safeguards**. The EU High-Level Expert Group on AI (AI HLEG), consisting of EU independent experts from academia, civil society and industry, called for (i) a clear definition of if, when and how AI can be used for automated identification of individuals and (ii) differentiation between the identification of an individual, versus the tracing and tracking of an individual, and between targeted surveillance and mass surveillance.[177] Against this backdrop, the Commission highlighted the varying levels of accuracy in the performance of facial recognition systems that can lead to discriminatory outcomes and singled out a scenario for regulating such practices in its impact assessment accompanying the proposal on an AI act.[178]

The **European Parliament** has called for limits to the use of facial recognition in the EU on several occasions. The Parliament has highlighted that the gathering and use of biometric data for remote identification purposes (such as facial recognition) in public areas bears particular risks for fundamental rights and stressed that such technology should only be deployed and used by Member States' public authorities for substantial public interest purposes.[179] The Parliament also invited the Commission to **consider a moratorium on the use of these facial recognition systems in public spaces** by public authorities and on education and healthcare premises,[180] and called for a **moratorium on the deployment of facial recognition systems for law enforcement**, until the technical standards can be considered fully fundamental rights compliant.[181] Some of the law-makers expressed their wish to go a step further and support **banning the use of facial recognition technologies** in specific contexts. For instance, the Parliament recommended banning automated biometric identification such as facial recognition for educational and cultural purposes (unless exceptionally allowed by law).[182] Following the same line of reasoning, a group of more than 100 Members of the European Parliament called on the European Commission to enshrine an explicit ban on biometric mass surveillance in public spaces in EU law.[183]

[176] See European Commission, White Paper on Artificial Intelligence, COM(2020) 65 final.

[177] See High-Level Expert Group on AI, Ethics guidelines for trustworthy AI, 2019 at 33.

[178] See European Commission, Impact Assessment accompanying the Proposal for an AI-framework, 2021, p. 19.

[179] See European Parliament, Resolution on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

[180] See European Parliament, Resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice, 2020/2013(INI).

[181] See European Parliament, Draft report on Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters, 2020/2016(INI).

[182] See European Parliament resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector, 2020/2017(INI).

[183] See MEPs' Letter to the European Commission, 8 March 2021.

4.2. Proposed artificial intelligence act

4.2.1. Main features

The European Commission unveiled a new proposal for an EU regulatory framework on AI in April 2021.[184] The legal framework focuses on the specific utilisation of AI systems and associated risks. The Commission proposes to enshrine **a technology-neutral definition of AI systems** in EU law and to lay down a **classification** for AI systems with different requirements and obligations tailored on a '**risk-based approach**'.

- Certain **particularly harmful AI practices are prohibited** as contravening Union values (article 5). They are considered a clear threat to people's safety, livelihoods and rights and are banned because of the 'unacceptable risk' they create. This includes systems that are designed to manipulate human behaviour through subliminal techniques and social scoring by governments.
- Some AI systems are considered as **'high-risk AI'** because they create adverse impact on people's safety or their fundamental rights.[185] This includes AI technology used in critical infrastructures (e.g. transport), educational or vocational training, product safety components (e.g. AI applications in robot-assisted surgery), employment, essential private and public services (e.g. credit scoring that denies citizens opportunities to obtain a loan), law enforcement, migration, asylum and border control management (e.g. verification of authenticity of travel documents) and administration of justice and democratic processes. A number of AI systems (such as biometric systems) have been specifically identified as high-risk and listed, in an Annex III, which the Commission would be empowered to update as necessary (article 7). Such 'high-risk AI' systems will need to undergo a **conformity assessment** before being placed on the market and comply with a range of **safety requirements** (regarding, for instance, risk management, human oversight and data governance). In addition, an **ex-post market surveillance and supervision** must be put in place to ensure compliance with the obligations and requirements for all high-risk AI systems already placed on the market (article 61).
- AI systems presenting **'limited risk'** would be subject to a limited set of obligations (e.g. transparency).
- All other AI systems presenting **'minimal risk'** could be developed and used in the EU without additional legal obligations, other than existing legislation.

4.2.2 Biometric systems and facial recognition

The draft regulation takes a technology-neutral stance and aims to be as future proof as possible, taking account of the swift technological and market developments related to AI. To that effect, the regulation would apply to all **remote biometrics identification (or RBI) systems** – including **facial recognition technologies**. All such systems operate at a distance without knowing whether the relevant person will be present in an area, capture biometric data (including through facial image

[184] See European Commission, Proposal for a Regulation on a European approach for Artificial Intelligence, 2021/0106 (COD). See European Parliament, Legislative Train, Artificial Intelligence Act.

[185] Article 6 of the draft regulation defines two groups of high-risks AI systems: AI systems that are safety components or products falling under a specific EU harmonised legislation (e.g. toys, motor vehicles) and standalone AI-systems that poses a high risk of harm to the health and safety or the fundamental rights of persons (e.g. AI systems used in road traffic and education).

recognition), compare it with an existing sample or database without significant delay and are used specifically for identifying an individual.[186]

4.2.2.1 'Real-time' and 'Post' biometric identification systems

The Commission proposes to distinguish between 'real-time' remote biometric identification systems and 'post' remote biometric identification systems and subject them to a different set of rules depending on their use. **'Real-time' biometric identification systems** would be defined as systems that are able to capture biometric data and run the comparison and identification processes instantaneously (or without a significant delay), based on 'live' or 'near-live' material, such as video footage, generated by a camera or other device. **'Post' biometric identification systems**, in contrast, would be systems enabling capture of biometric data and comparison and identification processes to run after a significant delay, based on pictures or video footage generated by closed circuit television (CCTV) cameras or private devices. Against this backdrop, different scenarios for regulation of facial recognition can be identified.[187]

4.2.2.2. Scenarios for FRT regulation

(i) Prohibited high-risk real-time remote biometric identification systems for law enforcement purposes

As matter of principle, the European Commission proposes to prohibit the use of AI systems for **'real-time' (or live) remote biometric identification** (i.e. RBI) of natural persons **in publicly accessible spaces** for the **purpose of law enforcement**.[188] Such systems are particularly intrusive, severely interfere with the rights and freedoms of the persons concerned, affect the private life of a large part of the population, may lead to constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other EU fundamental rights. Furthermore, the immediacy of the remote identification and the limited redress mechanisms available to individuals increases the risks for the rights and freedoms of the persons that are concerned by law enforcement activities.[189] In practice, the draft text intends to prohibit the use of RBI in publicly accessible spaces for the purpose of law enforcement, in cases such as when the police deploy **facial recognition systems** to identify persons participating in a **public protest**, or to locate persons who have only committed **minor offences**.[190] Because of their threat to EU fundamental rights and values, such FRT systems would be considered **'high risk' systems** and subject to a **general prohibition** in the EU.

(ii) Permitted high-risk real-time remote biometric identification systems for law enforcement purposes

However, **three exceptions,**[191] in which a substantial public interest outweighs the risks for fundamental rights, are envisaged for the use of RBI systems in publicly accessible spaces for the purpose of law enforcement. The first situation involves the **targeted search for potential victims of crime**, including missing children. The second situation concerns the prevention of a specific,

[186] See recital 8 and article 3 (33) of European Commission, Proposal for a Regulation on a European approach for Artificial Intelligence, 2021/0106 (COD).

[187] Another scenario that is not discussed here is the possibility for facial recognition systems to fall under the provisions of article 53 of 2021/0106 (COD), allowing AI regulatory sandboxes to provide a controlled environment for developing, testing and validating innovative AI systems for a short period before their placement on the market.

[188] See article 5(1)(d)); recital 33 and annex III(1)(a), 2021/0106 (COD).

[189] See recital 18, 2021/0106 (COD).

[190] See T. Christakis and M. Becuywe, Pre-Market Requirements, Prior Authorisation and Lex Specialis: Novelties and Logic in the Facial Recognition-Related Provisions of the Draft AI Regulation, European Law Blog, 2021.

[191] See article 5(1)(d)), 2021/0106 (COD).

substantial and imminent **threat to the life or physical safety** of persons or of a **terrorist attack**. The third situation relates to the detection, localisation, identification or prosecution of a perpetrator or individual suspected of a **criminal offence** referred to in the European Arrest Warrant Framework Decision.[192] This legislation facilitates the speedy and efficient extradition procedure between EU Member States (MS) of people who have committed a **serious crime**, and would therefore permit the real-time processing of biometric data including facial recognition in public spaces.[193]

These exceptions have been carved out because the use of remote biometric identification systems in public spaces would be justified for important public security reasons.[194] However, the draft regulation leaves it to the **Member States** to decide whether they want to implement the abovementioned exceptions for using RBI systems in their national laws or not.[195] In fact, the Commission's proposal takes account of the fact that national security matters largely remain an **exclusive competence** of the Member States and attempts to strike a balance between, on one side, national security and public order and, on the other side, the data protection and other fundamental rights that RBI systems such as facial recognition challenge.[196]

The use of such real-time RBIs would still be subject to the respect of the principles enshrined in the GDPR (see Section 3 above), as well as the existence of adequate procedural safeguards. In particular, the draft proposal stipulates that an **express and specific authorisation** should be granted by a **judicial authority** or by an **independent administrative authority** of a Member State prior to the use of RBIs, except in duly justified situations of urgency.[197]

(iii) Other permitted remote high-risk biometric identification systems

The draft proposal stipulates that other real-time and 'post' remote biometric identification systems should be classified as **'high-risk'**, given that technical inaccuracies in such systems could lead to biased results and entail discriminatory effects, especially when it comes to age, ethnicity, sex or disabilities.[198] A wide range of remote biometric identification systems may fall under this category. This includes, for instance, real-time use of RBI in publicly accessible spaces by public authorities for purposes other than law enforcement (e.g. to control building access); real-time use of RBI in publicly accessible spaces by private actors (e.g. scanning shoppers entering supermarkets, controlling entry to stadiums, schools and transport and for public health purposes); use of 'post' RBI, including when it is used by law enforcement authorities (e.g. for identifying a person who has committed a crime); and use of real-time RBI (including law enforcement authorities) in non-publicly accessible spaces (i.e. private places).[199]

[192] See Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.

[193] Article 2 refers to a long list of crimes offences punishable in the issuing Member State by a custodial sentence or a detention order for a maximum period of at least three years, such as participation in a criminal organisation, terrorism, trafficking in human beings and sexual exploitation of children and child pornography.

[194] See European Commission, Impact Assessment, 2021, p. 18. France, Finland, Czechia and Denmark, inter alia, supported this option.

[195] See recital 22, 2021/0106 (COD).

[196] See, in this sense, T. Christakis and M. Becuywe, 2021. The authors argue that article 5(1)(d) is intended to apply as *a lex specialis* with respect to the rules on the processing of biometric data contained in Article 10 LED.

[197] See recital 21, 2021/0106 (COD).

[198] See recital 33 and annex III(1)(a), 2021/0106 (COD).

[199] See T. Christakis and M. Becuywe, 2021. See also, C. Kind, Containing the canary in the AI coalmine – the EU's efforts to regulate biometrics, Ada Lovelace Institute, 2021. See eDRi, EU's AI law needs major changes to prevent discrimination and mass surveillance, 2021. See M. Veale and F. Zuiderveen Borgesius, Demystifying the Draft EU Artificial Intelligence Act, July 2021.

Such AI systems are not forbidden by default, despite being classified as 'high-risk', but instead subject to several compliance duties. They should only be placed on the Union market or put into service if they comply with certain **mandatory requirements** to ensure that their use does not pose unacceptable risks to important EU public interests, as recognised and protected by Union law.[200] To mitigate the risks to the fundamental rights involved, all RBI systems ('real-time' and 'post' RBI systems) would be subject to **stringent pre-market requirements**. Providers of facial recognition systems would be required to, inter alia, implement adequate risk assessment and mitigation measures, use high quality datasets, ensure transparency and provide users with adequate information, implement appropriate human oversight measures and ensure that such systems are designed with an appropriate level of accuracy, robustness and cybersecurity.[201] Furthermore, RBI systems would be subject to strict **ex-ante conformity assessment procedures** that providers (including importers and distributors) and users of facial recognition systems would have to fulfil.[202] In principle, AI systems used for biometric identification would need to undergo conformity assessment by an independent body (and not left to self-assessment as is the case for other type of high-risk AI systems) unless harmonised standards or common specifications exist (Article 43(1)).[203] Once an RBI system has obtained certification, it could be put on the market and used by public or private actors in accordance with existing EU law. In particular, it should maintain compliance with the **requirements of the GDPR**, which only permit the processing of biometric data under strict conditions (see Section 3 above).[204] In addition, there would also be an **ex-post system for market surveillance and supervision** of such RBI systems, by competent national authorities designated by the Member States.[205]

(iv) Biometric categorisation systems

Facial recognition technologies could also be considered, in theory, to be biometric categorisation systems (see Section 1). Such systems, defined as 'AI system[s] having the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data',[206] are not explicitly classified as a high-risk use of biometrics (when used for purposes other than identification).[207] Therefore – except in the law enforcement domain (see points i) and ii) above) – such systems would only be subject to **transparency measures** and the **persons exposed informed** (unless the use of the systems are permitted by law to detect, prevent and investigate criminal offences).[208]

[200] See recital 27, 2021/0106 (COD).

[201] See articles 8-15, 2021/0106 (COD).

[202] See articles 16-29, 2021/0106 (COD). It is worth noting that the rules proposed are stricter for RBIs (ex-ante conformity assessment would be mandatory unless harmonised standards adopted by the EU standardisation organisations are used) than for other high-risk AI systems (ex-post conformity assessment and internal checks).

[203] See recital 64, 2021/0106 (COD).

[204] See recital 24, 2021/0106 (COD).

[205] See article 61, 2021/0106 (COD).

[206] See recital 35, 2021/0106 (COD).

[207] See annex III.1, 2021/0106 (COD).

[208] See article 1, article 52, 2021/0106 (COD).

Table 1 – Proposed AI regulation: scenarios for facial recognition system regulation

REGULATED FRTs[209]	Real-time [remote] facial recognition systems in publicly accessible spaces for law enforcement purposes		Other [remote] facial recognition (real-time or post) identification systems	Facial recognition systems for categorisation purposes
Rule	prohibited as matter of principle (unacceptable risk)	permitted for specific exceptions (high risk) - search for victims of crime - threat to life or physical integrity or of terrorism - serious crime (EU arrest warrant)	permitted (high risk)	permitted (low risk)
Conditions		- ex-ante authorisation (judicial authority or independent administrative body)	- pre-market requirements - ex-ante conformity assessment (self-assessment or by third-party) - ex-post market surveillance and supervision	- transparency - information

4.3. Key policy issues for discussion

4.3.1. Differentiating high-risk and low-risk biometrics systems

The classification of technologies and their applications into high-risk and low-risk categories is disputable. It is, for instance, **questionable** to make a **distinction between 'real-time' and 'post' remote biometric identification systems**, as well as **between 'biometric categorisation' and 'biometric identification' systems**. Such differentiation risks being arbitrary, because biometric categorisation using multiple features may in fact permit identification (e.g. searching for persons of colour or darker skin-toned, middle-aged males passing a specific CCTV camera location), but also because the use of ex-post and remote biometric categorisation systems in public spaces can have an equally negative impact on fundamental rights as the use of real-time systems.[210] Furthermore, some researchers emphasise that **biometric categorisations fulfil all conditions to be identified as high-risk systems** posing a 'risk of adverse impact[s] on fundamental right[s]' and should therefore be explicitly included in the high-risk list of annex III of the proposal.[211] Moreover, the proposed approach could overlook the **ability of biometric systems deployed by private actors to have a chilling effect on the exercise of fundamental rights** (e.g. if private actors share information with law enforcement authorities or collaborate with them).[212]-

[209] In addition, pre-existing legislation, such as data protection and non-discrimination rules, apply.

[210] See C. Kind, Containing the canary in the AI coalmine – the EU's efforts to regulate biometrics, Ada Lovelace Institute, 2021. The authors stress that some of the most controversial facial recognition technology uses would qualify as "post" use, such as the Clearview AI tool sold to police forces internationally.

[211] See G. Malgieri and M. Ienca, The EU regulates AI but forgets to protect our mind, 7 July 2021.

[212] See N. Smuha and others, How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act, August 2021.

Against this background, academics have suggested, inter alia, **revising the proposed definitions** including of 'biometrics data' and 'biometric identification systems' which are seen as too narrow and allowing for a more **flexible adaptation of the list of prohibited AI practices.**[213] Furthermore, a **more rigorous justification** of the distinction made between private and public uses of remote biometric systems would be required to support a differentiation of the applicable legal rules.[214]

4.3.2. Calls for stricter rules

Under the draft regulation, a wide range of remote biometric identification systems would remain permitted. Critics raise concerns that the proposed ban on **biometric surveillance systems for law enforcement purposes is subject to wide exceptions** and argue that such a ban does not apply to other authorities (e.g. schools, local governments), or private companies (e.g. supermarkets, transport companies), despite evidence that these actors already undertake biometric mass surveillance.[215] Furthermore, since the proposed ban only applies to 'real-time' uses in publicly accessible spaces for law enforcement purposes, equally harmful use cases, such as police monitoring of people by means of controversial software, or surveillance by private actors on behalf of governments and public agencies in public-private partnerships, would still be possible.[216] Civil liberties organisations also ask for a ban or moratorium on the use of automated technologies in border and migration control scenarios until they are independently assessed concerning their human rights implications, and undergo authorisation.[217]

Furthermore, the draft legislation would still permit the police to use facial recognition technologies for **remote biometric categorisation**, despite only imposing very limited safeguards.[218] Furthermore, use of biometric categorisation for purposes other than identification are not, at the moment, explicitly classified as a high-risk use of biometrics in annex III to the proposal. Concerns have been voiced that police forces could therefore use biometric technologies to scan public spaces for people of a particular ethnicity, age, sexual or political orientation, or for people who 'appear suspicious', without any restriction, risk management approach or oversight.[219] The argument goes that real-time facial recognition systems used for the purpose of biometric categorisation would still be lawful in the EU[220] and the proposed AI act would legitimise, rather than prohibit, population-scale surveillance.[221] Against this backdrop, there **are calls to impose an outright ban on applications enabling 'biometric categorisation'** (and not merely subject them to minimal transparency obligations, as proposed by the European Commission).[222]

Likewise, the European Data Protection Supervisor (EDPS) has stressed that the proposal does not go far enough with respect to remote biometric identification and advocates a **stricter approach**

[213] See European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs study, Biometric Recognition and Behavioural Detection, 2021.

[214] See N. Smuha and others, 2021.

[215] See EDri, EU's AI law needs major changes to prevent discrimination and mass surveillance, 2021.

[216] Ibid.

[217] See Access now and others, Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance, 7 June 2021.

[218] See article 52(2), 2021/0106 (COD). The draft legislation explicitly exempts the police forces from disclosing the use of categorisation systems.

[219] See C. Kind, Containing the canary in the AI coalmine – the EU's efforts to regulate biometrics, Ada Lovelace Institute, 2021.

[220] See recital 70, 2021/0106 (COD). In this sense, see C. Kind, 2021.

[221] See M. Veale and F. Zuiderveen Borgesius, 2021, p. 9.

[222] See EDRi, 2021. See as well N. Smuha and others, 2021.

to automated recognition in public spaces, irrespective of whether these are used in a commercial or administrative context or for law enforcement purposes.[223] In a joint non-binding opinion, the EDPS and the European Data Protection Board (EDPB) **called for a general ban on any uses of AI for the automated recognition of human features in publicly accessible spaces** – such as recognition of faces, as well as of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals.[224] The data protection authorities stress that there is no adequate solution to properly inform individuals about such biometric processing and ensure the effective and timely exercise of individuals' rights. Furthermore, they argue that the intrusiveness of the processing does not always depend on the identification in real-time and that the use of biometric systems for private security equally threatens the fundamental rights of respect for private and family life and protection of personal data. Moreover, the EDPB and EDPS recommend a ban (for both public authorities and private entities) on AI systems (including facial recognition) that are used to categorise individuals according to ethnicity or gender, as well as political or sexual orientation, as this can lead to unfair discrimination.[225]

4.3.3. Member States' leeway in implementation

The draft proposal leaves it to the Member States to decide whether they want to implement the exceptions to the prohibition for using real-time facial recognition systems in publicly accessible spaces for law enforcement purposes (detailed in article 5(1)(d)) in their national laws and adopt 'detailed rules of national law' for this purpose.[226] Question arises as to **what 'detailed rules of national law' means exactly** and, especially, if, beyond mere legislative acts voted in Parliament, such rules could take the form of non-legislative acts (e.g. regulatory measures adopted by other authorities, such as the Home Affairs or Justice Ministers).[227] Some clarification would therefore be needed as regards the legal acts required at national level to use RBI systems in publicly accessible spaces for the purposes of law enforcement.

4.3.4. Standardisation and self-assessment

Standardisation will play a key role in providing technical solutions to ensure compliance with the proposed regulation. In particular, under the draft text, high-risk AI systems that are in conformity with **harmonised standards** would be presumed to be compliant with the common mandatory requirements applicable to the design and development of AI systems and therefore allowed to be placed on the market.[228] However, many questions are raised by the proposed standardisation process. The Commission's practice of delegating rule-making to standardisation bodies governed by private law has been criticised for years, essentially because of the lack of democratic oversight, inadequate participation of affected stakeholders, the lack of proper judicial control over harmonised standards and the fact that the European Parliament has no binding veto over harmonised standards mandated by the Commission.[229] Furthermore, while in theory, under the

[223] See EDPS, Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary, 2021.

[224] See EDPB – EDPS, Joint opinion 5/2021, 18 June 2021.

[225] Ibid.

[226] Recitals 22 and 23, 2021/0106 (COD).

[227] See T. Christakis and M. Becuywe, 2021. See as well C. Muller and V. Dignum, Artificial intelligence act, analysis and recommendations, 2021.

[228] See article 40, 2021/0106 (COD).

[229] See M. Veale and F. Zuiderveen Borgesius, 2021, p. 13-14. For an overview of the standardisation process in AI, see S. Nativi and S. De Nigris, AI Standardisation Landscape: state of play and link to the EC proposal for an AI regulatory

draft text, specific notified bodies must assess the conformity of high-risk remote identification systems, in practice, only **self-assessment** would be needed once harmonised standards covering those systems exist.[230]

Industry strongly supports self-regulation.[231] However, such an approach has been heavily criticised for leaving too much leeway for AI developers and to corporate actors who have a major self-interest in the deployment of these systems.[232] Also, experts stress that the proposed standardisation of AI systems is not a matter of purely technical decisions but requires a number of ethical and legal decisions, which should not be outsourced to private entities.[233] Against this background, some changes to the European standardisation process have been called for, inter alia, to grant European stakeholder organisations effective participation rights and to make the process a more transparent and inclusive standardisation system.[234]

4.4. Key findings

The draft AI regulation proposed in April 2021 intends to limit the use of biometric identification systems including facial recognition in the EU, and rests on the premise that such technologies pose the most significant threats to fundamental rights when they are used 'real-time' and for 'identification' purposes. In addition to the existing applicable legislation (e.g. data protection and non-discrimination), the draft AI act proposes to introduce new rules governing the use of FRTs in the EU and to differentiate them according to their 'high-risk' or 'low-risk' usage characteristics. A large number of FRTs would be considered 'high risk' systems that would be prohibited or need to comply with strict requirements. The use of real-time facial recognition systems in publicly accessible spaces for the purpose of law enforcement would be prohibited, unless Member States choose to authorise them for important public security reasons and that appropriate judicial or administrative authorisations are granted. A wide range of facial recognition technologies used for purposes other than law enforcement (e.g. border control, market places, public transportation and even schools) would, however, be permitted subject to a conformity assessment and compliance with some safety requirements before entering the EU market. Furthermore, facial recognition systems used for categorisation purpose would be considered 'low-risk' systems and only subject to limited transparency and information requirements. While EU law-makers are beginning to assess the AI draft act, critics question certain aspects of the proposal, including the distinction between 'high-risk' and 'low-risk' systems, the Member States' leeway for implementing the exception to the prohibition of remote facial recognition systems for law enforcement purposes, and the lack of proper public oversight over the proposed standardisation and self-assessment processes. Some strongly support stricter rules – including an outright ban on such technologies.

framework, 2021. See also M. Ebers, Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act, 2021.

[230] Ibid.

[231] See World Economic Forum, What to know about the EU's facial recognition regulation – and how to comply, 2021.

[232] See AlgorithmWatch's response to the European Commission's proposed regulation on artificial intelligence – A major step with major gaps, April 2021.

[233] See M. Ebers, Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act, 2021.

[234] Ibid.

5. International aspects

5.1. Rise of facial recognition surveillance in the world

The rise of biometric surveillance, in particular facial recognition technology, can be observed in different parts of the globe. According to a report from Amnesty International, at least 64 countries are actively using facial recognition systems in the world today.[235] China is noticeably one of the primary users of the technology. For instance, Chinese schools use face recognition to monitor library loans and compile annual nutrition reports for each student.[236] It has been reported that Chinese authorities use biometric identification, including facial recognition technology, to restrict the movements and activities of the Uyghur minority.[237] Chinese companies are proactive in proposing international technical standards for AI applications, including facial recognition, for instance in the United Nation's International Telecommunication Union (ITU).[238]

The increasing use of facial recognition cameras in public spaces has been particularly documented in a number of countries and regions around the globe, for example, in Kyrgyzstan, India, in Latin America, Israel, the United States, Australia and Russia.[239] It is reported that in Russia, AI-assisted surveillance tools are increasingly used against political dissidents and human rights activists and that the pandemic has accelerated the installation of a network of 100 000 facial recognition cameras to keep track of quarantined individuals.[240] Against this backdrop, policy-makers worldwide are discussing the possibility to put more or less strict legal frameworks in place to control the use of facial recognition systems.

5.2. United States' approach to FRT regulation

Besides the generally applicable privacy rules, there is currently no federal legislation regulating the use of facial recognition by private companies or in the context of law enforcement in the USA. However, the US Federal Trade Commission, in line with its consumer protection mission has issued some guidelines stating that companies should not mislead their consumers regarding how they use facial recognition algorithms.[241] In addition, potential prohibitions, restrictions, or moratoriums on the technology's use are being discussed around the country at State and local levels.[242] Some US cities, such as San Francisco, Boston and Portland, have banned facial recognition technology in public spaces[243] and the State of California has passed legislation that places a three-year moratorium on any facial recognition technology used in police body cameras as of

[235] See S. Feldstein, The Global Expansion of AI Surveillance, Carnegie Endowment for International Peace working paper, 2019.

[236] See ARTICLE 19, Emotional Entanglement: China's emotion recognition market and its implications for human rights, p. 33.

[237] See European Parliament, Digital technologies as a means of repression and social control, Policy Department for External Relations, Directorate General for External Policies of the Union, 2021, p. 15.

[238] See A. Gross, M. Murgia, and Y. Yang, 'Chinese Tech Groups Shaping UN Facial Recognition Standards', *Financial Times*, 1 December 2019;

[239] See European Parliament, Digital technologies as a means of repression and social control, 2021, p. 16.

[240] Ibid at p. 16.

[241] See E. Jillson, Aiming for truth, fairness, and equity in your company's use of AI, 2021.

[242] See Congressional Research Service, Federal Law Enforcement Use of Facial Recognition Technology, 27 October 2020. See also E. Rowe, Regulating Facial Recognition Technology in the Private Sector, *Stanford Technology Law Review*, Vol. 24(1), 2021.

[243] See Rachel Metz, Portland passes broadest facial recognition ban in the US, CNN Business, 2020.

1 January 2020.[244] Nevertheless, the existing patchwork of state and local laws and regulations does not provide legal certainty for public authorities, industry, and citizens. Additionally, the lack of a consistent federal approach is a liability for national security agencies (such as the Central Intelligence Agency (CIA)), which are increasingly using FRTs.[245]

Against this backdrop, there are calls to regulate the use of facial recognition technology in the USA by way of federal legislation, especially in the context of law enforcement surveillance and particularly to provide a unified solution to the emerging privacy issues induced by the use of real-time facial-recognition technology.[246] A range of proposals have been made in this respect including the proposal to enact a Commercial Facial Recognition Privacy Act of March 2019, which would generally prohibit organisations from using facial recognition technology to collect facial recognition data without providing notice and obtaining their consent.[247] Several other federal bills to regulate the use of facial recognition technology have been proposed and are still under discussion.[248]

5.2. China's approach to FRT regulation

In China, there are no laws or regulations in force that explicitly regulate FRT to date. Facial recognition is indirectly regulated by the Cybersecurity Law, which states some requirements for the collection, use, and protection of personally identifiable information including biometric data. However, the National Information Security Standardisation Technical Committee of China published a draft standard on Security Requirements of Facial Recognition Data in April 2021, which aims to set non-mandatory requirements for collecting, processing, sharing and transferring data used for facial recognition in China.[249] Furthermore, it is reported that Chinese legislators are working on enacting a new data privacy law with a strong focus on biometrics, and that China's private sector is attempting to address privacy concerns raised by the use of facial recognition systems through self-regulation, notably with the issuance of guidance and industry standards.[250]

5.3. Discussions on global norms

Today, regulation of AI is a universal topic.[251] How to address FRTs has been particularly addressed in the context of two **international forums**. In 2020, the **UN Human Rights Council** adopted a resolution specifically condemning the use of FRT in the context of peaceful protests, since these technologies create a chilling effect on the exercise of the right to protest by enhancing governments' abilities to identify, monitor, harass, intimidate, and prosecute protesters.[252] The Council called on states to refrain from using facial recognition technology to monitor individuals involved in peaceful protests. The **Council of Europe** (COE), the Strasbourg-based European human

[244] See G. Dunn, 2019 Artificial Intelligence and Automated Systems Annual Legal Review, 2020.

[245] See National Security Commission on Artificial Intelligence, Final report, 2021.

[246] See K. Ringrose, Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns, *Virginia Law Review Online*, Vol 105(1), 2019.

[247] See US Congress, S.847 – Commercial Facial Recognition Privacy Act of 2019.

[248] See G. Dunn, 2020.

[249] See National Law Review, China Publishes Draft Security Standard on Facial Recognition, 2021.

[250] See S. Lee, Coming into Focus: China's Facial Recognition Regulations, 2020. See also A. S. Levine, 'Deeply alarmed': China outpaces US on privacy law, *POLITICO Pro*, 8 July 2021.

[251] See the OECD AI Policy Observatory that provides real-time information and analysis of AI policies initiatives across the globe.

[252] See UN Human Rights Council, Resolution on the promotion and protection of human rights in the context of peaceful protests, A/HRC/44/L.11, 2020.

rights organisation, adopted Guidelines on Facial Recognition in January 2021.[253] These guidelines set out measures that governments, facial recognition developers, manufacturers, service providers and entities using FRT should follow and apply to ensure that they do not adversely affect the human rights and fundamental freedoms of any person, including the right to human dignity and to protection of personal data. The guidelines have a general scope and cover use of FRTs in the private and public sectors. They call for prohibitions on the use of particularly intrusive FRTs and suggest that safeguards should be enacted. The forthcoming work of the Council of Europe on drafting a legal framework for AI is also likely to address the norms applicable to facial recognition.[254] Furthermore, **bilateral cooperation** exists with, for instance, the **Trade and Technology Council** the EU and the USA have decided to set up as a platform for transatlantic collaboration and standard-setting for emerging technologies such as artificial intelligence.[255]

5.4. Key findings

There is a global surge in use of facial recognition technologies and concerns about state surveillance are mounting. Outside Europe, concerns are amplified by the fact that there are, so far, limited legally binding rules applicable to FRTs, even in major jurisdictions such as the USA and China. Policy- and law-makers around the world have the opportunity to discuss – in a multilateral and possibly in a bilateral context – how to put in place more or less strict controls on the use of facial recognition systems. It is crucial for the EU, which has declared its ambition to lead on global AI standards,[256] to engage in these discussions on FRT regulation.

6. Outlook

Academics, stakeholders and policy-makers largely share concerns over the respect of fundamental rights – especially data protection and non-discrimination – stemming from the increasing use of facial recognition technologies. However, the benefits brought by such technology that can actually improve security through more accurate authentication and heightened security are undeniable. Against this backdrop, law-makers face the challenge of encouraging legitimate uses of facial-recognition, while preventing misuse and protecting people's fundamental rights. Given the societal concerns relating to the use of these AI-powered technologies and the risk of fragmentation of the internal market should no action be taken, the Commission proposes to prescribe the specific circumstances that might justify such use and stipulate the necessary safeguards in an AI regulation. To that end, the EU approach to biometrics, and particularly to facial recognition, would rest on a distinction between 'high-risk' and 'low-risk' biometric applications that leads to the application of a more or less strict legal regime. The EU AI approach appears to complement the already applicable strict data protection and non-discrimination rules with a new layer of rules governing the placing on the market of facial recognition technologies. While stakeholders, researchers and regulators seem to agree on a need for regulation, some critics question the proposed distinction between low-risk and high-risk biometric systems and warn that the proposed legislation would enable a system of standardisation and self-regulation without proper public oversight. They call for amendments to the draft text, including with regard to the leeway afforded to the Member States

[253] See Council of Europe, Guidelines on Facial Recognition, 2021.

[254] See Council of Europe, CAHAI - Ad hoc Committee on Artificial Intelligence, 131st Session of the Committee of Ministers, 21 May 2021.

[255] See European Commission, press release, EU-US: A new transatlantic agenda for global change, 2020.

[256] See European Commission, Shaping Europe's digital future – Questions and Answers, 2020.

in implementing the new rules. Some support stricter rules – including an outright ban on such technologies.

References

Buolamwini J., and Gebru T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 2018.

Castelluccia C., and Le Métayer Inria D., Impact Analysis of Facial Recognition, *Centre for Data Ethics and Innovation*, 2020.

Christakis T., and Becuywe M., Pre-Market Requirements, Prior Authorisation and Lex Specialis: Novelties and Logic in the Facial Recognition-Related Provisions of the Draft AI Regulation, *European Law Blog*, 2021.

European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs study, Biometric Recognition and Behavioural Detection, 2021.

European Union Agency for Fundamental Right, Facial recognition technology: fundamental rights considerations in the context of law enforcement, Publications Office of the European Union, 2020.

Gerards J., and Xenidis R., Algorithmic discrimination in Europe, European Commission, 2021.

Leslie D., Understanding bias in facial recognition technologies, The Alan Turing Institute, 2020.

Nativi S., and De Nigris S., AI Standardisation Landscape: state of play and link to the EC proposal for an AI regulatory framework, 2021.

Rowe E., Regulating Facial Recognition Technology in the Private Sector, *Stanford Technology Law Review*, 2021.

Smuha N., and others, How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act, August 2021.

Xenidis R., and Senden L., EU non-discrimination law in the era of artificial intelligence : mapping the challenges of algorithmic discrimination, in Bernitz U. et al., *General principles of EU law and the EU digital order*, Kluwer Law International, 2020.

Annex 1 – Examples of FRT use in select EU Member States[257]

Country	Use cases	Relevant case law, administrative decisions and legislation
France	**FRT pilot projects at schools in Nice and Marseille:** FRT was tested to help safety agents to control access to two high schools, to prevent intrusions and identity theft and to reduce the duration of these controls. ***ALICEM* ID system:** In 2020, the French Ministry of Home affairs launched *ALICEM* (Certified online authentication on mobile phones), a smartphone application using FRT to allow individuals to prove their identity on the internet in a secure manner, using their smartphone and their passport or residence permit.	The administrative court of Marseille annulled the Marseille municipality decision to authorise FRT testing in the two schools in Nice and Marseille. The French data protection authority (CNIL) released a positive opinion on a draft decree authorising the creation of the *ALICEM* system.
Germany	**Crime prevention at train station:** In 2019, the police piloted the use of FRT to detect suspicious behaviour at the Südkreuz **train station** in Berlin.	
	Crime investigation at G20 summit: During the **2017 G20 summit**, the police authorities of the city of Hamburg deployed FRT for the detection and investigation of crimes.	In the G20 context, a first instance court overruled the Hamburg DPA's order to delete the police database of biometric templates. The Hamburg DPA has appealed. The police authorities initially relied on Sections 161 and 163 in conjunction with Section 98c of the **German Criminal Procedure Code** (GCPC). Subsequently, they referred to Sections 161, 163 or, alternatively, Section 483 GCPC.
	Zoo access control: News outlets reported that the **Berlin Zoo** is planning to introduce FRT to facilitate access controls. The Berlin DPA has launched an inquiry on the subject.	
	Safe city market: At least 19 German cities have been supplied with biometric-ready cameras. The Cologne Police Headquarters deployed 'biometric-ready' cameras capable of live facial recognition.	In a decision of 18 January 2021, the Cologne Administrative Court issued an injunctive order against the Cologne Police to stop video surveillance of Breslauer Platz and its side streets in Cologne.

[257] This non-exhaustive table is only meant to give a rough impression of FRT use-cases and of the legal environment in select Member States. It is partially based on the information provide in L. Montag and others, The Rise and rise of biometrics mass surveillance in the EU, A legal analysis of biometrics mass surveillance practices in Germany, the Netherlands, and Poland, EDRi – European Digital Rights, 2021.

Spain	**Surveillance at bus station:** A live face recognition system was deployed in Madrid's South Station in 2016 to fight acts of vandalism and petty crime.	
	Airport: Aena and Iberia operate a facial recognition system in the boarding process since 2019.	
	Immigration: Facial recognition technology is used to improve border control and to increase security at border crossings in Ceuta.	
	Supermarkets: The Spanish supermarket chain Mercadona rolled out FRT to detect people who received a restraining order or who have been banned by a court from supermarket premises.	
Italy	**Automatic Image Recognition System:** An Automatic Image Recognition System (SARI) is used by the police forces for identification purposes since 2019.	On 16 April 2021, the Italian data protection authority issued an opinion stating that the SARI system would result in a form of indiscriminate/mass surveillance if used as designed. A draft bill proposed a moratorium on the use on the use of facial recognition technologies in public spaces.
Ireland	**Public services card:** The Department of Social Protection has deployed a facial recognition system to prevent social welfare fraud.	
Netherlands	**Events control:** Municipalities are using facial recognition technology during carnivals and other large events. **Police control:** Since 2016, the Dutch police use a system of facial recognition technology called CATCH, aimed at identifying suspects or convicts of crimes through a criminal justice database. Police are also trialling the use of real-time facial recognition technology through smartphone pictures, body cams, and the cloud.	The Dutch DPA issued a Recommendation in which it is critical of the current biometric legal framework (*Wet Biometrie Vreemdelingenketen* (Wbvk)) and disapproves of the extension of its application period.

The European Union is considering regulating facial recognition in the proposed artificial intelligence act, currently under discussion. This EPRS publication explains the state of play and further highlights the concerns raised by the use and the potential impacts on people's fundamental rights of facial recognition technologies. Against this background, the paper explores the current EU legal framework applicable to facial recognition and examines the recent proposals for regulating facial recognition technologies at EU level in depth.

OA-01-21-197-EN-N

This is a publication of the Members' Research Service
EPRS | European Parliamentary Research Service

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

PE 698.021
ISBN 978-92-846-8503-5
doi:10.2861/140928