Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

European Union Law Working Papers

No. 91

EU Artificial Intelligence Act: Regulating the Use of Facial Recognition Technologies in Publicly Accessible Spaces

Bruno Zulehner

2024

European Union Law Working Papers

Editors: Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law Working Paper Series is to share "works in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The working papers can be found at http://ttlf.stanford.edu.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law's LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, at:

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Bruno Zulehner is currently studying law and international law at the University of Vienna. While interning at a law firm specializing in claims following the worldwide Volkswagen emissions scandal, his interest in European law was sparked. This, together with his fascination for technology, resulted in the writing of this paper. His other interests lie in the fields of gambling law, corporate law, and civil law.

General Note about the Content

Suggested Citation

This European Union Law Working Paper should be cited as:
Bruno Zulehner, EU Artificial Intelligence Act: Regulating the Use of Facial Recognition Technologies in Publicly Accessible Spaces, Stanford-Vienna European Union Law Working Paper No. 91, http://ttlf.stanford.edu.

Copyright

Abstract

With the Artificial Intelligence Act (AI Act), the European Union has drafted a pioneering piece of legislation aiming to regulate the variety of jeopardies AI systems can pose to its citizens, especially concerning the use of AI in surveillance. This thesis examines the problems caused by the usage of AI in facial recognition technologies (FRTs) comprising of e.g., fundamental rights violations regarding the collection of biometric data of individuals and the discrimination through biased outputs or technological inaccuracies by the respective AI systems as well as the methods and mechanisms applied by the AI Act in order to address those issues. In this context, the risk-based approach of the AI Act, which categorizes most FRTs as either a prohibited AI practice or as high-risk AI, and the prohibition on the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes is displayed, the latter being demonstrated to be not as strict as it seems at first glance due to its limited scope and broad exemptions. As the majority of FRTs fall within the category of high-risk AI systems, the AI Act subjects them to technological requirements, a fundamental rights impact assessment prior to their first application and provides remedies for protection of individuals such as the right to obtain an explanation on a decision taken by the AI system. The AI Act is proven to be a substantive framework for the regulation of AI and thus, despite omitting an outright ban of FRT use in publicly accessible spaces, it will probably show its full potential in the years after its entry into force.

Table of contents

List of abbreviations

(1:1) = Comparison of screened face to one particular image

(1:N) = Comparison of screened face to all images in database

AI (Act) = Artificial Intelligence (Act)

CCTV = Closed Circuit Television

EDPB = European Data Protection Board

EDPS = European Data Protection Supervisor

FRT(s) = Facial recognition technology(ies)

LEA = Law Enforcement Authority

LFR = Life Facial Recognition

MEP = Member of the European Parliament

PIPL = Personal Information Protection Law (China)

RBI = Remote biometric identification

1. Introduction

In a world that is likely to become more and more dangerous from year to year, the demand for new security-providing technologies has been greater than ever. Especially after the 9/11 terror attacks, where a picture of two of the terrorists was taken by a surveillance camera at the airport in Portland, Maine, the question emerged whether the attack could have been prevented altogether by using facial recognition technologies. The technology was already available at the time, with its earliest form dating back to the 1960s, but it was simply not used in the respective surveillance system. These events paved the way for a rapid implementation of facial recognition technologies (FRTs) into the world of security and surveillance in both the private and the public sectors.[1]

In today's world, FRTs are used frequently in many aspects of our daily lives, with features like "Face-ID" on smartphones and automated border control being some of the more popular examples. This might have its benefits, but it also creates a whole lot of issues, particularly regarding privacy, excessive mass surveillance, and data protection. This provides for the need of a closer regulation and oversight of FRTs.[2] With the European Parliament recently passing the "Artificial Intelligence Act", which according to the Commissions Directorate-General for Communications Networks, Content and Technology, is the first-ever legal framework on Ai[3], we might have a proper solution for the aforementioned issues. The elaboration of the AI Act is based on its most recent available version, namely the European Parliament Corrigendum of 16 April 2024.[4] This bachelor thesis aims to give a brief overview of both facial recognition

[1] Kelly A Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (NYU Press 2011) 1ff.
[2] Mark Andrejevic and Neil Selwyn, *Facial Recognition* (John Wiley & Sons 2022) 9.
[3] Directorate-General for Communications Networks, Content and Technology, `AI Act´ (Shaping Europe's Digital Future, March 1, 2024) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed on 17 March 2024.
[4] Corrigendum to the position of the European Parliament adopted at first reading on 13 March 2024 with a view to the adoption of Regulation (EU) 2024/ ..... of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797

technologies and artificial intelligence, as well as the AI Act in general and subsequently, examine the use and problems caused by the application of these technologies in publicly accessible spaces and answer the question, whether the EU Artificial Intelligence Act constitutes a sufficient legal framework for governing those issues. Furthermore, it will provide a quick glance into the foreseeable future regarding recent developments in both the legal and the technological components in this area and concisely compare FRT governance in other jurisdictions. Concluding, the key-findings of the thesis will be displayed in a condensed manner.

2. Facial Recognition Technologies (FRTs)

2.1 Definition

Facial recognition technologies are applications that automatically identify people by comparing their facial characteristics identified in a photo or a video frame with a multitude of faces previously collected in a database. Such systems can be used for verification or identification purposes. In the verification process, the face of a person is matched against the face of one particular person in order to evaluate if it is, in fact, the same person (1:1). In contrast, if the objective is to clarify the identity of a person, the scanned face is compared to every image in the database until it matches one of the database entries (1:N).[5]

Since FRTs use the unique physical characteristics of humans (facial features) as a point of reference for identification/verification, they fall into the category of so-called "biometrics". Other examples of biometrics would be the fingerprint, the voice, or the iris of the eye.[6] The given definition is congruent with the European Union's definition of "biometric data", as the Artificial Intelligence Act (AI Act) describes it as `personal data resulting from specific

and (EU) 2020/1828 (Artificial Intelligence Act) (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) [hereinafter AI Act].

[5] Sangram Thorat, Satyajit Nayak and Jyoti P Dandale, `Facial Recognition Technology: An analysis with scope in India´ (2010) 8 IJCSIS 325.

[6] ibid.

technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, such as facial images or dactyloscopic data´.[7] This definition shall be interpreted in the light of the corresponding definitions of biometric data given by other EU legislation such as the Law Enforcement Directive[8] (LED) or the General Data Protection Regulation[9] (GDPR).[10]

2.2 Historical development

The roots of FRT are found in the mid-60s, when Woody Bledsoe worked on a project where a computer used 20 different manually measured distances between facial features (e.g., distance between pupils, width of the mouth etc.) to create a profile of a face. These profiles were inserted into a database, and in a second phase, the recognition phase, matched against the face that was to be identified. To rule out errors, the computer "normalized" each distance by determining the rotation and tilt of the head, thus calculating the hypothetical distances as if the head was facing forward.[11] The development of FRTs gained momentum and was quickly taken over by government officials, above all the United Stated federal agencies. In 1993, the Defense Advanced Research Agency (DARPA) initiated the Face Recognition Technology Program (FRERET), whose objective was to develop a large-scale facial recognition system that could assist security, law enforcement officials, etc. in performing their tasks.[12] Following, the first civilian government agencies in the U.S., most importantly the DMV (Department of Motor Vehicles), started to incorporate FRTs to combat people obtaining multiple driver´s licenses.

[7] Article 3 (34) AI Act.
[8] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89 [hereinafter Law Enforcement Directive].
[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 [hereinafter General Data Protection Regulation].
[10] Recital 14 AI Act.
[11] Sangram Thorat, Satyajit Nayak and Jyoti P Dandale, `Facial Recognition Technology: An analysis with scope in India´ (2010) 8 IJCSIS 325.
[12] Kelly A Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (NYU Press 2011) 49.

This was achieved by comparing newly taken photos of applicants with existing photos stored in the DMV´s database, marking the first major commercial use of facial recognition technologies.[13] In the late 90s, scientists from Bochum, Germany, developed a truly groundbreaking new method for recognizing faces by using a grid to measure the structure of the whole face, thus abandoning the previously used "feature-based" approach.[14] Throughout the following decades, the technologies were steadily improved and progressively incorporated into security systems. At the 2001 Superbowl in Tampa, a large-scale biometric surveillance system was used for the first time to detect criminals in the crowds. With the ascending of social media in the 2000s, a remarkable increase in processing speeds of computers and huge advances in machine learning algorithms, the conditions for a faster-than-ever development of an efficient and precise FRT were established.[15] Today, FRTs are able to match scanned faces against databases consisting of billions of images, with leading companies claiming accuracy levels (i.e., level of correct identification of the person) close to 100%.[16]

2.3 Artificial Intelligence (AI)

2.3.1 Definition of AI

Defining the term "Artificial Intelligence" is not as easy as it might seem at first glance, especially without diving too deep into computer science and psychology. The difficulties of finding a suitable definition start already when determining, what "intelligence" really is, because that might be different for every other person. In very broad terms, one could say that intelligence is being able to acquire knowledge through understanding the objective world, identify and solve problems by applying the previously learned, and react according to past experiences.[17] With that in mind, AI could be defined as a computer system, hence artificial,

[13] Ibid. 52.
[14] Harry Wechsler, *Reliable Face Recognition Methods: System Design, Implementation and Evaluation* (Springer Science & Business Media 2009) 12.

[15] Mark Andrejevic and Neil Selwyn, *Facial Recognition* (John Wiley & Sons 2022) 11.
[16] Ibid. 12.
[17] Rajendra Akerkar, *Introduction to Artificial Intelligence* (PHI Learning Pvt Ltd 2014) 2.

which is capable of operating in a way that is perceived as intelligent due to imitating the previously mentioned characteristics for intelligent human behavior.[18] Another interesting approach is to use context-based definitions considering e.g., the amount of human intervention in the decision-making of the AI system.[19] Even though it is difficult to find a fully striking definition of AI, the given attempt to do so is sufficient for the purpose of this bachelor thesis (see also below, 4.2.1, for definition of "AI system" in context with the AI Act).

2.3.2 Operation of AI and its role in FRTs

AI systems might serve various purposes (e.g., problem solving or making automated decisions[20]) and make use of a multitude of mechanics in order to reach their previously set goals. Regarding facial recognition technologies, the given objective to be fulfilled by the respective AI will often be to distinguish a face in a video frame or an image from its surroundings and match the face with biometric data from a database. In order to correctly recognize a face, modern FRTs use machine learning and so called "artificial neural networks". Simply put, these algorithms are trained to recognize patterns in images. This is achieved through previous exposure to millions of images depicting faces in different angles and lightnings. The algorithm checks the image for a convolute of pixels typically found in pictures of faces. In the days of social media, providing the algorithm with training data is easier than ever, due to the large number of photos being uploaded to e.g., Facebook every day.[21]

[18] Ibid.
[19] Hannah Ruschemeier, `AI as a Challenge for Legal Regulation – the Scope of Application of the Artificial Intelligence Act Proposal´ (2023) 23 ERA Forum 361 <https://doi.org/10.1007/s12027-022-00725-6>.
[20] Stuart Jonathan Russell, Peter Norvig and Ernest Davis, *Artificial Intelligence: A Modern Approach* (Prentice Hall 2010) 64, 610.
[21] Taina Bucher, `Facing AI: Conceptualizing 'fAIce Communication' as the Modus Operandi of Facial Recognition Systems´ (2022) 44 Media, Culture & Society 638.

3. FRTs in publicly accessible spaces

3.1 Where FRTs are used

Even though the use of facial recognition is widespread among many areas of life such as smartphone security or profiling individuals[22], this bachelor thesis focuses on the use in publicly accessible spaces.

Primarily, FRTs are used by public authorities in CCTV systems for the surveillance of public spaces like airports, busy streets, or large crowds at music festivals to provide security and facilitate the identification of wanted criminals. The state-of-the-art technology used is Live Facial Recognition (LFR), where the faces of people caught by the CCTV cameras are constantly matched against a database of wanted criminals´ faces or stored temporarily in case of future investigations. Such technologies are globally utilized, notably in China, where over 600 million facial recognition cameras are implemented into the nationwide surveillance system. To a smaller extent, countries in the European Union have made use of FRTs as well. In Germany, for example, LFR has been used to monitor the Cologne Cathedral and its surroundings, streets during the G20 events, and train stations as part of a plan to increase public security.[23]

3.2 Problems arising with use of FRTs in publicly accessible spaces

As one could imagine, the use of FRTs in public might pose a variety of concerns among individuals. These issues arise not only from an ethical or legal point of view but also regarding the technical capabilities of FRTs.[24]

[22] Catarina Fontes and Christian Perrone, `Ethics of Surveillance: Harnessing the Use of Live Facial Recognition Technologies in Public Spaces for Law Enforcement´ (Technical University of Munich, 2021) <https://ieai.sot.tum.de/wp-content/uploads/2021/12/ResearchBrief_December_Fontes-1.pdf> accessed 22 April 2024.
[23] Ibid.
[24] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (European Parliamentary Research Service 2021).

3.2.1 Technical issues

As highlighted in the chapters above, the operation of FRTs requires databases containing large amounts of biometric information to properly identify a face. Such databases are at risk of breaches and consecutive misuse of the stored information. Furthermore, the quality of those databases is rarely subjected to manual checks (i.e., whether faces are labeled correctly or not) due to the sheer size of most modern biometrics databases. Moreover, the accuracy of FRTs may vary significantly when matching images with low resolution, bad lightning, large age differences between two images of the same person, or different facial expressions. This causes higher so-called "error rates", composed of the failure of identifying a face in an image (false negative) and wrongful identification of a person with an incorrect face or even a non-facial structure (false positive). Taking these issues into account, the capability of FRTs to be used as a reliable tool in public (e.g., law enforcement) is highly questionable[25], especially given that false positives might induce for example a wrongful prosecution or arrest.[26]

3.2.2 Gender and racial bias

The vast variation of accuracy in facial recognition technologies is often linked to the race and gender of the person who is to be identified. Many algorithms work best on identifying white Caucasian males due to the failure of the training data to display actual racial composition of the population and instead, it mostly consists of images depicting middle-aged white males. As a result, people of color and woman are prone to being exposed to much higher error rates. A study conducted by two U.S. scientists in 2018 revealed that out of four categories (dark skinned male/female, light skinned male/female), dark skinned females experienced the highest error rate, while light-skinned males the lowest error rate regarding gender classification by FRTs.[27]

[25] Ibid.
[26] Giuseppe Mobilio, `Your Face Is Not New to Me – Regulating the Surveillance Power of Facial Recognition Technologies´ (2023) 12 Internet policy review <http://dx.doi.org/10.14763/2023.1.1699>.
[27] Samuel D. Hodge Jr., 'The Legal and Ethical Considerations of Facial Recognition Technology in the Business Sector ' (2022) DePaul Law Review 731.

Such incorrect results can pose significant discrimination against the affected groups. Especially when it comes to law enforcement and the prosecution of criminals, false positives may have serious impact on a person's life. It is reportedly harder to prove one's innocence if a facial recognition system has previously identified one as the wanted suspect, thus shifting the burden of proof toward the suspect on grounds of erroneous biometric identification. This contravenes Article 21 of the Charter of Fundamental Rights (CFR)[28], which prohibits all discrimination on grounds of sex, color, ethnic origin (etc.)[29] as well as the Article 14 of the European Convention on Human Rights (ECHR).[30]

3.2.3 Privacy concerns and fundamental rights issues

The use of real-time facial recognition systems in public places might create an environment harmful to the right to privacy of an individual as it can always determine a person's current location. Constant and excessive surveillance is likely not only to impair a person's right to liberty enshrined in Article 6 CFR[31], but also their right to dignity (Article 1 CFR). The Italian Data Protection Authority already took position on this issue regarding a real-time image recognition system to monitor migrant disembarkation[32], stating that `automated processing of biometric data for facial recognition could constitute a form of indiscriminate mass surveillance´.[33] In the course of operation, (biometric) personal data is persistently collected, stored, analyzed, and thus processed by the respective facial recognition system and its operator. This makes the use of such an application hardly in line with the requirements laid down by the CFR in its Articles 7 and 8 regarding privacy and personal data. Especially in the light of the

[28] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (European Parliamentary Research Service 2021).
[29] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391 Article 21.
[30] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended by Protocols Nos. 11 and 14) (ECHR) Article 14.
[31] European Commission, ´Laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts´ (Impact Assessment) SWD (2021) 84 final.
[32] European Parliament, `Use of facial recognition technology for migrant disembarkation in Italy´ (Parliamentary Question) E-002182/2021.
[33] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (European Parliamentary Research Service 2021).

consent requirement of Article 8, it becomes evident that the operation of a facial recognition system is subject to high demands, at least in theory. Since it is not easy to acquire consent from every person affected, particularly when using FRTs in publicly accessible spaces, this requirement is rarely fulfilled. Time has shown that the requirement of consent has not been taken seriously by a multitude of FRT vendors, primarily when creating their biometric databases. Instead, they gathered biometric data from websites available to the public.[34]

Furthermore, the effects that facial recognition systems used in publicly accessible spaces have on a person's freedom of opinion, expression, assembly, and association[35] must be evaluated. These technologies enable authorities to monitor large gatherings of persons and identify individuals taking part. However, when surveilling a large number of people, a facial recognition system might reach its boundaries and falsely flag many individuals, although normally having a low rate of error. This might lead to unfounded interventions by security forces that disturb, for example, a permitted assembly of people. As assemblies are typically providing individuals with at least a certain degree of anonymity by acting as a crowd, this protection of being singled out is largely undermined by surveillance through FRTs. Therefore, people are less likely to engage in demonstrations, assemblies, and other political activities where such systems are used due to the fear of being individualized and prosecuted because of their attendance at the gathering and their political opinions.[36]

3.2.4 Subtle expansion of usage (function creep)

Another major concern is the possibility of a gradual expansion of the FRT-use beyond its initial purpose and thus, the extension of surveillance without appropriate protective measures.[37] It is

[34] Ibid.
[35] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391 Article 11, 12.
[36] 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) UN Doc A/HRC/44/24.
[37] Phillip Hacker, `Comments on the Final Trilogue Version of the AI Act´ (European New School, 23 January 2024) <https://www.europeannewschool.eu/images/chairs/hacker/Comments%20on%20the%20AI%20Act.pdf> accessed 22 April 2024.

easy for the respective user to widen the application of a facial recognition system due to the flexibility of such systems. This can be achieved through enlarging the underlying database by adding biometric data or using other existing databases. An example for this would be to aggrandize the group of monitored persons by adding biometric data of political activists to the database of a facial recognition system usually in operation for the search of missing persons. Furthermore, the use of such a system for a purpose other than its original, e.g., to monitor a crowd at a festival not only for wanted criminals but also additionally evaluate its racial composition, would constitute such an extension. Likewise, the enlargement of the application area in terms of streets, neighborhoods, etc. and exchanging the user of the facial recognition system might also be similarly problematic. This phenomenon is also referred to as "function creep", as the function of the AI system is successively expanded.[38]

3.2.5 The role of private actors

FRTs are predominantly developed by private companies and then sold to public (mostly law enforcement) authorities which raises the question of whether these actors might value their profits higher than the protection of individual rights. A fairly well-known example of a company making use of illegitimate practices is Clearview AI (see below 4.3.1). Many large tech companies like IBM or Microsoft have abandoned the development and provision of FRTs to law enforcement authorities due to insufficient legal guidelines and the corresponding fear of misuse.[39]

[38] Philip AE Brey, `Ethical Aspects of Facial Recognition Systems in Public Places´ (2004) 2 Journal of Information, Communication and Ethics in Society 97 <https://doi.org/10.1108/14779960480000246>.
[39] Giuseppe Mobilio, `Your Face Is Not New to Me – Regulating the Surveillance Power of Facial Recognition Technologies´ (2023) 12 Internet policy review <http://dx.doi.org/10.14763/2023.1.1699>.

4. The Artificial Intelligence Act (AI Act)

4.1 Historical origin

In February 2020, the European Commission published its White Paper on Artificial Intelligence, which sets out aims of securing European leadership in this field of technology and striking a balance between the use of AI and protection of EU citizens´ rights. Furthermore, the White Paper acknowledges potential serious violations of fundamental rights resulting from the use of AI and calls for a regulatory regime that minimizes the potential risks.[40] The following year, the Commission published a proposal for the Artificial Intelligence Act, thereby initiating the ordinary legislative procedure. The European Central Bank, the Committee of Regions and the Economic and Social Committee issued their opinions on the proposal. On March 13th 2024, the European Parliament adopted a text in its first reading and is now waiting for approval in the European Councils´ first reading[41], leaving the procedure ongoing at the time of writing this thesis. Most recently, the European Parliament issued a Corrigendum to its previously adopted position which corrects errors in language and numbering that were present in earlier drafts.[42]

4.2 Overall analysis

4.2.1 Main objectives

AI technologies represent a great opportunity for member states to improve processes in many areas of life such as healthcare and public services. Furthermore, the continuous development can provide them with competitive advantages on the global market. At the same time, these technologies can cause harm to EU citizens regarding especially in terms of fundamental rights

[40] European Commission, `White Paper on Artificial Intelligence - A European approach to excellence and trust´ (White Paper) COM (2020) 65 final.
[41] Publications Office of the European Union, `Procedure 2021/0106/COD´ <https://eur-lex.europa.eu/procedure/EN/2021_106> accessed 26 March 2024.
[42] Future of Life Institute, `The Act Texts´ (Future of Life Institute, 2024) <https://artificialintelligenceact.eu/the-act/> accessed 24 April 2024.

and psychological well-being (see also 3.2).[43] Therefore, the main objective of the AI Act is to establish harmonized rules for the development, placing on the market, putting into service, and use of AI systems. Simultaneously, it promotes the development of human-centered and trustworthy AI, fast innovation, and ensuring the protection of health, safety, and citizens´ fundamental rights enshrined in the CFR.[44]

4.2.2 Scope

The AI Act provides a broad personal scope of application, which includes providers who place an AI system on the market or put it into service regardless of their location, deployers established or located in the Union, importers, distributors, and all persons concerned who are located in the Union. It also applies to providers and deployers located or established in a third country if the output of the AI system is used in the Union.[45]

The term "deployer" describes any natural or legal person, including a public authority, agency, or other body, that uses an AI system under its authority.[46] The term "user", previously made use of in the Commissions initial proposal has thus been replaced, despite an unchanged definition.[47] There are exceptions for military use, scientific research purposes and purely personal, non-professional use.[48]

Regarding material scope, the AI Act applies to so-called "AI systems". Since AI is a hard to define term (see above, 2.3.1), EU lawmakers have chosen a wide, flexible definition, coordinated with international organizations working in the respective field of technology:[49]

[43] Recital 4-5 AI Act.
[44] Article 1 (1) AI Act.
[45] Article 2 (1) (a-g) AI Act.
[46] Art 3 (4) AI Act.
[47] European Commission, `Proposal for a regulation of the European parliament and of the council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts´ COM (2021) 206 final [hereinafter COM (2021) 206 final].
[48] Article 2 (3), (6), (8), (10) AI Act.
[49] Recital 12 AI Act.

´AI system' means a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.[50]

The definition focuses on distinguishing AI systems from traditional software by highlighting the capability to infer, which comprises of the ability to learn and reason and is achieved by e.g., machine learning[51], as implemented in AI supported FRTs (see 2.3.2).

4.2.3 Categorization and risk-based approach

According to its Recital 26, the AI Act follows a clearly defined "risk-based" approach. The goal is to provide a proportional and effective set of rules, achieved by tailoring the to-be-applied provisions to the possible extent of risk posed by the respective AI system. Therefore, AI systems are classified into different categories according to their previously calculated risk.[52] As laid down in section 3.1 of the Explanatory Memorandum of the initial proposal, the risk should be assessed case-by-case, considering the impact on rights and safety the system will have.[53]AI systems are categorized as either posing an unacceptable, high, limited, or minimal risk. Whereas there are no additional obligations for minimal risk AI systems and only certain specific rules for limited risk AI systems (e.g., regarding higher transparency obligations), systems falling within the other two aforementioned categories are extensively regulated by the AI Act. AI systems constituting an "unacceptable risk" are, with few exceptions, completely prohibited (e.g., social scoring). So called "high-risk" AI systems are permitted but are subject

[50] Article 3 (1) AI Act.
[51] Recital 12 AI Act.
[52] Recital 26 AI Act.
[53] COM (2021) 206 final.

to high safety standards, have to pass a conformity assessment carried out before market implementation and be thoroughly surveilled during operation.[54]

4.3 Application on FRTs

In general, AI supported FRTs constitute AI systems governed by the AI Act, and the most commonly used systems can be labeled as either posing unacceptable or high risk. However, in order to determine the specific rules applicable to a certain facial recognition system, a distinction has to be made between the characteristics of verification, categorization, and identification as well as "real-time" and "post" identification. Furthermore, the context of use has to be evaluated.[55] The AI Act does not speak of "facial recognition". Instead, the notion of "remote biometric identification (RBI) system", of which FRTs are a subcategory, is used. Alongside e.g., voice recognition, FRTs are one of many RBI systems which are thus regulated by the AI Act and can be subsumed under all provisions governing the use of RBI systems.[56]

4.3.1 Prohibited use of FRTs

With its Chapter II containing illicit AI practices, the AI Act addresses constellations where the use of FRTs constitute an unacceptable risk[57], as they are seen as particularly intrusive to the rights and freedoms.[58] Regarding use in public places, especially Article 5 (1) (h) lays down crucial rules for FRT operation.

The provision prohibits the use of so-called "real-time remote biometric identification systems" in publicly accessible spaces for the purposes of law enforcement altogether.[59] The notion of real-time describes a facial recognition system where the moments of capturing the biometric

[54] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (European Parliamentary Research Service 2021)
[55] Ibid.
[56] Catherine Jasserand, `The Future AI Act and Facial Recognition Technologies in Public Spaces´ (2023) 9 European Data Protection Law Review 430 <https://doi.org/10.21552/edpl/2023/4/9>.
[57] Art 5 AI Act.
[58] Recital 32 AI Act.
[59] Article 5 (1) (h) AI Act.

data, the comparison to the database, and the identification of the person all (nearly) coincide[60], whereas "remote" refers to the identification of a person without their active involvement, as commonly the case when using cameras.[61] For a location to be qualified as "publicly accessible" under the AI Act, it has to be accessible by an undetermined number of natural persons without, or with limited restrictions that can be fulfilled by an undetermined number of natural persons (e.g., age restrictions). Thus, it is irrelevant whether the space is publicly or privately owned and which purpose it serves.[62] As the wording of Article 5 (1) (h) indicates, it only applies to use in the context of law enforcement, which might be, for example the monitoring and identification of protesters.[63]

However, there are three scenarios stipulated in its subsections i-iii where the application of FRTs as described above is permitted: Firstly, the targeted search of specific victims of crimes like abduction, human trafficking, as well as missing persons. Secondly, prevention of imminent threats to the lives of natural persons and/or terrorist attacks. Thirdly, for the identification, investigation and/or prosecution of a person who is suspected to have committed a crime referred to in Annex II of the AI Act and punishable with a maximum of at least four years of imprisonment in the respective member state.[64] Sufficient offences included are, for example illicit trafficking of narcotics, organs, humans or weapons as well as terrorism and murder.[65] The legislator thus values the needs of the public interest in these situations higher than the prevention of threats posed by FRTs.[66] Even though the use of real time remote biometric identification systems in law enforcement might fall with an abovementioned exception, it may only be used for specific identification of the targeted individual after an

[60] Recital 17 AI Act.
[61] Art 3 (41) AI Act.
[62] Recital 19 AI Act.
[63] Theodore Christakis, Mathias Becuywe, and AI-Regulation Team, `Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021´ (2021) <https://ai-regulation.com/wp-content/uploads/2021/05/Final-Report-26-04.pdf>.
[64] Article 5 (1) (h) (i-iii) AI Act.
[65] Annex II AI Act.
[66] Recital 33 AI Act.

evaluation of the consequences an abstention of use would have, and an assessment of the impact on freedoms and rights of concerned persons. Moreover, law enforcement authorities have to register the system in the EU database, compile an assessment of effects on fundamental rights in accordance with Article 27 AI Act[67] and notify their respective market surveillance authority and national data protection authority.[68] Furthermore, use is only permitted if a judicial authority or independent administrative authority with capability of issuing binding decisions previously approves the application upon receiving a reasoned request by the law enforcement authority, considering the necessity and proportionality of the measure.[69]

Another interesting aspect of Chapter II is the prohibition of AI systems for facial recognition database creation or augmentation, given that they obtain facial images from previously recorded CCTV footage or the internet without targeting specific individuals.[70] Such a large-scale collection of biometric data without the consent of the individuals concerned could create a sense of mass surveillance and lead to violations of the right to privacy.[71]

4.3.2 Use of high-risk FRTs

Article 6 AI Act sets out rules for classifying certain AI systems as "high-risk" and mentions Annex III in its paragraph 2, which lists various areas of AI-application falling within the high-risk provision.[72] The Commission has been granted the ability to enlarge, restrict or amend this list by means of delegated acts pursuant to Article 7 AI Act, in order to adapt to quick changes and new developments in this dynamic field of technology (see also 6.2).[73]

[67] Article 5 (2) AI Act.
[68] Article 5 (4) AI Act.
[69] Theodore Christakis, Mathias Becuywe, and AI-Regulation Team, `Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021´ (2021) <https://ai-regulation.com/wp-content/uploads/2021/05/Final-Report-26-04.pdf>.
[70] Art 5 (1) (e) AI Act.
[71] Recital 43 AI Act.
[72] Article 6 (2) AI Act.
[73] Recital 52 AI Act (see also, Annex III 1 (a)).

Among various categories such as employment and critical infrastructure, Annex III defines "biometrics" as an area where the operation of AI systems poses a high risk due to the sensitivity of biometric data. In this respect, the legislator acknowledges the technological boundaries of remote biometric identification and the possible risks that come with its inaccuracies. Remote biometric identification systems are therefore classified as high-risk AI systems.[74] This approach offers a wide scope of application for Article 6 in conjunction with Annex III, which covers for example the use of RBI systems in publicly accessible spaces by private actors to e.g., monitor stadium entries, or in non-publicly accessible spaces.[75]

It should be noted that, in comparison to the abovementioned prohibited AI practice of real-time remote biometric identification for law enforcement purposes, the prerequisites of "real-time" as well as "law enforcement purpose" are not necessary to fall within the scope of Article 6 and be classified as high-risk. Therefore, also so-called "post RBI", where there is a significant delay in time between capturing biometric data, comparing it to the database, and identifying the person are encompassed by Article 6. Article 43 defines such "post RBI" only *e contrario* to real-time RBI.[76]

Moreover, mere biometric verification systems used for confirmation of a person's claimed identity are explicitly exempt from the provision[77], thus emphasizing the legal importance of the distinction between identification and verification systems as described above in 2.1.

The classification as high-risk entails far-reaching consequences for both providers/developers as well as users/deployers, stipulated in Sections 2 and 3 of Chapter III. Pursuant to its risk-based approach, the AI Act stipulates the duty of implementing a risk management system,

[74] Recital 54 AI Act.
[75] Theodore Christakis, Mathias Becuywe, and AI-Regulation Team, "Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021" (2021) <https://ai-regulation.com/wp-content/uploads/2021/05/Final-Report-26-04.pdf>.
[76] Ibid.
[77] Annex III 1 (a) AI Act.

consisting of continuous analysis of potential risks posed by the AI system to health, safety and fundamental rights when used according to its intended purpose. It also involves estimating the risks arising from foreseeable misuse throughout the entire operational process.[78] Following, appropriate and targeted measures to address those risks have to be adopted. The goal is to develop and design AI systems in a manner that minimizes potential risks as much as possible, while controlling ineliminable risks.[79]

Since state-of-the-art FRTs/RBI systems make use of AI models (see 2.3.2), Article 10 provides provisions on the quality criteria of datasets used for training and developing such AI systems. *Inter alia,* these datasets have to be free of errors and complete to the best extent for the intended field of application, as well as transparent about the original purpose of collecting the contained data.[80] Moreover, human oversight is to be enabled through the appropriate design of the respective AI system and training of the person in charge of monitoring the system throughout its lifecycle. For RBI systems, a further requirement is laid down. No decision or action by the deployer is to be taken solely based on the output of the system unless the result has been separately verified by at least two natural persons. However, this requirement might be circumvented since paragraph 5 of Article 14 enables member states to declare the requirement disproportionate through national or union law in the areas of law enforcement, migration, asylum, and border control.[81]

Article 15 AI Act aims to implement compulsory appropriate levels of accuracy, robustness, and cybersecurity (see more below, 5.2).

[78] Recital 65 AI Act.
[79] Article 9 AI Act.
[80] Recital 67 AI Act. It should be noted that the requirement of transparency is mentioned in Recital 67 regarding facilitation of compliance of the respective datasets with EU legislation such as Regulation 2016/679 (GDPR).
[81] Article 14 AI Act.

Furthermore, high-risk RBI systems have to undergo a so called "conformity assessment", in which the compliance of the system with the provisions of Chapter III Section 2 is examined.[82] This procedure is predominantly carried out by the provider of the AI systems themselves as the legislator plans to leave them with this responsibility at least for the initial phase of the AI Act. There is an exception with regard to biometrics as such AI systems have to be subjected to a third-party conformity assessment[83], carried out by a notifying body designated by each member states notifying authority.[84] The operation and appointment of these bodies are meticulously regulated in Section 4 of Chapter III.

4.3.3 Limited and minimal risk FRTs

As described above, facial recognition technologies can mainly be classified as either prohibited AI practices or high-risk AI. Notwithstanding, in some cases risk evaluation might lead to FRT being assessed as posing only limited or minimal risk. This happened to be the case with FRTs used for biometric categorization and emotion recognition under the ruleset of the commission's initial proposal.[85] However, this has changed as the adopted text now explicitly states both biometric categorization and emotion recognition in Annex III (1), labeling them as high-risk AI systems[86] and thus, rendering these categories rather inessential in regard to the usage of facial recognition technologies in public.

4.4 The AI Act in relation to other EU legislation

The rules of the AI Act are complementary to existing Union law, particularly in the areas of consumer protection, data protection and fundamental rights. Therefore, all rights and remedies

[82] Article 3 (20) AI Act
[83] Recital 125 AI Act.
[84] Article 28 AI Act.
[85] Recital 70 COM (2021) 206 final.
[86] Annex III 1 (b-c) AI Act (see also Report A9-0188/2023 of the European Parliament where the original wording of the Annex III 1 (a) proposal changed for the first time).

to which the individual is entitled to by e.g., consumer protection are unaffected by the AI Act and remain fully applicable.[87]

It should be noted that the AI Act is not the union´s first legal framework to govern FRTs. Two of the most notable existing rulesets are the Law Enforcement Directive (LED) and the General Data Protection Regulation (GDPR). As described in its very first Article, the LED aims to protect natural persons when their personal data is processed by law enforcement authorities. Article 10 LED therefore subjects the permission of processing of biometric data for identification purposes to certain prerequisites which have to be met. Nonetheless, the provisions of the AI Act regarding the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes constitute *lex specialis* to Article 10 LED and will thus be applied instead.[88] Outside the aforementioned area, Article 10 LED still applies in its entirety, as well as Article 9 (1) of the GDPR for cases without the involvement of law enforcement authorities.[89]

5. AI Act as a sufficient solution?

When new legislation is drafted, there might always be critique on e.g., whether the scope is too broad or too narrow, or whether the rules are too strict or too loose. Thus, since its first proposal in 2021, the AI Act has not been spared of criticism by a multitude of persons as well as international humanitarian rights organizations such as Amnesty International.[90] Especially in the area of facial recognition, biometrics and surveillance, the AI Act has been denounced by some for various reasons. These are for example the ambiguity of the scope and definitions

[87] Recital 9 AI Act.
[88] Recital 38 AI Act.
[89] Recital 39 AI Act.
[90] Amnesty International, "EU: Artificial Intelligence Rulebook Fails to Stop Proliferation of Abusive Technologies" (Amnesty International, March 14, 2024) <https://www.amnesty.org/en/latest/news/2024/03/eu-artificial-intelligence-rulebook-fails-to-stop-proliferation-of-abusive-technologies/> accessed April 16th, 2024.

given in the AI Act, the exceptions granted for some provisions, or the shortcoming of essential protection of fundamental rights.[91]

5.1 Discussing the extent of regulation

Since the use of FRTs for mass surveillance purposes enables law enforcement authorities to monitor vast numbers of people, this is considered a particularly severe intrusion into the private lives of a large part of the population. The legislator has therefore generally prohibited this practice but has provided three exceptions in which the use of such a system is permitted (see above 4.3.1).[92] However, one major point of criticism is the presumably easy circumvention of the ban on real-time remote biometric identification systems used in publicly accessible spaces for law enforcement purposes by the respective authority through one of the three exceptions stipulated in Article 5 (h) (i-iii). As Article 5 (h) already constitutes a rather narrow prohibition (e.g., including only law enforcement use), some critics perceive the exceptions to be too wide and to leave room for loopholes, possibly rendering the prohibition completely redundant.[93] However, it should be noted that all otherwise prohibited real-time RBI systems used by LEAs that are justified under the exceptions to Article 5 (h) are subject to an assessment of the impact on fundamental rights and the consequences for the affected people prior to the application of the system, as well as considerations on how to limit the application to what is strictly necessary in regard to the geographic scope and the period of usage.[94] Article 5 (h) (iii) AI Act reads as follows:

[The use of real-time RBI systems for law enforcement purposes is prohibited, except for] the localisation or identification of a person suspected of having committed a criminal offence, for

[91] Nathalie A Smuha and others, "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act" [2021] Social Science Research Network <https://doi.org/10.2139/ssrn.3899991>.
[92] Recital 32 AI Act.
[93] ARTICLE 19, `EU: AI Act Passed in Parliament Fails to Ban Harmful Biometric Technologies - ARTICLE 19´ (ARTICLE 19, March 13, 2024) <https://www.article19.org/resources/eu-ai-act-passed-in-parliament-fails-to-ban-harmful-biometric-technologies/> accessed 16 April 2024.
[94] Recital 34 AI Act.

the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

The exception covers a wide range of cases in which it may apply and thus, permit the use of possibly extensive public surveillance. As Annex II lists various offences such as armed robberies, environmental crimes, or the mere participation in a criminal organization involved in one or more crimes listed, the threshold for falling within the exception is not very high due to the fact that the only additional requirement is the maximum punishment of at least four years.[95] The legislator considers this requirement as assisting in narrowing the exception in order to justify otherwise prohibited use of RBI systems only in serious cases.[96] Pursuant, the demanded maximum sentence was increased from three to four years in contrast to the initial proposal.[97]

The European Data Protection Boards (EDPB) and the European Data Protection Supervisor (EDPS) critiqued the draft AI Act´s extent of regulation in a joint opinion, stating that remote biometric identification of individuals in publicly accessible spaces needs stricter governance. Their approach renders the distinction between post or real-time RBI irrelevant, as the impact on fundamental rights is not necessarily different. Correspondingly, the dissimilar treatment of law enforcement usage and other purposes such as private security is flawed as the intrusiveness of an FRT does not strictly dependent on its purpose. Furthermore, the third exception given in the proposed AI Act is deemed too vague and bound to render the prohibition inapplicable. Therefore, the EDPB and the EDPS suggest to outright ban the use of AI for the purpose of

[95] Nathalie A Smuha and others, "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act" [2021] Social Science Research Network <https://doi.org/10.2139/ssrn.3899991>.
[96] Recital 33 AI Act.
[97] Article 5 (1) (d) (iii) COM (2021) 206 final.

automated recognition of human features in publicly accessible spaces in any context.[98] Regardless, as of today, the wording of Article 5 (1) (d) "draft" AI Act ((h) in the corrigendum) has not seen significant changes[99] which indicates that the abovementioned opinion has not been incorporated by the legislator in this regard.

5.2 Consideration of technological issues

As mentioned above (3.2.1), the successful application of FRTs in publicly accessible spaces requires a high degree of accuracy in order to keep the error rates as low as possible and thus prevent e.g., false prosecutions or arrests.

The legislator addresses this issue by referring to the significant role and responsibility that lies upon such systems when they are in use, especially in the area of law enforcement, border control, asylum, and migration (which are all listed in Annex III) and emphasizing the importance of high quality training data and appropriate design for required performance.[100] The accuracy of AI systems and thus AI based FRTs is a prerequisite for the proper protection of fundamental rights when making use of FRTs, particularly in relation to people in vulnerable positions e.g., migrants looking for asylum.[101]

5.2.1 Accuracy and resilience

For the time of application, the AI Act thus provides complex rules to achieve accuracy, robustness, and cybersecurity levels in accordance with the requirements of the intended field of use. According to Article 15 (2) AI Act, the Commission shall promote the development of measuring and benchmarking methods to clearly define a way of measuring this metrics. This

[98] European Data Protection Board and European Data Protection Supervisor, `Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)´ (18 June 2021) <www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf> accessed 20 April 2024.
[99] Comparison of Article 5 (1) (h) COM(2021) 206 final and Article 5 (1) (h) of the current version of the AI Act.
[100] Recital 59 AI Act.
[101] Recital 60 AI Act.

is especially important regarding the assurance of an adequate level of accuracy for operation and fairness in commercial transactions between vendor and buyer of AI systems.[102]

In terms of resilience, AI systems have to be robust towards errors, unexpected events in their operating environment and, especially against attempts by unauthorized third parties aiming to influence the output of the system by exploiting its vulnerabilities (e.g., hacking).[103] The legislator suggests the implementation of so-called "fail-safe" plans to safely shut down the AI system if predetermined operating boundaries are crossed (see also 5.5) or other anomalies occur, since such events could affect the fundamental rights of individuals.[104]

5.2.2 Quality criteria for datasets

In consideration of the significant impact that the quality of training data has on the output of AI systems using learning techniques, Article 10 stipulates quality criteria that have to be met by such systems, in this context RBI systems. Appropriate data governance practices have to be adopted regarding the design of the AI system, the processes of data collection, the purpose, and the origin of the collected data[105] which might contribute transparency and the tracking of illicit data scraping as described below in 5.4. Furthermore, datasets have to be sufficiently representative, free from errors and complete with respect to the intended use i.e., regarding geographical, contextual, and functional aspects particular to the intended use.[106]

5.3 Evaluating bias problematics

One of the major concerns in the context of the use of FRTs is the abovementioned possibility of biased outputs by AI systems through e.g., wrongful training data which then can become the source of discrimination.

[102] Recital 74 AI Act.
[103] Article 15 (4-5) AI Act.
[104] Recital 75 AI Act.
[105] Article 10 (1-2) AI Act.
[106] Article 10 (3-4) AI Act.

Therefore, the AI Act enshrines in its Article 10 (2) (f) the need for examination of datasets in respect to possible biases which might affect fundamental rights or lead to discrimination. Special attention should be paid to so-called "feedback loops", where generated outputs by the AI system influence inputs and thus, might lead to the further amplification of bias.[107] Subsequently, appropriate measures to prevent future biases and to mitigate identified biases (referring to (f)) have to be adopted according to Article 10 (2) (g) Furthermore, the legislator enables the provider of an AI system to the exceptional processing of special categories of personal data (including biometric data according to Recital 54) for the purpose of anti-discrimination actions to eliminate bias. This may only be done if strictly necessary and under the application of the conditions laid down in Article 10 (5) (a-f) as well as those for the processing of personal data enshrined in the LED, the GDPR, and Regulation 2018/1725. The identification and correction of bias in AI systems is considered to be of substantial public interest.[108]

5.4 Privacy and Fundamental rights protection

As the AI Act acknowledges that certain AI systems possibly infringe fundamental rights of individuals and describes the enhancement of human well-being as the ultimate goal of AI,[109] it comes as no surprise that it provides various means of fundamental rights protection.

Article 27 AI Act obliges certain deployers of high-risk AI systems to carry out a fundamental rights impact assessment prior to putting it into service. Deployers that are bodies governed by public law as well as private entities providing public services fall within the provision. It also applies to real-time remote biometric identification systems in publicly accessible places for law enforcement purposes, which would normally be prohibited, if the use is permitted by one

[107] Recital 67 AI Act.
[108] Recital 70 AI Act.
[109] Recital 6 AI Act.

of the exceptions in Article 5 (1) (h) (i-iii) (see also 4.3.1).[110] Article 5 (2) thus refers to Article 27 regarding the extent of the impact assessment.

The aim of the fundamental rights impact assessment is to identify specific risks to the rights of individuals or groups of individuals likely to be affected and an evaluation of measures to be taken by the deployer if these risks materialize. Such measures could include, for example, complaint mechanisms or internal governance arrangements for human oversight. Furthermore, it shall take into account the process of usage by the deployer and the intended purpose, as well as describe the time period and frequency with which the system will be active.[111] The requirement to carry out a fundamental rights impact assessment only applies to the first use of the AI system. The deployer is permitted to rely on impact assessments previously conducted by other parties in similar cases or by the provider. If relevant aspects of the AI use, such as e.g., the affected group of persons or the timespan of application, are deemed to be outdated, the deployer has to actualize the information.[112]

The method of biometric database creation or expansion through untargeted scraping of facial images from CCTV footage or the internet constitutes a prohibited AI practice laid down in Article 5 (1) (e) AI Act. With this provision, the legislator intends to address the issue of personal privacy and violation of individuals´ fundamental rights, and might put a halt on shifty practices applied by AI system development companies such as Clearview AI or PimEyes, scraping hundreds of millions of facial images, labeled with the respective person´s name, from websites without the approval of the affected people.[113] This is aided by the obligation to provide detailed technical documentation before placing an AI system on the market, which has

[110] Article 5 (2) AI Act.
[111] Recital 96 AI Act.
[112] Article 27 (2) AI Act.
[113] Amba Kak, `Regulating Biometrics: Global Approaches and Open Questions´ (AI Now Institute 2020) <https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions>.

to include *inter alia* the information about the methods of obtaining training data and their origin.[114]

Another remedy for fundamental rights protection of individuals is the right to an explanation of individual decision-making enshrined in Article 86 AI Act. Where a person is subject to a decision made by a deployer, which is primarily based on the output of a high-risk AI system and has legal or similarly serious consequences that might impact fundamental rights of the concerned individual, one has the right to obtain a detailed and meaningful explanation regarding the role the AI system played in making the decision as well as the key elements of the decision.[115] At this point, it should be noted that according to Recital 53 AI Act, no decision that has an adverse legal effect for an individual is to be taken solely based on the output of a RBI system. The explanation has to constitute a sufficient base for exercising one's rights.[116] This provision might be especially relevant in the light of FRT use in publicly accessible spaces, since its scope seems to cover a wide variety of cases and thus, may enable large numbers of people to demand such an explanation.

Furthermore, natural, and legal persons are enabled to file a complaint with the market surveillance authority of their respective member state whenever there are reasonable grounds to believe that there has been an infringement of the AI Act. This provision applies without prejudice to the remedies provided by national law as well as other union law.[117]

5.5 Tackling the "function creep" phenomenon

Pursuant to the abovementioned critique concerning the exceptions to the prohibited AI practices regarding real-time RBI for law enforcement purposes, questions arise regarding the resulting ability for LEAs to implement facial recognition technologies into their surveillance

[114] Article 11 AI Act referring to Annex IV AI Act.
[115] Article 86 AI Act.
[116] Recital 171 AI Act.
[117] Article 85 AI Act, Recital 170 AI Act.

architecture. Since real-time RBI system use for law enforcement purposes is not completely prohibited, the technical components necessary for application of these practices are likely to be installed on a large scale due to the possibility of an exceptional permitted use. This renders the concern about the gradual enlargement of the systems field of operation even more serious because individuals cannot be sure whether the system is in operation or not whenever they are exposed to it.[118] Based on that, one could argue that the AI Act in its current state does not sufficiently discuss the issue of "function creep" regarding the use of facial recognition technology in publicly accessible spaces. However, it has to be taken into consideration that the respective provisions in the AI Act constitute a minimum set requirement for member states, which can be expanded anytime to guarantee greater protection of privacy and fundamental rights.[119]

6. Glance into the future

6.1 Recent and foreseeable developments

Due to recent noteworthy achievements in the tech sector, especially in computer performance and vision, biometric identifiers and artificial intelligence, the use of FRTs will continue to evolve and expand into many more areas of life. New fields of application might be personalized advertising, gaming or above all, healthcare, and medical diagnostics. Researchers in this field are evaluating possibilities to use FRTs for early detection of multiple illnesses such as Parkinson's disease. Additionally, new technological possibilities and trends such as so-called "multimodal biometrics" emerge, which allow more accurate and precise facial recognition, particularly for public surveillance.[120] Multimodal biometrics consolidate more

[118] Nathalie A Smuha and others, `How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act´ [2021] Social Science Research Network <https://doi.org/10.2139/ssrn.3899991>.
[119] Phillip Hacker, `Comments on the Final Trilogue Version of the AI Act´ (European New School, 23 January 2024) <https://www.europeannewschool.eu/images/chairs/hacker/Comments%20on%20the%20AI%20Act.pdf> accessed 22 April 2024.
[120] Faslul Haq Fathima Nasu Sahana and Nadeeka Dissanayake, `Navigating the Ethical and Technological Landscape: The Future Trajectory of Facial Recognition Technology´ (2024) 3 International Journal of

than one biometric characteristic in order to identify an individual and thus achieve higher levels of accuracy. What is very promising is the combination of the face and the ear, due to the fact that the ear is a 3D structure which almost remains unchanged despite aging and different facial expressions. Furthermore, biometric information regarding face and ear can be collected without intrusive measures e.g., using CCTV cameras, rendering it a highly attractive opportunity for advanced surveillance.[121]

6.2 AI Act, fit for the future?

At the time of writing the AI Act has not entered into force so it is not yet clear to what extent its contents are capable of meeting the goals it aims to achieve. However, stakeholders and experts already expressed their doubts about the lack of flexibility and adaptability as well as the fact that the level of fundamental rights protection is not up to date. The biggest problem the union legislator is facing in terms of sustainable regulation within the field of AI is to keep pace with the forthcoming rapid technological progress, which has already been witnessed in the past years. The AI Act reacts to this problematic, for instance, through the possibility of fast modification of most of the annexes through delegated acts by the commission (see also 4.3.2). The legislator tried to strike the balance between sufficiently rigid provisions and adequate vagueness in order to leave room for interpretation in court.[122]

According to Laura Caroli, who is the senior policy advisor to MEP Brando Benifei in the European Parliament and led negotiations on technical aspects of the AI Act, the regulation has one flaw which could jeopardize its implementation. The categorization of AI systems into the risk categories which subsequently trigger the legal consequences, is made dependent on the

Agrobiotechnology and Veterinary Medicine <https://sciencebox.uz/index.php/tibbiyot/article/view/9948/9083> accessed on 20th April 2024.

[121] Yichao Ma and others, `An Overview of Multimodal Biometrics Using the Face and Ear´ (2020) 2020 Mathematical Problems in Engineering 1 <https://doi.org/10.1155/2020/6802905>.

[122] Laura Caroli, `Will the EU AI Act Work? Lessons Learned from Past Legislative Initiatives, Future Challenges´ International Association of Privacy Professionals (April 17, 2024) <https://iapp.org/news/a/will-the-eu-ai-act-work-lessons-learned-from-past-legislative-initiatives-future-challenges/> accessed on 20th April 2024.

intended use. Only a few systems have a certain single case of use, providers can easily circumvent the regulation by claiming that their AI system is not intended to be used for a purpose listed in the AI Act. This emphasis is not well-suited for complex technologies such as AI.[123]

6.3 International comparison

Facial recognition technology regulation is a contemporary issue not only in Europe, but also all across the globe, so the following section takes a brief look beyond EU borders at selected jurisdictions.

At the time of writing, there are no laws in the United States that regulate the use of FRTs in publicly accessible spaces at a federal level. However, some individual states have passed legislation on this issue, for example California or Illinois. These laws primarily regulate the use in the private sector. In contrast, cities like San Francsico or Oakland have already imposed full-on bans on FRT use in the public sector. Recently, the U.S. Senate has debated over the "Facial Recognition Technology Warrant Act" which obliged law enforcement authorities to obtain a warrant from a judicial authority before using FRTs for surveillance purposes[124] comparable to the prerequisite of approval to make use of an exception from the general prohibition of real-time RBI in public by LEAs under the AI Act (see above 4.3.1). The bill focuses on regulation of the public sector and has been accompanied by the "Ethical Use of Facial Recognition Act", introduced to the senate in 2020, which aims to restrict the use of FRT by government institutions until an appropriate ruleset is adopted.[125]

In China, the steadily growing, excessive use of FRT over the last decades has raised concerns among individuals about privacy and protection of their sensitive personal data. In 2019, the

[123] Ibid.
[124] Wenhao Chen and Min Wang, `Regulating the Use of Facial Recognition Technology across Borders: A Comparative Case Analysis of the European Union, the United States, and China´ (2023) 47 Telecommunications Policy 102482 <https://doi.org/10.1016/j.telpol.2022.102482>.
[125] Ibid.

first case regarding FRT abuse was brought before a Chinese court by an individual accusing an amusement park of biometrical data collection through a facial recognition system. The proceedings raised awareness among citizens on the lack of regulation regarding these technologies. Subsequently, China issued the "Personal Information Protection Law (PIPL)" in 2021 which is its first comprehensive piece of legislation to explicitly govern the use of FRTs in public places.[126] In its Article 26, the PIPL stipulates that in case of FRT use in publicly accessible places, the installation of these systems shall be in accordance with other state regulations, clearly indicated by signs and the biometric data collected might only be used for safeguarding public security. Otherwise, explicit consent for the collection of biometric data has to be obtained separately of each individual.[127]

[126] Ibid.

[127]Rogier Creemer and Graham Webster, `Translation: Personal Information Protection Law of the People's Republic of China - Effective Nov. 1, 2021 – DigiChina´ (DigiChina, January 5, 2022) <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/> accessed on 19th April 2024.

7. Concluding remarks

Considering the rapid technological developments of the 21st century as well as the current and prospective use of AI, especially in improving facial recognition technologies for surveillance purposes, the AI Act comes just in time to address some of the key issues in this area of technology. Despite being extensively criticized, the AI Act constitutes a pioneering legal framework tackling an area of legal and ethical problematics that have not yet been fully researched. Time will tell if the risk-based approach provides a sufficient basis for categorizing and subsequently regulating both FRT and AI due to the sheer unlimited possibilities of application. The Commission's ability to quickly amend Annex III and subsequently widen the scope of the high-risk provisions is a great way to react to the rapid developments in the tech sector.

The application of facial recognition technologies in publicly accessible spaces leads to problems with regard to privacy, fundamental rights, and nondiscrimination. The prohibition of untargeted scraping of facial images from the internet will force companies to find new approaches of database creation and liberate individuals from the feeling of losing control over their pictures uploaded to the internet. The AI Act governs the FRT practices most intrusive to fundamental rights but does not go as far as to ban them in their entirety in contrast to the recommendations of the EDPB and EDPS, issued before the presumably final text was adopted by the European Parliament. Concerning the ban on utilizing real-time remote RBI in publicly accessible spaces for law enforcement purposes, its exemptions seem too broad for the provision to have a sufficient impact on LEAs and for making them refrain from this practice. Therefore, the demand for stricter regulation in this regard will not cease even after the AI Act enters into force and member states might implement superseding prohibitions surpassing the level of fundamental rights protection.

Nevertheless, the AI Act provides well needed guidance in an otherwise, at least partial, legislative void concerning AI and facial recognition. It addresses the significant issues of bias in AI, the need for accurate and robust FRTs for an implementation of biometrics into public surveillance without discrimination as well as the impact FRTs in surveillance have on the fundamental rights of the population. Remedies for individuals like the right to file a complaint or to obtain an explanation are established to protect their rights. The legislator is herewith taking important steps towards governing the variety of issues emerging by FRT usage.

What is more, the AI Act attempts to provide comprehensive, usually difficult to understand definitions that can serve a reference for further legislation in the field of AI and facial recognition. Globally, the AI Act is a forerunner in its area of application and is likely to influence other jurisdictions in their future legislation.

To sum up, the AI Act appears to miss the chance of banning the use of facial recognition technologies in publicly accessible spaces as a whole. However it provides a good starting point in facing this emerging world of legal challenges.

8. Bibliography

Akerkar R, *Introduction to Artificial Intelligence* (PHI Learning Pvt Ltd 2014)

Amnesty International, `EU: Artificial Intelligence Rulebook Fails to Stop Proliferation of Abusive Technologies´ (Amnesty International, March 14, 2024) <www.amnesty.org/en/latest/news/2024/03/eu-artificial-intelligence-rulebook-fails-to-stop-proliferation-of-abusive-technologies/> accessed on 15 April 2024

Andrejevic M and Selwyn N, *Facial Recognition* (John Wiley & Sons 2022)

ARTICLE 19, `EU: AI Act Passed in Parliament Fails to Ban Harmful Biometric Technologies´ (ARTICLE 19, March 13, 2024) <www.article19.org/resources/eu-ai-act-passed-in-parliament-fails-to-ban-harmful-biometric-technologies/> accessed 15 April 2024

Brey PAE, `Ethical Aspects of Facial Recognition Systems in Public Places´ (2004) 2 Journal of Information, Communication and Ethics in Society 97 <https://doi.org/10.1108/14779960480000246>

Bucher T, "Facing AI: Conceptualizing 'fAIce Communication´ as the Modus Operandi of Facial Recognition Systems" (2022) 44 Media, Culture & Society 638

Caroli L, `Will the EU AI Act Work? Lessons Learned from Past Legislative Initiatives, Future Challenges´ International Association of Privacy Professionals (April 17, 2024) <https://iapp.org/news/a/will-the-eu-ai-act-work-lessons-learned-from-past-legislative-initiatives-future-challenges/> accessed on 19 April 2024

Charter of Fundamental Rights of the European Union [2012] OJ C 326/391

Chen W and Wang M, `Regulating the Use of Facial Recognition Technology across Borders: A Comparative Case Analysis of the European Union, the United States, and China´ (2023) 47 Telecommunications Policy 102482 <https://doi.org/10.1016/j.telpol.2022.102482>

Christakis T, Becuywe M, and AI-Regulation Team, `Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021´ (2021) <https://ai-regulation.com/wp-content/uploads/2021/05/Final-Report-26-04.pdf>

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended by Protocols Nos. 11 and 14) (ECHR)

Creemer R, Webster G, `Translation: Personal Information Protection Law of the People's Republic of China - Effective Nov. 1, 2021 – DigiChina′ (DigiChina, January 5, 2022) <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/> accessed on 19 April 2024

Directorate-General for Communications Networks, Content and Technology, `AI Act′ (Shaping Europe's Digital Future, March 1, 2024) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed on 17 March 2024

European Commission, `Laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts′ (Impact Assessment) SWD (2021) 84 final

European Commission, `On Artificial Intelligence - A European approach to excellence and trust′ (White Paper) COM (2020) 65 final

European Commission, `Proposal for a regulation of the European parliament and of the council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts′ COM (2021) 206 final

European Data Protection Board and European Data Protection Supervisor, `Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)′ (18 June 2021) <www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf> accessed 20 April 2024

European Parliament, `Use of facial recognition technology for migrant disembarkation in Italy′ (Parliamentary Question) E-002182/2021

Fontes C and Perrone C, `Ethics of Surveillance: Harnessing the Use of Live Facial Recognition Technologies in Public Spaces for Law Enforcement′ (Technical University of Munich, 2021) <https://ieai.sot.tum.de/wp-content/uploads/2021/12/ResearchBrief_December_Fontes-1.pdf> accessed 22 April 2024

Future of Life Institute, `The Act Texts′ (Future of Life Institute, 2024) <https://artificialintelligenceact.eu/the-act/> accessed 24 April 2024

Gates KA, Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance (NYU Press 2011)

Hacker P, `Comments on the Final Trilogue Version of the AI Act′ (European New School, 23 January 2024)

<www.europeannewschool.eu/images/chairs/hacker/Comments%20on%20the%20AI%20Act.pdf> accessed 22 April 2024

Hodge Jr SD, `The Legal and Ethical Considerations of Facial Recognition Technology in the Business Sector´ (2022) DePaul Law Review 731

Jasserand C, `The Future AI Act and Facial Recognition Technologies in Public Spaces´ (2023) 9 European Data Protection Law Review 430 <https://doi.org/10.21552/edpl/2023/4/9>

Kak A, `Regulating Biometrics: Global Approaches and Open Questions´ (AI Now Institute 2020) <https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions>

Ma Y and others, `An Overview of Multimodal Biometrics Using the Face and Ear´ (2020) 2020 Mathematical Problems in Engineering 1 <https://doi.org/10.1155/2020/6802905>

Madiega T and Mildebrath H, *Regulating facial recognition in the EU* (European Parliamentary Research Service 2021)

Mobilio G, `Your Face Is Not New to Me – Regulating the Surveillance Power of Facial Recognition Technologies´ (2023) 12 Internet policy review <http://dx.doi.org/10.14763/2023.1.1699>

Publications Office of the European Union, `Procedure 2021/0106/COD´ <https://eur-lex.europa.eu/procedure/EN/2021_106> accessed 26 March 2024

Ruschemeier H, `AI as a Challenge for Legal Regulation – the Scope of Application of the Artificial Intelligence Act Proposal´ (2023) 23 ERA Forum 361 <https://doi.org/10.1007/s12027-022-00725-6>

Russell SJ, Norvig P and Davis E, *Artificial Intelligence: A Modern Approach* (Prentice Hall 2010)

Sahana F and Dissanayake N, `Navigating the Ethical and Technological Landscape: The Future Trajectory of Facial Recognition Technology´ (2024) 3 International Journal of Agrobiotechnology and Veterinary Medicine <https://sciencebox.uz/index.php/tibbiyot/article/view/9948/9083>

Smuha NA and others, `How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act´ [2021] Social Science Research Network <https://doi.org/10.2139/ssrn.3899991>

Thorat S, Nayak S and Dandale JP, `Facial Recognition Technology: An analysis with scope in India´ (2010) 8 IJCSIS 325

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) UN Doc A/HRC/44/24

Wechsler H, *Reliable Face Recognition Methods: System Design, Implementation and Evaluation* (Springer Science & Business Media 2009)