NEW LEGAL FRAMEWORK FOR AI-BASED FACIAL RECOGNITION

Jonas Pfister / Jessica Fleisch / Jakob Zanol

Jonas Pfister, Researcher, University of Vienna, Centre for Computers and Law
Schottenbastei 10–16/2/5, 1010 Wien, AT
jonas.pfister@univie.ac.at; http://rechtsinformatik.univie.ac.at

Jessica Fleisch, Researcher, University of Vienna, Centre for Computers and Law
Schottenbastei 10–16/2/5, 1010 Wien, AT
Jessica.fleisch@univie.ac.at; http://rechtsinformatik.univie.ac.at

Jakob Zanol, Researcher, University of Vienna, Centre for Computers and Law
Schottenbastei 10–16/2/5, 1010 Wien, AT
jakob.zanol@univie.ac.at; http://rechtsinformatik.univie.ac.at

Schlagworte: ***Artificial Intelligence, AI, Face Recognition, Artificial Intelligence Act***

Abstract: *In 2021 the European Commission proposed a new framework for Artificial Intelligence made in Europe. Within the consortium of the XAIface project, which aims to analyze the legal and ethical framework for AI-based Facial Recognition (FRT), the team at University at Vienna dissect the new proposals and demonstrates their implications for FRTs. The following article will examine selected provisions of the proposal for an AI-Act.*

1. Introduction

The use of AI-based Facial Recognition (hereinafter "FRT") is widespread. Use cases range from security systems of private companies to law enforcement – or simply unlocking your phone display. The aim of FRT is to authenticate or identify a person.[1] For some, FRTs are emblematic of a dystopian surveillance state and therefore prohibited in certain cities.[2] The most controversial use cases are related to publicly accessible spaces. They can range from practical, such as replacing boarding cards at the airport, to impractical, such as being necessary for access to toilet paper.[3] *Heldt* argued that part of the reason, why the topic is so controversial, is the lack of regulation of the matter.[4] However, this is about to change. With the new proposals for AI regulation of the European Commission, European secondary law will also specifically address FRTs. In the following analysis, the authors will analyze parts of the proposed legal framework, which consists of the AI-Act[5], the AI liability directive[6] and the amendments to the product liability directive[7]. The new framework will therefore include a regulation on product safety (AI-Act) as well as new liability norms for such products. The AI-Act will even directly address FRTs, which will be the focal point of the analysis.

---

1 EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf (accessed on 04.10.2022) p. 1.

2 Hemmert-Halswick, Neue Face Recognition App „Clearview AI" MMR-Aktuell 2020, p. 425644.

3 Heldt, Gesichtserkennung: Schlüssel oder Spitzel? Einsatz intelligenter Gesichtserfassungssysteme im öffentlichen Raum, MMR 2019, p. 285.

4 Ibidem.

5 COM (EU) Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM 2021/0106 206 final. ["AI-Act proposal"].

6 COM (EU) Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) COM 2022/0303 496 final.

7 COM (EU) Proposal for a Directive of the European Parliament and of the Council on liability for defective products (AI Liability Directive) COM 2022/0303 495 final.

1.1. XAIface and FRTs

This analysis is based on interim results of the project XAIface, in which the authors analyze the legal and ethical framework of the use of AI-based FRTs.[8] The goal of the project is to increase the level of trust and social acceptance of face recognition technology. The XAIface consortium aims to better the understanding of the underlying mechanisms in face recognition based on machine learning in general and deep learning in particular. The consortium studies the impact of influencing factors and tries to explain their role in the overall performance of a system. Further desired outcomes include the creation of guidelines for the legal and ethical use of FRTs, which will include the new requirements of the AI-Act and parts of the new liability regime.

2. Proposal for the AI-Act

FRTs currently seem to be a thorn in the flesh for data protection authorities. The Canadian[9], Australian, French and UK[10] data protection authorities already ordered the controllers of the system to cease the data processing in question.[11] Recently, the Italian data protection authority followed suit. Likewise, the Greek data protection authority imposed a fine on the controller amounting to 20 million Euros.[12] Italy now even went a step further and completely banned FRTs except for judicial purposes and crime prevention, even though further exemptions are to be expected.[13] Within the institutions of the EU, several groups have even called for a ban of FRTs.[14] Although the European Commission did not go as far as to outright outlaw FRTs, the AI-Act proposal specifically addresses FRTs and bans certain use cases of said technology.

2.1. Scope

Like the GDPR[15], the AI-Act proposal does not only apply to the Member States of the European Union. If the FRT system is put into service in the European Union, the AI-Act will apply, regardless of where the provider is established. Similarly, the regulation may apply to users and providers if *"the output produced by the system is used in the Union"*[16]. Naturally, it also applies to any user within the European Union.

A provider in the sense of the AI-Act proposal, is someone who develops a system or lets someone else develop a system to place it on the market under their own name or trademark.[17] It should be noted that no distinction is made between public or private entities. The definition of a user contains something akin to a "household exception". The definition does not apply to any activities outside of a professional setting. Hence, the private usage of FRT, for example on a private smartphone, will not fall within the scope. Similar delimitation problems to Art. 2 par 2 lit. c GDPR may arise.[18] *Geminn* argues, that it should be evaluated if any

8 For more detailed information see: https://xaiface.eurecom.fr.

9 Kanada: Datenschutzbehörde wirft Clearview illegale Massenüberwachung vor, ZD-Aktuell 2021, p. 5045.

10 Strauch, UK: ICO Fines Clearview AI Facial Recognition Company for Breaches of Data Protection Law, ZD-Aktuell 2022, p. 1299.

11 Qasim, Italien: Kein Freifahrtschein für Gesichtserkennungssoftware – Bußgeld iHv 20 Mio. EUR gegen Clearview AI, ZD-Aktuell 2022, p. 1144.

12 Etteldorf, Griechenland: 20 Mio. EUR Bußgeld gegen Clearview AI, ZD-Aktuell 2022, p. 1275; Datenschutzbehörde Italien: Einstweilige Verfügung gegen Clearview AI, ZD-Aktuell 2022, p. 1090.

13 Reuters, Italy outlaws facial recognition tech, except to fight crime, 14.11.2022, Italy outlaws facial recognition tech, except to fight crime | Reuters.

14 For details see EPRS, Regulating facial recognition in the EU (2021) p. 23.

15 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 (General Data Protection Regulation), OJ L 119/1.

16 Art. 1 par. 1 lit. c AI-Act proposal.

17 Art. 3 cif. 2 AI-Act proposal.

18 Kuner, Bygrave, Docksey, Drechsler, The EU General Data Protection Regulation (GDPR), Oxford 2020, Art. 2 par 2.

private use cases of FRTs couldn't also be deemed an unacceptable risk.[19] If FRTs are specifically designed for military purposes, the proposal will not apply.[20] Furthermore, the regulation will not apply to third country public authorities or international regulations, where certain agreements are in place for law enforcement and judicial cooperation. In similar cases to Clearview AI, where the system is used by US law enforcement services, this could result in application to the provider, but not to the user. The provisions are criticized for being unclear, especially with regard to Software-as-a-Service solutions[21], which is a potential scenario for FRTs.

The material scope is defined by the term "artificial intelligence system"[22]. Definitions of Artificial Intelligence used in other disciplines do not necessarily coincide with this specific legal definition.[23] The current definition in the proposal, however, will undoubtedly be satisfied by FRTs. The first criterion a system must satisfy is "software", which won't really lead to much differentiation, since all FRTs are software. The system must be developed with one of the techniques or approaches listed in Annex I[24], which is rather far-reaching.[25] Since FRTs are usually based on machine learning, specifically deep learning in some cases[26], the criterion is also fulfilled. Furthermore, the system must have human defined objectives and generate outputs such as content, predictions or decisions, which in turn must influence the environments they interact with.

The other criteria shall be demonstrated by a hypothetical scenario[27]:

> An Austrian enterprise installs a security system on their premises including 'smart' cameras. The cameras conduct facial scans and references them in a database. The output of the system is the (non-)identification of a specific person. The output can already be considered a decision if no further human intervention is envisaged. ('This is person A' = identification) This decision prevents certain persons on a blacklist from gaining access to a building by automatically locking a door or keeping said door locked and alerting security. The system influenced the environment. (Locked door, alerted security) The human-defined goal for the system was to provide security by identifying people and preventing some of them from entering.

Whether an event must have an effect to be considered a decision, is currently an open question.[28] Bomhard/Merkle highlight the complex relationship with the territorial scope, if outputs are produced and reused in the EU.[29]

It can be argued that the term environment[30] includes humans, such as security staff. This interpretation is mainly derived from the usage of the word 'recommendation' in the definition, which by nature is usually directed solely towards a human counterpart.

---

19 Geminn, Die Regulierung Künstlicher Intelligenz, ZD 2021, p. 356.

20 Art. 1 par. 3. AI-Act proposal.

21 Bomhard/Merkle, Regulation of Artificial Intelligence, EuCML 2021, p. 257.

22 Art. 3 cif. 1 AI-Act proposal.

23 See Norvig/Russell, Artificial Intelligence: A Modern Approach, Global Edition[4] (2021).

24 Annex I of the AI-Act proposal does not only include machine learning but also logic and knowledge-based approaches (p.ex.: expert systems) and generally statistical approaches.

25 Bomhard/Merkle, Regulation of Artificial Intelligence, EuCML 2021, p. 258.

26 See Hu, Yang, Yi, Kittler, Christmas, Li, Hospedales, When Face Recognition Meets with Deep Learning: an Evaluation of Convolutional Neural Networks for Face Recognition, Proceedings of the IEEE International Conference on Computer Vision (ICCV) Workshops, 2015, pp. 142–150.

27 This example is a part of the unpublished draft of Legal Guidelines Deliverable v.1. of the XAIface project.

28 See for example the problems of defining what constitutes a decision within the framework of Art. 22 par. 1 GDPR; Similarly see for the problems with the word "action" and "decision" Wendehorst, The Proposal for an Artificial Intelligence Act COM (2021) 206 from a Consumer Policy Perspective (2021), p. 102.

29 Bomhard/Merkle, Regulation of Artificial Intelligence, EuCML 2021, p. 258.

30 Kalbhenn argues, that influencing an environment could be interpreted as the distinguishing factor to "normal" software, see Kalbhenn, Designvorgaben für Chatbots, Deepfakes und Emotionserkennungssysteme: Der Vorschlag der Europäischen Kommission zu einer KI-VO als Erweiterung der medienrechtlichen Plattformregulierung, ZUM 2021, p. 663.

2.2. Prohibitions

Some FRTs will have to fulfill special obligations under the AI-Act and will – a priori – be prohibited, which is a direct result of the risk-based approach.[31] The common denominator of the relevant definitions in the AI-Act proposal is the term "biometric data"[32], which is identical to the definition in the GDPR.[33] This choice leads to the conclusion, that the same interpretation should be applied. Hence, the definition is intrinsically linked to the unique identification of a natural person and special technical procedures. Therefore, if the data processing is not linked those aspects, the definition does not apply.[34] Not every AI-system that processes images therefore falls within the scope of one of these prohibitions, since the processing of images would at least have to be linked to identification efforts.[35] A simple face detection system, for example, will therefore not fall under these provisions in the AI-Act proposal.

The first listed technology based on biometric data is an "emotion recognition system", which refers to "an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data."[36] This technology does not fall within the typical definition of FRTs[37] and is therefore not covered by the XAIface project. Due to similar inherent risks, however, this specific application will also be covered by the AI-Act.

A "biometric categorisation system" refers to "an AI system for 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".[38,39] The system does not identify or authenticate any natural person, but rather categorizes them based on chosen criteria inherent to their biometry. Like the emotion recognition system, this is not a typical FRT use case.

The typical use cases are covered by the term "remote biometric identification system", which refers to "an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified".[40]

Two different variations of these remote biometric identification systems exist, separated by a temporal component:

a) "Real-time remote biometric identification system": "a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention."[41]

b) "Post remote biometric identification system": "a remote biometric identification system other than a 'real-time' remote biometric identification system."[42]

---

31 The associated risks, especially with regard to law enforcement are intrusive and severe interferences with rights and freedoms, especially the right to a private life and could have a "chilling effect", see EPRS, Regulating facial recognition in the EU (2021) p. 25, 28.

32 Art. 3 cif. 33 AI-Act proposal.

33 Art. 4 cif. 14 GDPR:

34 See Kindt, A First Attempt at Regulating Biometric Data in the European Union, Regulating Biometrics: Global Approaches and Urgent Questions, p. 62.

35 See Rec. 51 GDPR., EDPB, Guidelines 3/2019 on Processing of Personal Data through Video Devices, on Video Surveillance, January 29, 2020, § 74 ("EDPB Guidelines 3/2019 on video devices").

36 Art. 4 cif. 34 AI-Act proposal.

37 EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf (accessed on 04.10.2022) 1.

38 Art. 4 cif. 35 AI-Act proposal.

39 For examples see Wendehorst, The Proposal for an Artificial Intelligence Act COM (2021) 206 from a Consumer Policy Perspective (2021), p. 100.

40 Art. 4 cif. 36 AI-Act proposal.

41 Art. 4 cif. 37 AI-Act proposal.

42 Art. 4 cif. 38 AI-Act proposal.

Art. 5 par 1 lit. d AI-Act proposal specifically prohibits the use of real-time remote biometric identification, but only for publicly accessible spaces and only for the purposes of law enforcement. A publicly accessible space is defined as "*any physical place accessible to the public, regardless of whether certain conditions for access may apply*".[43] Generally, we argue for a broad interpretation of the term "publicly accessible", which can be seen in the following example[44]. Wendehorst links the definition of publicly accessible spaces to the potential, that an indefinite number of persons enters the space, which seems appropriate.[45]

> A public university provides space for leisure, learning, meetings and sports activities on their own campus. The area is partially open-air, partially indoors and surrounded by a large fence.
>
> In order to gain access, one must provide either a student or staff license or a visitor's pass. On a daily basis hundreds of students and visitors frequent the area.
>
> Locations such as this university campus may be considered "publicly accessible", even if one might need to be a student, staff or a registered visitor to enter it.

Even for law enforcement purposes, the use of real-time remote biometric identification may be allowed, if public interests outweigh the risks. The European Commission, however, anticipates the weighing of interests[46] and only allows the use for example for the search for missing children, prevention of terrorist acts or similar threats or the detection, localization, identification or prosecution of specific serious crimes, as demonstrated by example 3[47,48]:

> At 06:30h local time, the Dutch police receive a credible and concrete threat and a tip from Europol, that a person is planning to shoot random passengers at Amsterdam Central Station at 08:30. Documents of the potential shooter are stored in the Europol Information System (EIS). It is currently rush hour at Amsterdam Central Station and the police do not want to cause a panic, but rather identify and apprehend the potential shooter before any harm is caused. Alarming the potential shooter by sending multiple squads in to comb the area could result in him opening fire. Fortunately, the station is equipped with multiple video cameras. The police run a scan of the live feeds and cross reference with the biometric data stored in the Europol database. The potential perpetrator is identified by the system and apprehended. The operation ends, the system is deactivated.

It should be noted that the use of the system is not legitimized by the provision in the proposal of the AI-Act. The public authorities still must comply with the respective national laws and the respective European data protection law.[49,50] However, since there was a substantial (death or bodily harm) and imminent (within the next one or two hours) threat to the life or physical safety of natural persons or (depending on the motivation) a terrorist attack and the crime could be prevented, the exemption may apply, if the use cases passes the strict

43 Art. 3 cif. 39 AI-Act proposal.

44 This example is a part of the unpublished draft of Legal Guidelines Deliverable v.1. of the XAIface project.

45 Wendehorst, The Proposal for an Artificial Intelligence Act COM (2021) 206 from a Consumer Policy Perspective (2021), p. 88.

46 Since some applications are deemed an unacceptable risk, see Kalbhenn, Designvorgaben für Chatbots, Deepfakes und Emotionserkennungssysteme: Der Vorschlag der Europäischen Kommission zu einer KI-VO als Erweiterung der medienrechtlichen Plattformregulierung, ZUM 2021, p. 663.

47 This example is a part of the unpublished draft of Legal Guidelines Deliverable v.1. of the XAIface project.

48 For a similar example see Wendehorst, The Proposal for an Artificial Intelligence Act COM (2021) 206 from a Consumer Policy Perspective (2021), p. 91.

49 See for the discussion in Germany Mysegades, Keine staatliche Gesichtserkennung ohne Spezial-Rechtsgrundlage NVwZ 2020, p. 852.

50 Furthermore, it is up to the Member States to make use of these exceptions, see EPRS, Regulating facial recognition in the EU (2021) p. 26.

necessity test required by the provision. For the necessity test, arguments may be based on harm avoided by the system vs probability, scale and seriousness of human rights infringements.[51]

The necessity could arguably be based on the fact, that no alternatives with the same outcome and lower risk to the people were available. But even if the strict necessity test is passed, further restrictions apply. In addition to necessity, the use case must be proportionate, which will mainly be achieved by specific safeguards. The relevant safeguards for example 3 can be summarized as follows:

a) The system is not used without prior cause. The cause is a tip from Europol and a credible and concrete threat.[52]
b) Geographical limitation: The system is only used within the station, the area of the potential crime, not in the whole city.
c) Temporal limitation: The system is only used until the suspect is apprehended.
d) Personal limitation: The system is only scans people within the station and references specific database entries.

While these tests are generally a good measure of proportionality, Ebers. et al. argue, that the provision which detection, localization, identification, or prosecution of certain crimes is to broad, since it includes crimes with comparably short prison sentences (3 years).[53, 54]

The proposal also limits the usage of facial recognitions systems further by demanding "prior authorization granted by a judicial authority or by an independent administrative authority of the Member State".[55] An exception can be made in case of urgency. Authorization may then be requested post factum.

As such, the articles already provide solid guidance for the use of FRT for the purposes of law enforcement. The exemptions still allow for a wide range of use cases, but again, the use of FRT must also comply with national and other European laws. Generally, the use of FRT for law enforcement without special cause will infringe data protection law.[56] As noted by the European Economic and Social Committee, the prohibition does not cover "post" and "near" biometric FRTs or biometric systems which don't identify natural persons.[57]

While some authors recognize that these provisions impose serious requirements[58], not everybody agrees that the provisions provide an appropriate test of necessity and proportionality. The EDPS and EDPB rather argue in a joint opinion, that automated biometric recognition in public spaces should be prohibited entirely due to the high risk the use case poses for fundamental rights.[59] Furthermore, these provisions only apply to law enforcement, while private use cases may still be problematic. Ebers et al. even go so far as to argue, that all of these systems, whether used by private or public actors, should be prohibited.[60] The total prohibition should include ex post identification. The aim would be to prevent a priori mass surveillance. They argue, and in my opinion for good reason, that the fear of being identified by itself has already a restricting effect.

---

51 See Art. 5 par. 2 AI-Act proposal.

52 See also Geminn, Die Regulierung Künstlicher Intelligenz, ZD 2021, p. 356.

53 Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter, Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf, RDi 2021, p. 528 (531).

54 Similarly: EPRS, Regulating facial recognition in the EU (2021) p. 29.

55 Art. 5 par. 3 Proposal for the AI-Act.

56 See ECJ, 8.04.2013, C-293/12 and C-594/12 ('Digital Rights Ireland').

57 European Economic and Social Committee, Opinion AI/Regulation – Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM (2021) 206 final – 2021/106 (COD)] INT/940 (2021) p. 5.

58 Bomhard/Merkle, Regulation of Artificial Intelligence, EuCML 2021, p. 259.

59 EDPB/EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (2021).

60 Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter, Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf, RDi 2021, p. 528 (531).

Additionally, it should be noted, that Wendehorst specifically distinguishes between identification and authentication. Where authentication is a one-to-one relationship and the natural person claims to have an identity, identification is a one-to-many relationship. If the system tests, if the person is one of many and the person does not claim a specific identity, the definition is fulfilled. Therefore, authentication methods for securing buildings usually don't fall within the prohibition.[61] She also argues, that the limitation of the prohibition to 'real'-time identification does not take into account the potential threat of ex post identification to fundamental rights.[62] This argument is generally convincing. On a similar note, the EPRS noted that the distinction between 'real-time' and 'post' remote identification systems risks being arbitrary.[63]

Geminn argues, that due to the lack of real categorical prohibitions, the creation auf an AI-based surveillance infrastructure remains possible.[64]

2.3. Classifications & Dealing with Bias

If a system is not prohibited, it will likely be classified as high-risk according to article 6 of the proposal and will therefore have to comply with further requirements. The classification is essentially based on two options. Either the system is covered by certain legislation[65], which concerns for example machines or medical products, or it is covered by Annex III of the AI-Act proposal. The main problem with this type of classification is, that the assessment will be conducted by the providers of the AI-systems. Risk of a certain technology, however, can only be evaluated based on its specific use case, which the provider won't always be able to anticipate.[66] One of the cases described in Annex III is the use of biometric identification and categorisation of natural persons, specifically those systems intended for real-time and post remote biometric identification of natural persons.[67] Even though the provision states, that AI-systems must be intended for the 'real-time' *and* 'post' remote biometric identification of natural persons, it is clearly the intention of the proposal to categorize a system as high-risk if it fulfills one of those criteria. The provision may be changed in the future. It's noteworthy that this provision is not the only possible way FRTs can fall within the high-risk category[68], even though it's the explicit one. However, if one is to follow Wendehorst's previously mentioned opinion on the strict distinction between authentication and identification, typical entrance security examples will still not be covered, even if they pose significant risks of surveillance to – for example – employees.[69]

As mentioned, the result of the classification is the obligation to comply with further requirements. One of these is set out in Art. 10 AI-Act proposal and concerns data governance. The provision generally concerns the usage of data for training, validation and testing. Providers of AI-systems must employ various data governance and management practices, which are partially not unlike those set out in data protection law.[70] The provision also requires providers to examine potential biases, which is a known issue for FRTs.[71] One provision should especially be highlighted. Paragraph 3 postulates the requirement, that all mentioned data sets "*shall be relevant, representative, free of errors and complete".* The interpretation of this clause is subject to academic debate. It is especially questionable, what the termini "free of errors" are supposed to encapsulate.

---

61 Wendehorst, The Proposal for an Artificial Intelligence Act COM(2021) 206 from a Consumer Policy Perspective (2021), p. 84.
62 Wendehorst, The Proposal for an Artificial Intelligence Act COM(2021) 206 from a Consumer Policy Perspective (2021), p. 85.
63 EPRS, Regulating facial recognition in the EU (2021) p. 28.
64 Geminn, Die Regulierung Künstlicher Intelligenz, ZD 2021, p. 356.
65 For details see Art. 6 par. 1 lit. a,b AI-Act proposal.
66 EDPB/EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (2021).
67 See Annex III p 1 AI-Act proposal.
68 There is a wide variety of possibilities, see EPRS, Regulating facial recognition in the EU (2021) p. 26.
69 The EPRS, however, states, that systems, such as access control, may still fall in the high-risk category based on Recital 33 and Annex III p 1 AI-Act proposal: EPRS, Regulating facial recognition in the EU (2021) p. 26.
70 Bomhard/Merkle, Regulation of Artificial Intelligence, EuCML 2021, p. 257 (260).
71 For a detailed analysis see EPRS, Regulating facial recognition in the EU (2021) p. 7.

Practically, and with special regard to large data sets, it should be virtually impossible to ensure complete freedom from errors.[72] Additionally the requirement of using representative data sets is furthered through the inclusion of the obligation to use appropriate statistical properties as well as paragraph 4, which requires the provider to take into account the context in which the system will be used.

Art. 10 par. 5 of the proposal facilitates the usage of such data for the purposes of "*ensuring bias monitoring, detection and correction in regulation to high-risk AI systems*". The data may be used, but only to the extent, it is **strictly** necessary for said purpose. Appropriate safeguards must be set up. According to Ebert/Spiecker, the provision is based on Art. 9 par. 2 lit. g GDPR. They interpret the elimination of bias as public interest.[73] Whether that is the case, will have to be discussed in the future. But in short, the provision has the potential to provide long sought-after legal certainty.

2.4. Human Oversight Measures

Finally, another relevant provision for FRTs in Art. 14 AI-Act proposal since it explicitly mentions them. Facial recognition technology will have to comply with the special paragraph on biometric systems[74] in Art. 14 of the proposal. This concerns real time as well as post remote biometric identification of natural persons. According to this provision, "*no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons*." The usefulness of the provision is already called into question due to the lack of guidance and means for compliance.[75] The measure could also be criticized, because teams are not always more effective in avoiding automation bias than individuals and therefore the risk is not automatically lower.[76]

2.5. Conclusions

FRTs currently are a hot topic for data protection authorities as well as the European Legislator. The AI-Act will create a new legal framework for the use of FRTs. There is no consensus on which rules should apply to FRTs. However, the opinion appears to be, that newly created a priori prohibitions do not go far enough, mainly due to the inherent risks of mass surveillance. Debates range from broadening the material scope of the prohibitions to including private actors. However, the prohibitions are certainly a powerful tool to combat some of these risks with regard to law enforcement. The AI-Act will furthermore provide a much-needed legal basis for processing special categories of personal data to prevent biases. While having a good intention, the provision on human oversight in its current form is of little use to reduce risks. A further point of criticism is the constant use of vague terms and concepts.[77] The academic discussion and the widely varying opinions demonstrate not only the risks of the use of FRTs, but rather the need for a democratically legitimized decision on the matter – in the form of the AI-Act.

3. Acknowledgement

This work has been partially supported by the European CHIST-ERA program via the *Austrian Research Promotion Agency (FFG)* within the XAIface project (grant agreement CHIST-ERA-19-XAI-011).

[72] Bomhard/Merkle, Regulation of Artificial Intelligence, EuCML 2021, p. 257 (260).
[73] Ebert/Spiecker, Der Kommissionsentwurf für eine KI-Verordnung der EU, NVwZ 2021, p. 1188 (1191).
[74] Systems according to Annex III par 1 lit. a Proposal for the AI-Act.
[75] Wendehorst, The Proposal for an Artificial Intelligence Act COM(2021) 206 from a Consumer Policy Perspective (2021) p. 102.
[76] See Pfister, Automation Bias & Proposal of the AI-Act, JusletterIT 24.02.2022.
[77] See also Zankl, KI: Hohes Risiko nur unter menschlicher Aufsicht, 04.05.2021.