UiO : Faculty of Law
University of Oslo

Facial Recognition: efficient security or dystopian nightmare?

—— Addressing Challenges Raised by Facial Recognition Technology in the Private Sector

Candidate number: 9003

Submission deadline: 01.12.2021

Number of words:17900

Abbreviations

A29WP	Article 29 Data Protection Working Party
ADM	Automated Decision Making
AIA	The Proposed Artificial Intelligence Act
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CFR	Charter of Fundamental Rights
CJEU	Court of Justice of the European Union
Commission	The European Commission
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
ECHR	European Convention on Human Rights
EDPB	The European Data Protection Board
EDPS	European Data Protection Supervisor
EU	The European Union
FRT	Facial Recognition Technology
GDPR	General Data Protection Regulation
RBS	Remote Biometric System

Table of contents

"Biometric mass surveillance reduces our bodies to walking barcodes with the intention of judging the links between our data, our physical appearance and our intentions. We should protect this sensitive data because we only have one face, which we cannot swap or leave at home. Once we give up this data we will have lost all control. "[1]

-Lotte Houwing

1. Introduction

1.1. Background

Imagine one day you and your friend enter a shopping mall together. As you walk in, the billboard recognizes you immediately and prompts products that you searched online before, while your friend is kicked out by the security guard as the facial recognition system shows he or she is on the ban list. What was considered dystopian science fiction in the film *Minority Report*, in which the main character's face is recognized as he walks into the retail store, has become a reality today, as facial recognition technology (FRT) is evolving and expanding at an explosive rate. It is one form of remote biometric system (RBS). The terms FRT and RBS will be used interchangeably in this thesis.

FRT is widely used to improve security, efficiency and customer service. In 2021, the global facial recognition market is worth 4.45 billion USD and is expected to grow at a compound annual rate of 15.4% from 2021 to 2028.[2] The revenue from FRT is forecast to reach 12.11 billion USD in 2028.[3] The widespread use of biometric data, however, raises concerns regarding its impact on fundamental rights. Essentially, FRT reduces people's bodies to walking barcodes, and links their appearance with their intentions.

As with any "*Minority Report*-esque tech"[4], most of the controversy in terms of the use of FRT stems from the inaccuracy of the technology, leading some people to argue that the technology should be prohibited until it completely removes the potential algorithmic bias.[5] However, it is not enough to only focus on regulating the technical standard of FRT; more meaningful regulatory mechanisms could perhaps focus on regulating and tightening the use of

[1] Houwing (2021).

[2] Facial Recognition Market Size & Trends Report, 2021-2028.

[3] Ibid.

[4] Song (2020).

[5] Castro (2019).

such technology.[6] This shift in focus will mitigate many issues and will not hamper innovation in the meantime.

Although much has been written about the use of FRT by law enforcement agencies in a criminal justice context, the danger raised by the technology employed by private actors for non-law enforcement purposes has been overlooked.[7] Private use of FRT could effectively enhance security. However, without adequate protections for fundamental rights and restrictions on the use of FRT, the widespread use of this technology is likely to become a dystopian reality. This is augmented by the collaboration between private organizations and law enforcement agencies, leading to face surveillance. In other words, whether FRT in the private sector leads to efficient security or a dystopian nightmare depends on the protection level for fundamental rights provided by regulatory mechanisms.

This thesis is going to focus on the use of FRT by private entities in publicly accessible spaces for safety purposes. There are multiple non-law enforcement purposes for private companies to use FRT, such as marketing, customer service, and attendance tracking. This thesis will, however, focus on safety control since it is one of the most intrusive uses of FRT. "Publicly accessible spaces" refers to physical places that are open to the public such as shopping malls, supermarkets and sports venues. Since the focus is on physical places, online spaces are excluded by this definition. While this thesis emphasizes non-enforcement purposes, the danger that police might get access to biometric data from the private sector could not be neglected. Therefore, the possibility that law enforcement may use the private databases will fall within the scope of this thesis.

At present, the regulatory landscape in the EU relevant to FRT is complicated and continually evolving. There is a highly developed human rights framework to safeguard data protection, privacy and non-discrimination in the Charter of Fundamental Rights (CFR) and the European Convention on Human Rights (ECHR). Although the Charter is aimed at "EU institutions and member states when implementing Union Law"[8], it also affects the relationship among private parties due to the "horizontal effect".[9] This thesis will discuss how FRT affects funda-

[6] Chun (2019), p.102.

[7] Rowe (2020), p. 3.

[8] CFR Article 51(1).

[9] Frantziou (2020), pp. 208-209.

mental rights when analyzing the risks and concerns posed by this technology. Due to the word limitation, it will not give exhaustive analysis of the Charter and ECHR.

In addition to the primary law, secondary legislation implementing basic rights, and sector-specific regulations, govern emerging technologies in more detail. For facial recognition, the GDPR is the only existing specific regulatory regime applicable to biometric data. But there is also emerging regime like the proposed Artificial Intelligence Act (Proposal or AIA) that governs the use of high-risk AI like FRT. Released in April 2021, the new Proposal introduces specific provisions regarding remote biometric systems, which also include facial recognition systems.

Accordingly, as the EU stands at the crossroads of the significant decision of how to regulate FRT, this thesis aims to offer a more effective regulatory approach by evaluating the adequacy of existing and emerging laws that regulate FRT. The thesis will first outline the critical issues related to the use of FRT. Then it will analyze the regulatory mechanisms that are applicable to FRT in the GDPR and the proposed AI Act to evaluate if the current approach sufficiently protects individuals' rights. Due to the word limit, this thesis is going to put more focus on AIA than the GDPR since the AIA is a proposal that is still being shaped and developed. Analyzing the AIA and recommending changes and improvements to it would therefore be more valuable and practical. This does not mean, however, that the GDPR is unimportant. On the contrary, the GDPR is essential to protect individuals against the invasion of privacy by FRT.

1.2. Research question

In view of the above observations, this thesis tries to answer the following research question:
How to address the challenges raised by facial recognition systems used in the private sector in publicly accessible places through legal regulatory means?

To answer this research question, the thesis will assess the following sets of sub-questions:

1. *What is facial recognition technology? How is this technology being used in publicly accessible spaces? What challenges are posed by the use of FRT in the private sector?*

2. *What rules in the GDPR are relevant to address these challenges? What are the remaining concerns that haven't been solved through the implementation of the GDPR?*

3. *What rules in the AIA are relevant to address these challenges? Are they sufficient to tackle the risks of FRT?*

4. *How could FRT be regulated more efficiently in order to mitigate risk and safeguard human rights?*

1.3. Methodology

This thesis used a doctrinal research methodological approach. It constitutes of analysis of current legal sources that are applicable to FRT in section 3, followed by a critical-descriptive analysis of the proposed AI Act in section 4. It gives critical evaluation of the existing and emerging legal framework for facial recognition systems. Furthermore, sections 3.2, 3.3 and 4.4 feature case study to demonstrate how the rules can be applied in practice. The legal analysis is based on EU legislations, with a focus on the GDPR and the Proposal. Implementation by Member States falls within the scope of this paper.

Although the thesis relies on fundamental rights analysis since FRT implicates the fundamental rights of affected persons, the thesis will not explore CFR and ECHR in detail. Instead, it illustrates how FRT affects the fundamental rights enshrined in the Charter and ECHR in the analysis of the risks posed by this technology in section 2.3.

In addition to provisions applicable for FRT, the sources for this thesis also include academic journals, case decisions and information collected from the internet.

1.4. Structure

The structure of this thesis will be as follows:

Section 2 describes the background information about the technological perspective, the current uses of FRT for safety control around the world by private actors, and the serious concerns it caused as a result of its impact on privacy and other fundamental rights enshrined in the first legislation.

Section 3 explores the current second legislation that is applicable to the use of FRT. It discusses how rules in the GDPR have been utilized to protect individuals' fundamental rights that are affected by FRT. It analyzes two cases that occurred in EU to evaluate the adequacy of mechanisms in the GDPR, and identities the remaining concerns that are not addressed by the implementation.

Section 4 explores the requirements in the proposed AI regulation, including the specific provisions for remote biometric systems and general requirements for all high-risk AI systems. It will critically assess if these rules are sufficient to reduce the risks of FRT and safeguard human rights. In doing this, it will analyze the regulatory approach in the Proposal and apply these rules to the case of using FRT in a supermarket and a stadium.

Section 5 gives recommendations to regulate facial recognition technology more efficiently and adequately, and close the potential gaps in the GDPR and the proposed AI Act to safeguard fundamental rights. Section 6 will draw a conclusion.

2. Background of Facial Recognition Technology

This part will provide background information on FRT regarding its definition, how the system is trained, the current situation with respect to the use of FRT and various stakeholders' interests, and the risks and concerns posed by the employment and development of FRT.

2.1. Technological background and the current application

This section will introduce the technical perspective of FRT and look at one of the major applications of this technology to identify relevant stakeholders.

2.1.1. What is facial recognition technology?

Facial recognition technology refers to any technology or software system that is used to identify individuals through analyzing the similarity between faces in photos and videos based on people's facial characteristics.[10] It is one form of many biometric identification methods, including iris recognition, fingerprint recognition and behavioral biometrics such as walking patterns, gestures and voice recognition. [11] However, facial recognition has a different and unique danger in comparison to other biometric systems, which will be introduced in section 2.3. It is designed to combine humans' excellent perception skills with computers' huge processing power and storage capacity.[12]

There are three common types of facial recognition: identification, verification and characterization. Identification is also known as "one to N", which is used to determine if a face of an

[10] Woodward Jr, John D., et al. (2003), p. 7-8.

[11] Aggarwal, Gaurav, et al. (2008).

[12] Welinder (2012), p 170-172.

unknown person exists in a large database of known records.[13] Characterization refers to a facial analysis method which is used to classify a single record according to characterizations such as gender, age and emotion. Facial characterization is a different technology from facial recognition regarding its developmental process and uses, but the terms are sometimes used interchangeably. Verification is known as one-to-one matching, and is used to confirm that if an individual is connected to a specific identified face.[14] Due to the word limitation, this paper will focus only on identification, since this type of FRT is considered to be the most problematic.

2.1.2. How this technology works

There are three steps to identify a person through FRT. Firstly, the system will detect and locate human faces in photos and video clips, which is called Face Detection.[15] Secondly, the Face Capture process will transfer the face into numerical information to generate a face template. [16] Thirdly, the Face Match process will determine if the two faces belong to one individual.[17]

Currently, facial recognition technology is developed through deep learning. [18] This is a form of machine learning that uses artificial neural networks to process data.[19] Developers create software programs with the help of deep learning to transform face characteristics into digital expressions called templates, which are able to be compared to determine the similarity of faces.[20] The old method to generate templates is to locate certain key points of a face and measure their distance. However, today's approach is more sophisticated, as it generates face templates by passing a face though "filters".[21] It manipulates pixel values according to a set of programmed rules with the purpose of transforming the face into the simplified "faceprint". [22]

---

[13] Ibid.

[14] Ibid.

[15] Thales Group (2021).

[16] Ibid.

[17] Ibid.

[18] Lewis (2021).

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] Ibid.

To identify the best filters for generating robust templates, developers use deep learning to automate the trial and error process. The training is to provide the system with a series of " triplets"- collection of three faces in which two belong to one individual and one belongs to someone else. [23] The system transfers the three images into templates and compares the similarity. [24] The algorithm constantly adjusts the operations performed by the filter.[25] The system will keep the change that leads to improvement, or try something else if the performance gets worse.

The accuracy of this technology depends on a few factors, including the amount of input training images, the methodology used to develop the system, and the quality of the images and videos.[26] Therefore, FRT could lead to false positives and false negatives, like other machine learning systems.[27] A false positive means that an algorithm falsely concluded that two different faces belonged to the same person.[28] A false negative refers to the incorrect conclusion that two different images of the same person's face belong to different people.[29] It is impossible to avoid the trade-off between false positives and false negatives, due to the decision of the threshold of probability.[30] The false negatives will increase while the false positives will decrease if the threshold is lower, and vice versa.[31] This should be kept in mind when discussing the risk raised by FRT, as even a small percentage of errors means hundreds of individuals would be incorrectly matched.

2.1.3. How this technology is being used for safety and security control

Nowadays, FRT has been widely used among private companies all over the world, which reveals the depth and width of its engagement in daily life. [32] The most prevalent application of FRT is to enhance the safety and security of a certain environment. There is a trend to adopt FRT in publicly accessible spaces, such as stores, stadium and schools, for non-law en-

---

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] Zhao & Rama (2011), p. 293.

[27] EUAFR (2019), p. 26-27.

[28] Allevate. 2020.

[29] Ibid.

[30] See note 27.

[31] Ibid.

[32] Rowe (2020), p. 22.

forcement purposes. Stores use it for safety purposes and to identify thieves. For instance, a supermarket chain called "Mercadona" in Spain adopted FRT in 48 shops for months to identify people with criminal convictions and restraining orders, especially individuals who received restraining orders because they assaulted store employees or were convicted for store-related incidents.[33] The system captured everyone's facial image when they entered the supermarket, including customers and employees.[34] In addition, schools use FRT to stop certain adults in the database from entering the campus and to help track potential shooters in school.[35] For example, a school district in New York launched facial recognition system to detect individuals who were deemed to be a threat, such as sex offenders, suspended employees and students, and to alert the administration if the system found one. [36]

2.2. Challenges posed using facial recognition

Despite the variety of benefits associated with FRT with respect to safety, security and efficiency, the specific feature of FRT combined with its potential influence on individuals' fundamental rights raises some challenges in the development and employment of this technology. Therefore, this section will classify and present these challenges to better understand stakeholders' concerns and how they may influence the regulations in this area.

2.2.1. Accuracy and other unique concerns raised by technical features

As illustrated before, facial recognition technology is only one form of biometric identification system. There are other biometric technologies such as iris scans, fingerprints, and walking patterns. Therefore, some may hold the view that there is no differences between the challenges that stem from FRT and from other existing biometric technologies. However, that opinion is misguided, as facial recognition poses certain concerns due to its unique technical features.

Firstly, facial recognition technology requires the use of deep learning, which differs from most other biometric processing, leading to a high chance of false positives. Meanwhile, it is difficult to implement human oversight for manual checking and labelling as data sets powered by deep-learning continue to grow. Regardless of the improvement of accuracy because of increased computational power, the algorithm of FRT can only give probabilities instead of a 100% definitive outcome.

---

[33] Privacy & Information Security Law Blog (2021).

[34] Ibid.

[35] Duren. 2019.

[36] Ibid.

Secondly, faces are central to an individual's identity, while being easy to capture in a cost-effective way from a distance without notification or consent.[37] The face plays an essential role in social interaction, as it presents emotion and attentiveness.[38] However, unlike iris scans and fingerprints, people cannot reasonably stop themselves from being identified in the street or in a shopping mall.

Thirdly, unlike other biometric features which need an initial capture of biometric information, facial images do not require any enrollment phase. Therefore, a large number of faces are already available, as many facial pictures have been collected by public and private actors or have been uploaded by users on social media. For instance, MegaFace, a huge facial-recognition database, contains seven hundred million facial images, some of which were obtained through Flickr, a photo-sharing site. [39]

2.2.2. Different performances based on race and gender

Discrimination means an individual is treated less favorably than other people in a comparable situation, based on perceived or real personal characteristics.[40] The prohibition of any discrimination on the basis of personal features is protected in Article 21 of the EU Charter, and reflected in Articles 12 and 14 of the ECHR.[41] Discrimination occurs in algorithmic decision making because biases may intentionally or unconsciously be incorporated in the algorithm itself during design, testing, and implementation. [42] It may also occur on account of the way the outcomes are handled by the officers using the facial recognition system. Once different performances are present in an algorithm, it is often impossible or extremely difficult to remove them by programmatic solutions. [43]

The reason why biases are rooted in the algorithm itself is because of the quality of data used to develop facial recognition software. In principle, the more facial images developers feed the software, the more accurate and effective the algorithm would be. However, the number of

---

[37] Chen. 2020.

[38] Leopold. 2010.

[39] Hill & Aaron. 2019.

[40] EUAFR (2019), p. 27.

[41] Ibid.

[42] Ibid.

[43] EUAFR (2018), p 24.

facial images processed by the software is not the only factor in determining the accuracy.[44] The quality of such images, which requires a representative set of faces reflecting all races of people, would also influence the accuracy.[45] However, in the Western world, most of the algorithms are trained with more images of white men than images of women or people of color. [46] As a consequence, facial recognition software tends to be more accurate if the subject is a white man than a woman of color.

Different reflections of light also affect the results of facial matching in FRT. Too much reflected light influences the image quality of very fair-skinned people, and not enough light influences the image quality of very dark-skinned people. [47] These people are usually subject to a higher likelihood of a false positive when comparing their images against the database, which may cause certain groups of individuals to be wrongly stopped more frequently because of their skin color. [48]

There are wider influences and moral harms of facial recognition, suffered by people who are directly affected by the risk of misuse and abuse when using this technology.[49] Academics have found concerns relevant to "distributive injustice", which refers to the refusal of access to benefits, resources or opportunities toward persons of a discriminated-against social group.[50] For instance, if the FRT deployed in a shopping mall misidentified a customer in a database as not allowed to enter, he or she might be wrongly stopped and could not freely enter the place like others.

Another concern is related to "recognitional injustice", which happens among people who belong to a discriminated-against social group, where their identity claims are denied in a way that reaffirms their marginalized position.[51] For example, if a facial recognition system is built with the intended goal of making an administrative process more efficient for some privileged

[44] EUAFR (2019), p. 29.

[45] Ibid.

[46] Ibid.

[47] Ibid.

[48] Ibid.

[49] Madiega & Mildebrath (2021), p. 7.

[50] Ibid.

[51] Ibid.

social group, it may increase the burden of time and effort for marginalized groups to complete the same process.[52]

2.2.3. Data collection and storage

The use of FRT consists of a sequence of processes such as collection, comparison, and storage of highly sensitive biometric data of individuals' facial features. This leads to invasive results for persons' right to protection of personal data, which is enshrined in Article 8 of the Charter.[53] It also affects the right to private life, which is set out in Article 7 of the Charter.[54]

One of the biggest concerns relates to explicit consent when using FRT. Reports show that consumers' biometric data could be used by companies to build large databases, train FRT algorithms, and could even be shared with other companies without the consumer's consent.[55] For instance, one facial recognition software, MegaFace, collected a large number of faces from Flickr to develop and train the algorithm without users' knowledge.

Additionally, the storage of biometric data is also a real concern under the global expansion of FRT with only a few regulations. People worry about who else could gain access to their personal data, which are encrypted and stored by companies on their data centers or secured networks. Another threat that cannot be ignored is hacking. A security company, Suprema, whose responsibility is to ensure building security, manages a biometric database without encryption or other protection measures.[56] This leaves one million individuals' facial recognition information, which was accessed by UK Metropolitan Police and banks, publicly accessible. [57] Therefore, this flaw in the system allows anyone to access and even change their 23 GB of data (or 27.8 million records) by URL search criteria manipulation.[58] The utter scale of the data breach is appalling, as the system is used not only in London but also in other 1.5 million worldwide locations.[59]

---

[52] Leslie (2020), p. 23.

[53] CFR. Article 8.

[54] CFR. Article 7.

[55] Rowe (2020), p. 36.

[56] England (2019).

[57] Ibid.

[58] Ibid.

[59] Ibid.

2.2.4. Potential misuse and concerns for fundamental rights

It is possible that the use of facial recognition software will be extended beyond its originally permitted and authorized purpose, which entails some concerns in the long term. For instance, the extensions could occur when using data collected on databases beyond its initially allowed purpose or when bringing new functionalities into an existing system.[60] Such expansion could be part of the strategy to promote FRT by using it when the purpose seems to be legitimate in the first place, and then gradually expanding the scope of use, which is also known as the "slippery slope" argument.[61]

There is also an increasing use of facial recognition technology in publicly accessible spaces in the EU which may result in mass surveillance. This will have negative impact on freedom of expression, which is enshrined in Article 11 of the Charter and in Article 10 of the ECHR.[62] As long as such systems are in operation, it is possible to track individuals, and therefore it might be impossible for people to move in public space anonymously. For instance, even though the FRT deployed by a supermarket collects customers' data anonymously, the employees in the supermarket can still identify them. Besides, private sectors might share their data with law enforcement agencies for investigation. This will inevitably affect individuals' freedom of expression and movement.

Furthermore, studies demonstrate that facial recognition technology can be used to predict people's political orientation and sexual orientation, which raises the concern of misuse. In 2021, research conducted by Stanford University showed that FRT could expose persons' political stance, and the accuracy of the result is 72% across countries such as the U.S and the UK.[63] This finding illustrates the critical influence of FRT for the protection of people's civil liberties. In 2018, FRT developed by researchers from Stanford University could distinguish gay men in 81% of cases, and gay women in 71% of cases, which exposes a danger to the privacy and safety of the gay community.[64]

---

[60] Madiega & Mildebrath (2021), p. 5.

[61] Castelluccia & Inria (2020).

[62] EUAFR (2019), p. 29.

[63] Kosinski (2021), p. 2.

[64] Wang & Kosinski (2018).

In summary, although FRT has real advantages regarding safety, security and efficiency, such technology may cause serious threats to individuals' fundamental rights in terms of privacy, non-discrimination, and the freedom of expression.

These rights are enshrined in the first legislation CFR and ECHR. Yet in practice, such fundamental rights are still being formed, [65] and their applicability to conflicts in the private sector is uncertain.[66] The first legislation hardly provides practical guidance for the deployment of facial recognition, and only indirectly resolves disputes at the interface of fundamental rights and new technologies.[67] Hence, the CFR and the ECHR are not sufficient to protect individuals against algorithmic discrimination and infringement of privacy.[68] Against this backdrop, these risks are worrying, especially considering the increasing use of FRT in publicly accessible spaces.

3. Legal Framework for Privacy and Data Protection

With these concerns in mind, this section is going to look at the existing law that regulates the use of FRT in the private sector. It will introduce the regulatory mechanisms in the GDPR that are applicable for the use of FRT. To critically assess if the GDPR affords effective protection for affected individuals, this section will analyze two real-world cases that happened in EU Member States.

3.1. An overview of the European Union's General Data Protection Regulation

Adopted in 2016, the GDPR modernizes data protection legislation and allows it to protect fundamental rights in the digital era.[69] It is applicable to partly or fully automatic AI programs, such as FRT, that process individuals' personal data.[70] FRT collects data regarding individuals' facial features, which is biometric data subject to rules under the GDPR (Art. 4 (14)).

---

[65] Fuster & Hijmans (2019).

[66] Google Spain, CJEU; Ward (2018); Frantziou (2020), pp. 208-209.

[67] Madiega & Mildebrath (2021), p. 10.

[68] Hacker (2018), p. 1143.

[69] Colonna (2021).

[70] Ibid.

This regulation contains several core principles for data collection and processing listed in Article 5 of the GDPR. Article 6 requires personal data to be processed using at least one of six legal bases in order for the processing to be lawful under Article 5(1).[71] Article 9 prohibits the processing of special categories of personal data, such as biometric data, unless the data processing meets certain conditions. Moreover, the GDPR provides various rights to the data subject, such as the right to be given information regarding the collection and use of their personal data, the right to access their data, and the right to correct inaccurate or incomplete information.[72]

In addition, since the output generated by FRT is based on automated decision making, Article 22 of the GDPR is applicable. Articles 13-15 require data subjects to receive meaningful information about the logic involved in an automated decision-making system, including the significance and foreseeable consequences of the system.

Furthermore, under Article 25, data controllers are obligated to implement technical and organizational measures in their processing to meet the regulation's requirements and protect the rights of data subjects.[73] Therefore, the GDPR imposes the duty on controllers of facial data that they must consider privacy and data protection when purchasing and deploying a facial recognition system.[74]

To ensure the security of processing, Article 32 explicitly refers to pseudonymization and encryption of personal data as appropriate technical measures which are required in Article 25. Article 32 also recommends regular testing and evaluation of the effectiveness of existing technical and organizational measures.[75]

With so many rules in the GDPR that are applicable for biometric data, it may seem that this regulation already offers adequate protection for the subjects of facial recognition systems. However, the risks brought by FRT are not restricted to data privacy. As discussed in section 2, FRT has a critical impact on other fundamental rights. The next part will analyze specific

[71] GDPR. Article 5(1).

[72] Madiega & Mildebrath (2021), p. 10.

[73] Bygrave (2017), p. 106.

[74] ICO report (2021).

[75] GDPR, Article 32

provisions regulating biometric data through two cases to assess if the GDPR provides sufficient protection for users' fundamental rights.

3.2. Two real-word cases of using facial recognition systems

3.2.1. Deploying FRT in a supermarket -The Spanish case

In January 2020, Mecadona, a large supermarket chain in Spain, began using FRT to prevent persons convicted of robbery or other relevant crimes from entering the store.[76] Their system was from the Israeli company AnyVision. It is an identification system used to identify any individual with a court decision against them for robbery or other relevant crimes who is therefore prohibited from entering Mecadona stores.[77] Once the system identifies an individual with a restraining order, it sends an alert which will be confirmed by the security staff. If the output has been verified, the security forces will be alerted. If the output is negative, the biometric data will be destroyed 0.3 seconds after collection.[78] Mecadona displayed information banners in all 40 stores using the system. They claim that they rely on the legal basis of Article 6 (1)(e) and Article 9(2)(g). They applied to the court for permission to use the facial recognition system before conducting the DPIA.

On June 5, 2021, the Spanish Data Protection Authority (AEPD or Spanish DPA) issued an administrative fine about €2,520,000 for the use of FRT violating Article 5(1)(c), 6(1), 9(1), 12, 13, 25(1) and 35 of the GDPR.

3.2.2. Deploying FRT in a stadium -The Danish case

In July 2019, a football club called Brøndby IF in Denmark started to deploy facial recognition technology at Brøndby Stadium.[79] Their system automatically identifies people who have been prohibited from attending football matches since they violated the club's own code of conduct.[80] The FRT system uses cameras to scan the public area in front of the stadium entrance in order to "pick out" individuals in the database from the crowd before they enter the

[76] AEPD. PS/00120/2021.

[77] Ibid.

[78] Ibid.

[79] Lund (2020).

[80] Ibid.

stadium.[81] During each football match, around 14000 persons' biometric data will be collected and processed by this system, while there are only 50 persons on the ban list.[82]

The Danish Data Protection Authority (Datatilsynet or the Danish DPA) gave prior approval to the football club for the use of FRT with a number of conditions related to data minimization, transparency and security.[83] The legal basis for biometric data processing relies on the public interest under Article 9(2)(g) of the GDPR.[84] Brøndby IF became the first company which obtained approval for the use of FRT in Denmark.

3.3. Rules that should be considered when deploying FRT under GDPR

The two cases above show that national authorities have handled the use of facial recognition systems differently. The FRT employed by the Spanish supermarket and the Danish football stadium were both identification systems (i.e., not systems for authorization or categorization). They were both employed in publicly accessible places by private entities for safety and for non-law enforcement purposes. The decisions regarding their lawfulness by their respective DPAs, however, are contrary. The following content will discuss what rules should be considered when deploying FRT under the GDPR, and what risks have yet to be addressed by these rules. The analysis is based on a comparison of the two cases.

3.3.1. Processing of special categories of data

When using FRT under the GDPR, the first issue to consider is whether the data used by the controller is considered a special category of data under Article 9(1).[85] In both cases, the use of FRT involved facial data, i.e., biometric data, for "the purpose of uniquely identifying" individuals. Thus, data processed by these systems includes special categories of data.[86] This was recognized by both the Spanish and the Danish DPA.

3.3.2. Legal basis

The processing of special categories of data is prohibited by Article 9(1) of the GDPR, and therefore controllers must seek exemptions under Article 9(2) to legally process data. Since

[81] Ibid.

[82] Ibid.

[83] Ibid.

[84] Datatilsynet.

[85] GDPR. Article 9(1).

[86] AEPD. PS/00120/2021.

the FRT deployed in both cases captures faces from a distance, it is unlikely that the supermarket and the football club could get explicit consent from individuals (exemption under Article 9(2)(a)). However, there are two exemptions relevant for the processing of facial data.

The first ground the supermarket and stadium both tried to rely on is public interest under Article 9(2)(g). This exception based on public interest must be set by national law, which should be proportionate and provide suitable measures to safeguard fundamental rights.[87] This is most relevant for public actors when conducting tasks in the public interest. Private entities therefore have limited access to this legal basis. If Member States choose to interpret this exemption in Article 9(2)(g) strictly, most FRT used in the private sector will not meet its conditions. This is because such systems continuously automatically collect individuals' facial images from a distance, which greatly intrude on fundamental rights and individual freedom.[88] Therefore, strict interpretation of this rule will prevent the expansion of such technology and mitigate the risk of biometric mass surveillance.

However, as demonstrated by the two cases, different countries have a different understanding of what constitutes necessary and proportionate processing to protect the public interest. The Spanish DPA recognized the risks associated with FRT and stated that there is no national law allowing such processing of data.[89] Furthermore, because the supermarket only pursued private interests, there was no real connection between the purpose of using FRT and the public interest.

The Danish DPA held a different view; they claimed that the football club could rely on public interest as a legal basis. Their decision was based on the consideration of safety during large sporting events with large crowds. Although there was no national law that provided a legal basis for the use of FRT, the general exemption in Section 7(4) of the Data Protection Act could be used to permit processing of any type of special categories of personal data.[90] The explanatory remarks on Section 7(4) pointed out that the interpretation of this provision must be narrow, while excessive discretion leaves it up to authoritative decisions by the DPA to decide the scope of exemptions. [91]

---

[87] GDPR. Article 9(2)(g).

[88] AEPD. PS/00120/2021.

[89] Ibid.

[90] Lund (2019).

[91] Ibid.

The Spanish supermarket further tried to rely on the legal basis of court orders under Article 9(2)(f). The purpose of Mercadona's use of FRT was to comply with court claims that allowed the use of electronic means, such as facial recognition, which was mentioned in some cases.[92] The court orders only gave them ground to impact the rights of convicted individuals. Their system, however, processed the biometric data of anyone who entered the store.[93] Moreover, not all court orders mentioned FRT as a means to implement the restraining orders, and the use of FRT was not suitable for all situations.[94] When using FRT, one should therefore consider the seriousness, possibility, and scale of potential damage, as well as the consequences to individuals' rights. Taking all the above into account, the Spanish DPA concluded that the supermarket could not rely on this exemption as a legal basis.

In conclusion, the prohibition on processing special categories of personal data with strict exemptions in the GDPR does offer some protection for individuals exposed to FRT. But the risk of biometric mass surveillance will remain in the EU, because of the likely expansion of FRT used in the private sector. There is a tendency for private entities to rely on the public interest exemption in order to use FRT. Coupled with the excessive discretion of the DPA, the broad interpretation of this exception may give unprecedented opportunities for private organizations to use FRT, in spite of risks such as discrimination. Therefore, the prohibition on processing special categories of personal data is insufficient to stop the trend of using FRT in publicly accessible places.

3.3.3. Proportionality

Article 5 of the GDPR sets out proportionality principle, which requires the data processing to be adequate, necessary, and proportionate to balance persons' rights and freedoms of the subjects. The controller must balance many elements to determine if the loss of privacy is proportionate to the expected benefit, and measure the risks posed by collecting biometric data. The EDPB also suggests that surveillance should only be used when it is suitable and adequate for the pursued purpose.[95]

---

[92] AEPD. PS/00120/2021.

[93] Ibid.

[94] Ibid.

[95] EDPB Guideline 3/2019. para 24.

In relation to FRT used by private entities for safety control, there are multiple factors that need to be taken into consideration:

Consequences to individuals' fundamental rights	Presence or absence of solely automated decision making	Reasons why these individuals are prohibited from entering
Number of persons that need to be scanned / Numbers of persons on the ban list	Risk-mitigation strategies to safeguard individual's rights	Existence of alternative options for safety control
Adequate technical and organizational measures to secure data	Accuracy rate of prediction / Level of human oversight	Seriousness, possibility and scale of potential damage

Table1

In light of these factors, even if the processing in the Spanish case was adequate, it was not necessary. There were other ways to achieve the purpose, such as requiring security staff to recognize and prevent the convicted individual from entering the store.[96] Furthermore, the processing not only affected convicted individuals, but also affected the privacy of other potential customers and employees.[97] Thus, the Spanish DPA concluded that the use of FRT in the supermarket was not proportionate.

The Danish DPA, on the other hand, stated that the data processing was adequate and necessary because FRT was the only effective way to enforce the internal quarantine list.[98] Normally around 14,000 people would attend a football match, and there were only 50 persons on the ban list. It would take a long time for security to manually examine each visitor. The longer people stand in line, the greater the risk of unrest. The Danish DPA found the use of FRT to be proportionate because there was no other alternative to achieve the same level of effectiveness as FRT within a reasonable time frame.[99]

[96] AEPD. PS/00120/2021.

[97] Ibid.

[98] McGhie (2019).

[99] Ibid.

The DPAs considered different factors when assessing the proportionality of the use of FRT. The Spanish DPA considered the fundamental rights of other affected individuals such as the employees and potential clients. Mercadona claimed the use of FRT was the only appropriate way to enforce the entry prohibition because they had 1,623 stores and 95,000 employees. Mercadona also claimed that the system would be more reliable and provide more safeguards than any other measure. The Spanish DPA, however, did not allow convenience to override the data subjects' fundamental rights.

The Danish DPA, on the other hand, did not seem to take into full consideration the fundamental rights affected by FRT such as the right to privacy, non-discrimination, and freedom of expression. There were only 50 people on the ban list, while the system would be processing 14,000 data subjects' sensitive data every football match. Although they did consider individual rights by setting conditions for the use of FRT, these conditions only focused on data minimization, transparency, and security (see 3.3.4.2-3.3.4.4). They overlooked the risk of bias and social exclusion, since they did not mention human oversight or other protective measures.

FRT challenges the necessity and proportionality principles in the GDPR.[100] As confirmed by settled case-law of the CJEU, "an objective of general interest—such as crime prevention or public security—is not, in itself, sufficient to justify an interference with a Charter right". [101] [102] For this reason, the hypothetical claims of any organization to increase efficiency, to comply with a court order, or to protect public security by using FRT are insufficient to justify the violation of fundamental rights.[103] Without adequate protective measures when using FRT, the cost to individual rights and democratic values far exceeds the perceived benefits.[104]

In summary, the proportionality principle could have prevented the arbitrary use of FRT. If authorities had allowed for the use of such systems only when necessary, this could have mitigated the risk of infringement on privacy and prevent biometric mass surveillance. However, different interpretations and insufficient considerations regarding proportionality by Member States may have undermined this protection.

---

[100] Renda., et al. (2021). p. 43.

[101] Ibid.

[102] CJEU. Joined Cases C−203/15 and C−698/15.

[103] See note 100.

[104] Ibid.

3.3.4. Data protection principles

In addition to the proportionality principle, Article 5 of the GDPR defines other data protection principles, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. There are four principles that are most relevant to the use of FRT: purpose limitation, transparency, data minimization, and data security.

3.3.4.1. Purpose limitation

The first principle is the purpose limitation principle in Article 5(1)(b). Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[105] This requirement may address the risk of misuse and "functional creep" of FRT. However, there is a public interest exemption for processing data. This means police may get access to the private databases owned by the supermarket or the stadium, which will not be counted as incompatible with the initial purposes. Hence, the risk of a chilling effect and biometric mass surveillance are likely to remain. In both cases, the DPAs did not consider this impact on fundamental rights.

3.3.4.2. Transparency and automated decision making

The second principle is the transparency principle in Article 5(1)(a) and Articles 12-15 of the GDPR. The controller needs to provide information to data subjects in a clear, concise and comprehensible format.[106] In the Spanish case, merely displaying information banners in the stores to inform people that they are using the system can hardly justify that the data processing is transparent. The information on the banners was only related to convicted individuals, while there was no reference to the data of potential clients or employees being collected.[107] Moreover, Mercadona did not specify in which stores and during what times the systems were in operation.[108] This was confirmed by the Spanish DPA. The Danish DPA took a different approach. They only required the club to display clear signs with an explanation on how FRT was being used and what data was being collected. They did not require information regarding risks and how FRT interferes with individuals' rights to be given.[109]

---

[105] GDPR. Article 5 (1)(b).

[106] GDPR. Article 12.

[107] AEPD. PS/00120/2021.

[108] Ibid.

[109] Datatilsynet. See also Dautlich (2020).

Considering that FRT is a type of automated decision making (ADM), it will be caught by Article 22, and the transparency requirements that regulate machine learning applications in Recital 71, and Articles 13(2)(f), 14(2)(g) and 15(1)(h). Article 22(1) indicates that individuals have the right not to be subject to FRT, when such a system is "solely" ADM and has "significant" effects on individuals.[110] However, it is not clear what is "solely" ADM and what constitutes "significant" effects.[111]

There is also a debate whether Article 22(1) gives a right to individuals not to be subject to ADM, or is a prohibition on the use of ADM. The Spanish DPA concluded that the supermarket must remove all FRT equipment, otherwise the processing did not comply with Article 22(1). The Spanish DPA considered Article 22 as a general prohibition on ADM. However, there are scholars who argue that this provision is a right "to be exercised at the discretion of data subjects".[112] This interpretation leaves it up to affected individuals to decide if they oppose being subject to FRT. The Danish DPA, on the other hand, did not consider Article 22(1).

Regardless of whether Article 22 provides a right or a prohibition, organizations need to comply with transparency requirements related to ADM in Recital 71, and Articles 13(2)(f), 14(2)(g) and 15(1)(h).[113] These requirements indicate that the supermarket and football club must provide information and explanation of their decisions in a way that ensures that people who are prohibited from entering get adequate information needed to change the decisions.[114] The right to an explanation is essential to enhance the accountability and transparency of FRT, and to avoid bias and discrimination. On the other hand, the right to obtain an explanation and to challenge the decision are only clearly stated in the preamble (i.e., Recital 71), which does not have binding legal force. Thus, there is uncertainty over the actual protection given to data subjects and the long-term effectiveness of Article 22 when regulating FRT. [115]

3.3.4.3. Data minimization

The third principle is data minimization, defined in Article 5(1)(b) and (e), which requires controllers to collect the minimum amount of data in order for the processing to be balanced

---

[110] GDPR. Article 22(1).

[111] A29WP Guidelines 2016/679 merely stated that the "significant" effect depends on the specific characteristics of the case. see also Wachter.,et al. (2017), p. 76.

[112] Bygrave (2020), p. 17.

[113] Bygrave (2020), p. 20-21; Bygrave (2019), p. 8; see also Mendoza & Bygrave (2017), p. 93.

[114] Ibid.

[115] Bygrave (2020). p. 24.

with the rights of the data subject. It is difficult for FRT to comply with this principle, as it involves the processing of massive amounts of biometric data. For both cases, the facial data of every potential client and employee were collected, solely for the purpose of controlling a small number of individuals. The Spanish DPA thus concluded that the supermarket violated this principle, while the Danish DPA merely required that the controller not store personal data that did not match with the ban list.

3.3.4.4. Data security

The fourth principle is the data security principle in Article 5(1)(f). It is in line with Article 25, which states that the controller should take technical and organizational security measures to ensure the security of biometric data. This principle is critical to tackle the risks of hacking and misuse. In the Spanish case, there was not enough information regarding the controller's security measures. In the Danish case, the DPA required that 1) the controller must encrypt personal data; 2) FRT cameras must not be accessible via the internet; and 3) two-factor authentication must be in place for all authorized personnel with access to the data.[116] These conditions are useful in ensuring data security.

3.3.5. Data protection by design and by default

Article 25 defines data protection by design and by default, requiring that the core data protection principles outlined above are integrated into the design and development of the data processing system. This is essential to ensure that privacy-related interests are taken into account throughout the lifecycle of development of such systems.[117] However, due to vague and complex language, and the lack of clear guidance on the appropriate framework and methodologies, Article 25 is difficult to enforce in practice.[118] Moreover, the obligations under this provision are formulated in a general way, which makes it difficult to assess the violation of this Article.[119]

In relation to the two cases, Mercadona did not take account of privacy by design sufficiently. Due to the lack of training data regarding vulnerable groups, algorithm bias may result in discrimination and social exclusion, which poses an unacceptable risk by design. Especially in the current context of the pandemic, there is a high risk of errors due to the use of masks. For these reasons, the Spanish DPA concluded that the store violated Article 25. Meanwhile, it seems that the Danish DPA did not consider data protection by design, since they did not give

[116] Dautlich (2020).

[117] Bygrave (2017), p. 106.

[118] Ibid. p. 117.

[119] Ibid. p. 114.

any condition for the football club to put technical or organizational measures in place to avoid bias and protect persons' rights.

3.3.6. Data protection impact assessment

According to Article 35 of the GDPR, the controller should conduct a data protection impact assessment (DPIA) before putting facial recognition into use, since this type of processing is regarded as high risk under EDPB Guideline 3/2019.[120] This obligation is important in order for FRT users to identify risks and minimize the negative impact on fundamental rights. However, it is possible that the controller will fail to comprehensively consider the risks and fundamental rights involved in the deployment of FRT, because they seek to put their systems into use.

In the two cases, both companies conducted a DPIA before using FRT. As pointed out by the Spanish DPA, the supermarket failed to consider several risks, such as the risk of discrimination, violation of the accuracy principle, and social exclusion of the convicted individuals.[121] For example, even after the sentence has been served and the criminal record is canceled, the convicted person may continue to be identified and denied enter to supermarkets.[122] These risks may also be present in the FRT used by the football club, but the Danish DPA reviewed their DPIA and gave their permission to use FRT with conditions regarding data minimization, transparency and security (see 3.3.4.2-3.3.4.4), which could be helpful in alleviating the privacy risk. These conditions, however, do not include risk-mitigation methods, such as human oversight, to deal with the risk of bias.

To summarize, these data protection principles and data protection by design are useful in addressing some risks associated with FRT, especially interference with privacy. There are other risks, such as bias and discrimination inherent in the algorithm that are difficult to tackle under the GDPR.

3.4. Summary of existing gaps in the framework for privacy and data protection

The legal framework on data protection in the EU is strong and modern.[123] The use of FRT by private entities may, however, challenge the effectiveness of the current framework to protect individuals. The arbitrary use of FRT opens up unprecedented chances for discrimination,

---

[120] EDPB Guideline 3/2019. para 73.

[121] AEPD. PS/00120/2021.

[122] Ibid.

[123] Impact Assessment. p18.

biometric mass surveillance, and significant interference with individuals' privacy and other fundamental rights.[124] Wherever FRT is used, persons who enter that space will be followed, which affects their personal data and autonomy. The use of FRT also undermines freedom of expression, resulting in a chilling effect. Beyond the negative consequences on individual rights, such technology impacts societal and EU values, and principles such as democracy and freedom.[125]

If all Member States choose to strictly interpret the exemptions in article 9 (e.g., public interest and court claims), it may hinder or slow the expansion of FRT in the private sector and thereby minimize the risks associated with FRT. However, there is no clear guidance on how the proportionality principle can be broken down into detailed factors applicable for FRT to balance public interest versus individual rights.[126] Although EDPB Guideline 3/2019 does mention the balancing of interests,[127] it only refers to legitimate interests such as protection of property. Moreover, the criteria it mentions are very broad and general, which can hardly be viewed as clear guidance. This results in contradictory decisions by DPAs. Similar uses of FRT have been blocked by some authorities due to the impact on fundamental rights, whereas permitted by other national authorities to cope with increasing security concerns. Therefore, the risks of biometric mass surveillance and misuse are likely to remain in the EU, especially in countries that are less strict with regard to FRT.

For this reason, if the private use of FRT in publicly accessible spaces is allowed in some Member States, the measures taken by data controllers in accordance with data protection principles and privacy by design are essential to reduce risks and protect individuals' fundamental rights. Unfortunately, there is legal uncertainty on how to apply these rules to FRT.

Furthermore, it is not enough to only place the burden of compliance on the users, because there are so many risks that already exist at an early stage of design and development. System providers are left outside of the scope of the GDPR.[128] The controller is responsible for potential breaches of fundamental rights obligations, but they are often not capable of fully under-

---

[124] Ibid.

[125] Ibid.

[126] Liu. 2009.

[127] EDPB Guideline 3/2019 (para 30) stated that controller need to consider 1)to what extent the video surveillance affects "interests, fundamental rights and freedoms of individuals" and 2) if this causes violates data subject's rights.

[128] Recital 78 states that the producers are not directly bound by this legislation.

standing how FRT works unless they are given all the necessary information. For example, they may not understand how accurate the system is, despite of the fact that this system can never reach 100% accuracy because of the variance inherent in machine leaning. Therefore, they may overly rely on the output generated by the system without confirming whether the outcome is correct. Furthermore, as mentioned in section 2, the risk of bias stems from the training of the algorithm. If the providers are not required to input large amounts of data and ensure the diversity of these data, the risks of bias and discrimination may not be mitigated. Hence, these challenges are likely to remain in the EU.

Rules in the GDPR do afford some level of protection for individuals' fundamental rights, especially the right to privacy. However, legal uncertainty and complexity on how existing rules apply to FRT undermine the effectiveness of the data protection legal framework.[129] Moreover, there are other existing regulatory gaps in the current EU legislation, since the GDPR only addresses challenges relevant to biometric data collection and processing, not the use of this technology or the manufacturing of FRT. As many scholars also pointed out, the GDPR is therefore insufficient to prevent the widespread use of AI, especially regarding machine learning technologies such as FRT. [130] Possible solutions to fill the gaps in the GDPR will be explored in section 5.1.

4. Legal Framework Governing Artificial Intelligence

After looking at the existing legislation that is applicable for FRT, this section will explore emerging new regulation that regulates this technology—the proposed Artificial Intelligence Act (AIA or Proposal). Just like the GDPR, the AIA is a "regulation", not a "directive", and will have binding legal force in the EU.[131] One of the main regulatory targets of this Proposal are AI based remote biometric systems, including FRT (RBS and FRT will be used interchangeably). The EU commission abandoned the idea of banning facial recognition in 5 years,[132] instead choosing to tighten the control over the use of highly intrusive technology. This is undoubtedly a big step towards a better regulatory framework for facial recognition technology.

[129] Renda, et al. (2021), p. 8.

[130] Renda, et al. (2021), p. 36; Wachter, Mittelstadt and Russel (2021), p. 30.

[131] Floridi (2021), p. 216.

[132] Stolton (2020).

This section will discuss rules in the Proposal that are applicable for facial recognition technology, including specific provisions aiming at regulating biometric systems and general regulation for high-risk AI systems, such as facial recognition. It will also assess if the Proposal provides effective protection to persons whose fundamental rights are affected by FRT, and if the AIA is sufficient to complement the GDPR. The following content will analyze the Proposal itself and the cases of using FRT in a supermarket and a stadium.

4.1. An overview of the proposed AI Act

In order to better assess the rules applicable for FRT, it is important to first understand the logic and principle behind this Proposal. This part will present an overview regarding this Proposal by exploring the background and the main features of this regulation. Then it discusses the strengths of the regulatory approach taken by this Proposal.

4.1.1. Background of this legislation

The first step toward regulating AI in the EU was the 2019 publication of *Ethics Guidelines for Trustworthy AI*, which states that trustworthy AI should be "lawful", "ethical" and "robust".[133] The Guidelines called for a clear definition regarding 1) if, when and how AI can be used for automated identification and 2) the difference between identification and tracking of a person, and between targeted surveillance and mass surveillance.[134] This clarification would be crucial to achieve "Trustworthy AI". However, the *Guidelines* does not have binding legal force and it is limited to ethical and robust AI, without discussing Lawful AI.[135]

The next essential step was the February 2020 release of the White Paper on Artificial Intelligence.[136] It pointed out the need for hard law and proposed a risk-based regulation for AI.[137] It explicitly recognized biometric identification as a high-risk application of AI, which should therefore only be used when "duly justified, proportionate and subject to adequate safeguards".[138]

---

[133] HLEG, "Ethics Guidelines".

[134] HLEG. "Ethics Guidelines"; Madiega & Mildebrath (2021), p. 23.

[135] Colonna (2021).

[136] European Commission. "White Paper" (2020).

[137] Ibid.

[138] Ibid.

Finally, in April 2021, the Commission presented the AIA t to address the third component of "Trustworthy" AI, which is "Lawful" AI. The Proposal establishes legally binding norms and institutional mechanisms required for Lawful AI in order to further fill the gap left by *Ethics Guidelines*.[139] The main features and strengths of this legal framework are as follows.

4.1.2. Main features

All AI systems will be classified according to their risks, and subjected to different requirements. There are four level of risk. The first level is "unacceptable risk" AI which infringe on EU values, including harmful AI such as remote biometric systems used by law enforcement.[140] These AI practices will be banned under Article 5 since they pose a danger to individuals' safety, livelihoods and rights.[141]

The second level is "high-risk" AI under Article 6, categorized as such because of their adverse impact on individuals' safety and fundamental rights.[142] Some AI technologies like biometric systems are specifically identified as high-risk, and are listed in Annex III of the Proposal. Such "high-risk AI" will be subject to a conformity assessment before being launched in the market, and must comply with a series of safety requirements such as risk management, human oversight and data governance.[143] Furthermore, post-market surveillance and supervision should be implemented to ensure the compliance with these requirements and obligations for all high-risk AI technologies that have been placed on the market.[144]

The third level is "limited risk" AI, which will be subject to a limited range of obligations such as transparency. The fourth level, "minimal risk" AI, would only be subject to existing legislation without additional legal obligations.

4.1.3. The strengths

The AIA is the first AI legislation proposed by a major group of countries.[145] In an area that was previously full of inconsistent standards and uninspiring proposals, it proposed relatively

---

[139] Madiega & Mildebrath (2021), p. 23.

[140] AIA. Article 5.

[141] Ibid.

[142] AIA. Article 6.

[143] See note 139, p. 25.

[144] AIA. Article 61.

[145] Greenleaf (2021), p. 2.

clear and broad coverage.[146] Considering the rapid technological and market development associated with AI, the Proposal adopts a technology-neutral stance, aiming to adapt to the future as much as possible.[147] The obligations imposed by the Proposal are essential to balance between “innovation-friendliness" and a high level of rights protection.[148]

In terms of biometric technology, the Proposal applies to all remote biometric identification (RBI) systems, including facial recognition technology.[149] It refers to all such systems that operate at a distance, capture biometric data such as facial images, compare it with databases without significant delay and specifically use it to identify a person. [150]

In comparison to the GDPR, which only regulates the user of AI, this Proposal made a significant contribution to Trustworthy AI by imposing more obligations on the provider of the AI programs. The responsibility of controlling risk will not be constrained to the controller, as under the the GDPR, but will also extend to the manufacturer in this new Proposal. This is an essential step to minimize the risks existing at an early stage of design and development and enhance the transparency of the AI system.

In the context of FRT, for example, the algorithm has poorer performance when used on women and darker-skinned people, because of insufficient training data. Under this legislation, the provider has to comply with data governance requirements, which will reduce bias and discrimination. Furthermore, the provider needs to give sufficient information to the user. This will help the controller to understand the limitations of FRT, such as its inaccuracy, and thus will alleviate the risk of misidentification.

In spite of these strengths, it seems that the Proposal does not take a principled approach toward FRT. Detailed analysis regarding rules applicable for FRT in the Proposal will be discussed in the next two sections.

---

[146] Ibid.

[147] Madiega & Mildebrath (2021), p. 25.

[148] EDPB-EDPS. Opinion 5/2021. para 36.

[149] Ibid.

[150] AIA. Recital 8 and Article 3(33).

4.2. Specific provisions regulating remote biometric systems

In this section, the specific rules toward RBS will be examined, including different types of RBS with regard to FRT as defined in this proposal, the prohibition toward certain uses of RBS and the different regulatory mechanisms between RBS used by private and public actors.

4.2.1. Basic rules for different types of RBS in the Proposal

The AIA defines an identification system under Article 3(36) as a remote biometric identification system, and views this system as high-risk AI. [151] Since FRT used for safety reasons collects facial images at a distance for identification, it is therefore falls within the scope of the AIA. Further, Article 3 of the AIA differentiates biometric systems used in "real time" (live)[152] or "post"[153]. The difference lies in whether there is a "significant delay" between the collection and comparison of biometric data.

Rules for the law enforcement use of FRT and uses for other purposes are different (see table2 below). The police use of "real time" RBS in public places is prohibited under Article 5(1)(d), except for significant public security reasons that are authorized by Member States and granted by appropriate judicial authorizations.[154] [155] The other real-time and "post" RBS are classified as "high risk". Hence, FRT deployed in the private sector for safety purposes will be classified as high-risk AI, irrespective of whether it is a real time or post system.

The use of FRT	Real time	Post
Law enforcement purpose	Prohibited with three exemptions	Permitted as high-risk AI
Other purposes, including safety control by private entities	Permitted as high-risk AI (Subject to pre-market requirements; *ex ante* third-party or self conformity assessment; *ex post* market surveillance and supervision)	

Table 2

[151] AIA. Article 3(36).

[152] AIA. Article 3(37). A real-time system collects and compares the data subject against the database "without a significant delay" with the basis of "real-time" materials, such as a video clip that generated by camera.

[153] AIA. Article 3(38). The post system captures biometric data and makes the comparison after a significant delay with the basis of images or video clips from private devices.

[154] AIA. Article 5(1)(d).

[155] The three exceptions are 1) the RBS is used to search for victims of crime and missing children; 2) it is used for the prevention of an imminent threat to the life or physical safety of persons or of a terrorist attack; or 3) it is used for identification of a perpetrator or criminal referred to in the European Arrest Warrant Framework Decision.

4.2.2. The scope of prohibited RBS is too narrow

As mentioned before, the Proposal introduced a ban toward the use of RBS in public spaces.[156] However, the prohibition is restricted to law enforcement purposes with limited conditions, which allows for broad exceptions for FRT and therefore fails to afford sufficient protection for fundamental rights.

Firstly, the Proposal only bans "real time" RBS used by police and does not mention any "post" system. Therefore, it does not prohibit law enforcement agencies from getting access to private databases, which are generated by RBS in publicly accessible places such as shopping malls, sports venues and stores. This means that police can use a private database without any restrictions as set out in the proposal, without even being limited to the three exemptions. As demonstrated before, the possibility that private entities may share biometric data with police will lead to mass biometric surveillance, resulting in a chilling effect.

Secondly, the Proposal also does not intend to prohibit live RBI in publicly accessible spaces by private companies. Thus, retailers could use such systems to identify customers entering the stores to reduce shoplifting and abuse of staff. A concert held in a stadium could employ FRT to prevent banned fans from entering. Schools and transport companies could also use FRT for entrance control.

As a consequence, the prohibition only covers the limited use of biometric systems, and a very limited range of actors.[157] However, as illustrated in Section 2, the use of this technology by private entities also affects fundamental rights in an inevitably disproportionate way,[158] because the technology needs to process a large amount of biometric data, belonging to many individuals, in order to identify a few people.[159] Thus the prohibition should be expanded to cover more organizations which have the power to deploy FRT on a large scale. Moreover, the prohibition should at least be expanded to cover access to private databases by police unless under urgent conditions.

---

[156] AIA. Article 5(1)(d).

[157] Christakis & Mathias & AI-Regulation Team (2021).

[158] Ibid.

[159] Ibid.

4.2.3. The distinction between the use of RBS by public and private sector lacks justification

The AIA distinguishes between the use of FRT by law enforcement and private companies, which creates a "two-tier" regulatory system, providing individuals with "an asymmetric level of protection".[160] It justifies this in Recital 18, which claims that the use of RBS by police is "particularly intrusive" as it may create "a feeling of constant surveillance". [161] The Proposal seems to have made the assumption that the private use of FRT is less intrusive. However, the dangers of biometric surveillance also exist in the private sector. Today AI-embedded facial recognition systems expand the power of private entities and therefore enable new types of misuse, impacting fundamental rights. [162]

By contrast, the GDPR does not contain a distinction between the public and private sectors. The GDPR prohibits the processing of sensitive personal data, irrespective of whether the controller is a public organization. Meanwhile, the AIA does not ban the use of FRT in the private sector, which compromises the protection for affected individuals in the private sector, as private entities are held to lower standards.[163]

This does not mean that the distinction in AIA could not be made legitimately. Yet it should be justified with the reason why the difference is necessary, and why FRT used in private companies causes less harm to individuals' fundamental rights.[164] Beyond the interference with privacy and individual rights, FRT used by private actors in publicly accessible places implies that infrastructure to support the technology can be promoted on a large scale in Member States.[165] If people only notice the infrastructure without knowing if it is currently in operation, it may still lead to a chilling effect. Hence, the spread of FRT could lead to potential abuses of such infrastructure.

Against this backdrop, currently there are many voices calling for stricter rules towards RBS. For example, the EDPB and EDPS advocate a general ban on FRT.[166] The AIA disregards the

---

[160] Smuha, et al. (2021), p. 27.

[161] AIA. Recital 18.

[162] Taylor (2021).

[163] See note 160, p. 25-26.

[164] Ibid.

[165] Ibid.

[166] EDPB-EDPS. Opinion 5/2021. p. 2.

widespread practice of FRT among private organizations.[167] FRT is used in publicly accessible places such as airports, shopping malls, and sports venues, which has a negative impact on individuals' expectations of being anonymous in open spaces.[168] A stricter approach is also necessary because of the serious proportionality problems, as FRT processes "an indiscriminate and disproportionate" amount of biometric data for the purpose of finding a small number of persons.[169] Additionally, civil liberties organizations released an open letter asking for a ban or moratorium on FRT beyond law enforcement purpose to prevent mass surveillance,[170] for the reason that private organizations could collect large amounts of biometric data and share it with authorities.[171]

In summary, private AI-enabled FRT could directly cause a "feeling of constant surveillance". Thus, the gap arises as the "two-tier" approach in the Proposal seems to ignore the widespread private use of biometric systems. To fill the gap, the EU commission should consider tightening the rules for the use of RBI by private actors.

4.2.4. Apply the specific provisions toward the use of FRT in two cases

In the case of the facial recognition systems used in the supermarket and stadium, FRT is used by private companies to detect people entering the space who are on the ban list, for safety reasons. Their systems will be classified as a real time remote biometric identification system. The Proposal does not intend to ban the use of RBS by private and public actors for non-law enforcement purposes. Instead, it imposes limited prohibition regarding RBS, only prohibiting the use of the systems by law enforcement agencies with three exemptions. Consequently, the FRT employed by the supermarket and stadium will not be prohibited under the Proposal, since it is not used for law enforcement purposes.

To summarize, the specific provisions towards RBS differentiate the systems used by law enforcement agencies from those used by other entities, which established an unjustified "two-tier" regulatory system, and overlooked the threat coming from private actors. Therefore, these specific provisions do not afford adequate protection for individuals whose fundamental rights are affected by FRT.

---

[167] Zarra & Favalli & Ceron (2021).

[168] Ibid.

[169] Ibid.

[170] Access now, and EDRi,. et al. (2021).

[171] Ibid.

4.3. General compliance requirements for high-risk AI

High-risk AI applications that are listed in Article 6 and Annex III of the Proposal will be subjected to a set of strict requirements and obligations before placement into the market. In relation to FRT, the most relevant and important requirements include risk assessment, data governance, transparency and human oversight. [172]

Theoretically there would be a third-party conformity assessment to ensure the compliance of RBS with these requirements. However, once there exists a harmonized standard covering these systems, only self-assessment is required. With the ambiguous and complex requirements for high-risk AI, this ineffective approach may result in legal uncertainty, creating a weak protection for affected persons. This section will explore the most relevant requirements in detail and discuss the strengths and weaknesses of these requirements.

4.3.1. Risk assessment (Article 9)

Article 9 of the draft requires organizations to establish, implement, document and maintain a risk management system with regular updates throughout the entire lifecycle of the AI systems.[173] Such a risk management system should estimate current risk and foreseeable misuses, and adopt suitable risk management measures. Furthermore, when eliminating the risks associated with the use of high-risk systems, providers are required to consider the "technical knowledge, experience, education, [and] training" expected by users and the environment in which the system will be used.[174] In addition to risk management documentation, the Proposal requires the testing of AI systems, which shall ensure that these systems are following the requirements listed in this Chapter.[175]

4.3.1.1. The strength

Risk assessment is a valuable tool to achieve the protection of public interest. In relation to FRT, as mentioned in section 2, the risk of discrimination stems from the training of the algorithm. With this obligation, providers will be well placed to mitigate some risks that emerge already in the initial development and design of an AI system. Consequently, they need to consider the risk of product inaccuracy and adopt risk management measures, such as using the diversity and large quantity of training data against

[172] Christakis & Mathias & AI-Regulation Team (2021).

[173] AIA. Article 9(1) and (2).

[174] AIA. Article 9(4).

[175] AIA. Article 9(5).

algorithmic bias. They also have to take into account whether their training data is collected lawfully, and prevent the risk of using pictures of individuals without notification, as mentioned in section 2.3.3. In addition, the provider needs to consider the environment in which FRT will be used, since FRT deployed outdoors or indoors will have different light conditions, which will also influence its accuracy.

4.3.1.2. The weakness

However, the requirement of risk assessment is inconclusive with regard to what types of risk should be considered.[176] Although it requires the identification of "foreseeable risks" associated with an AI system, there are many risks that are irrelevant to the objective of the Proposal, such as financial risks or risks of developmental delays.[177] It should be clear that the relevant risks are associated with safety, fundamental rights and freedoms of persons.[178]

Moreover, the imprecise language will leave excessive discretion for providers in the execution of the risk management process. In the context of FRT, the system may only need to undergo self-assessment if it is covered by harmonized standards. Therefore, it may be up to the provider to decide how to adopt measures to minimize risks until it is acceptable.[179] Because there is no definition regarding what is "residual risk" or sufficient guidance on what makes the risks "acceptable", the decision of which residual risks are regarded as "acceptable" is left to the providers of FRT, who are seeking to market their technology.[180] Moreover, it is possible that providers cannot evaluate all risks, since they depend on different uses of the AI system.[181] Once the system is placed on the market, the risks are associated with the ways users deploy it.[182]

Under the GDPR, the user also needs to carry out a data protection impact assessment, while very often the controller fails to comprehensively consider the risks as they pursue putting their systems into use. As shown in the Spanish case, the supermarket also conducted a DPIA and did not consider many important risks. The same situation may happen to the provider

---

[176] ZVEI (2021).

[177] Ibid.

[178] Ibid.

[179] AIA. Article 9(4).

[180] Fraser & Villarino (2021).

[181] Bergholm (2021).

[182] Ibid.

when they are carrying out the risk assessment, since the FRT provider may face the challenge of whether they should spend a large amount of money and time for a 1% or even smaller reduction in the risk of racial discrimination.[183] The balance between the cost and the performance of products depends on what level of residual risk is acceptable.[184] Thus, regulators need to further clarify what factors and interests should be considered in the cost-benefit analysis. [185]

Although AI providers would be required to communicate these remaining risks to users, this does not bring much relief.[186] For a facial recognition system, even if the provider should communicate with the company intending to deploy FRT, subjects of the system still cannot participate in the risk assessment process. People who are affected by the system should be empowered to participate in the design of risk management and determination of risk-mitigation measures.

4.3.1.3. Apply this requirement to the cases

In the two cases, before deploying FRT in the supermarket and stadium, the providers of the system need to conduct risk assessment throughout such systems' lifecycle. However, this does not require the involvement of affected persons. This means the employees who may walk into the supermarket and football stadium, individuals on the ban list, customers who often go to the stores and football match, and other legitimate stakeholders cannot participate in the process of risk assessment. Consequently, this process is insufficient to protect these persons' rights, especially considering woman and Black people may be disproportionately influenced by the risks of the system.

In conclusion, the lack of involvement of affected stakeholders, and unclear rules in risk assessment with respect to risk evaluation and testing will lead to legal uncertainty and leave a large amount of discretion to AI providers. Thus, this approach is insufficient to safeguard fundamental rights, as previously outlined.

4.3.2. Data governance (Article 10)

The obligation of data governance also lacks conceptual precision. According to Article 10, the training, validation and testing data sets should have "appropriate" statistical properties

[183] See note 180.

[184] Ibid.

[185] Ibid.

[186] AIA. Article 9(4)(c).

and be subject to "appropriate" data governance.[187] Moreover, the processing of special categories of data should be subject to "appropriate" safeguards to ensure bias monitoring. However, it is not clear what composes an appropriate statistical property.[188] For example, in the context of FRT, it is unclear if the data sample should represent the entire population or merely the potentially affected individuals.[189]

4.3.2.1. The strength

Despite the legal uncertainty, it is important that the Article specified the minimal requirements for data sets, especially the stress on data quality as a means to avoid bias.[190] Data accuracy is set out under Article 5 (1) (d) of the GDPR, which requires that the personal data be accurate, kept up to date and that the inaccurate data be erased.[191] The provisions in the AIA extend the data accuracy principle, by requiring the training data set to be "complete" and "free of errors".[192] As mentioned before, the risk of bias stems from the training of the algorithm, as most FRT is trained disproportionately with faces of male and white people, which is left outside of the GDPR's scope. Such risks could be tackled by the data governance obligation under the AIA.

4.3.2.2. The weakness

On the other hand, this might be an unrealistic obligation for AI providers.[193] It is not clear if it is feasible for the data set of FRT to be 100% error free, no matter how well it is analyzed.[194] If the threshold is too high to achieve, or the specific requirements are too abstract to understand, such mechanisms may cause the opposite effects than intended.[195] This rule is likely to be reduced to a box-ticking exercise, since it would be difficult for providers to translate into operational terms.[196] These unrealistic expectations could potentially

---

[187] AIA. Article 10.

[188] Smuha, et al. (2021), p. 33.

[189] Ibid.

[190] Christakis & Mathias & AI-Regulation Team (2021).

[191] GDPR. Article 5 (1) (d).

[192] AIA. Article 10 (3).

[193] Ibid.

[194] Christakis & Mathias & AI-Regulation Team (2021).

[195] Mökander & Axente,. et al. (2021), p. 19.

[196] Ibid.

undermine the legitimacy of the regulatory framework as a whole.[197] Therefore, the Proposal should provide more detailed guidance to facilitate the requirement's effectiveness in practice.

Besides, the amount of data available is also essential. There should be rules ensuring that the dataset used for assessment is large enough to support solid results.[198] When comparing the EU situation with US assessment capabilities developed by NIST, the difference in performance relies on the differences in the amount of data available.[199] This is because the US scientists have a larger amount of data which can be used as a basis for evaluation, while this capability was lacking at the EU level.[200]

4.3.2.3. Apply this requirement to the cases

In the two cases, the providers of FRT need to comply with the data governance requirements and ensure that the training data sets have appropriate statistical properties. But it is not certain if the statistical properties apply to the entire population of their country or merely the potentially affected groups, such as the people who enter the supermarket or stadium. It would also be difficult for the manufacturers to ensure that the data is complete and free of error.

In summary, the rules under the data governance obligation leave a large amount of discretion for AI providers, pursuing "error free" data sets, which seems unrealistic. Hence, this approach can hardly be regarded as adequate for safeguarding fundamental rights.

4.3.3. Transparency obligation (Article 13)

The Proposal intends to facilitate fundamental rights protections for individuals. One of the proposed methods is to impose a transparency obligation. According to recital 32, the design and development of a high-risk AI program should ensure that the program's operation is sufficiently transparent in order for users to interpret the output of the system and use it appropriately.[201] Moreover, high-risk AI applications are required to provide users with instructions that have "relevant, accessible and comprehensible" information.[202] Such information should contain human oversight measures, the capabilities and limitations of the

---

[197] Power. 1997.

[198] See note 194.

[199] Ibid.

[200] Ibid.

[201] AIA. Recital 32.

[202] AIA. Article 13.

systems' performance related to the residual risks to fundamental rights based on the intended use or misuse, and other information.[203] But terms like "sufficiently" transparent and "appropriate" level of transparency leave uncertainty regarding the compliance of AI systems.

4.3.3.1. The strength

Transparency is critical to expose FRT to public supervision and increase risk management by offering the access to remedies. The provisions under the AIA symbolize steps in the right direction. For example, in contrast to the GDPR, the transparency obligation is applicable irrespective of whether the decision making is automated, and of whether personal data is processed.[204] Besides, the GDPR only requires controllers to provide information to the data subjects. The AIA complements GDPR by requiring the controller to receive sufficient information about this product. If the provider gives the user enough information regarding the accuracy of the system, they would be more cautious when they make a final decision to prevent someone entering the place. Hence, transparency is beneficial to address the risk of bias and discrimination.

4.3.3.2. The weakness

However, a significant problem remains in this transparency approach, as the Proposal only emphasizes transparency for users, rather than for those who are potentially affected by the AI system. The user is defined in Article 3 (4) of the Proposal as anyone using the system with the exception of affected individuals.[205] Thus, there is no direct involvement of data subjects during the design and development of FRT. Although GDPR requires that data subjects receive adequate information from controllers, the scope of this information is different from the requirement in the AIA. The draft does not ensure that the general public are provided with adequate information to understand the risks of the FRT that they are exposed to.[206]

As mentioned above, the level of transparency is strongly linked to non-discrimination. However, the draft pays too little attention to algorithmic fairness. The recitals express the concerns regarding the documentation of algorithmic bias[207], yet the requirement to publish

---

[203] AIA. Article 13(3).

[204] Hacker (2021).

[205] AIA. Article 3(4).

[206] Smuha, et al. (2021), p. 35.

[207] Propp & MacCathy (2021). For instance, data governance requires using data regarding sensitive properties for bias monitoring. Another example is that technical documentation must contain metrics used to measure potential discriminatory influence and information about the potential results of risks such as bias.

the documentation regarding fundamental rights infringement is surprisingly lacking.[208] There are no requirements ensuring that these documentation that contains bias assessment will be provided to users, the general public or people potentially influenced by algorithmic bias.[209] The lack of this requirement could not sufficiently safeguard fundamental rights.

Moreover, affected individuals are not equipped with clear routes to contest the use of FRT using the obtained information. The draft does not contain any legal right for individuals to complain to market surveillance authority or sue the provider and user if they failed to comply with the AIA.[210] In comparison, data subjects can complain and seek a judicial remedy under the GDPR. [211] The EDPB and EDPS also criticized the absence of such rights and remedies in AIA.[212]

4.3.3.3. Apply this requirement to the cases

In the two cases, although the supermarket and football club may receive adequate information about the system, the transparency obligation set in the AIA does not mention any information provided for persons who will be subject to this system. While data subjects may get information from the supermarket and stadium based on the GDPR, the scope of information given through the GDPR is different. Consequently, it is difficult for affected individuals, including the employees of the supermarket and the football club, people on the ban list, and potential customers, to get sufficient information in order to safeguard their fundamental rights.

In conclusion, with these limitations and shortcomings, this obligation is not likely to improve existing transparency provisions in practice.[213] Merely notifying the individual that intrusive FRT has been used will hardly provide protections to safeguard human rights.

---

[208] Propp & MacCathy (2021).

[209] Ibid.

[210] Veale & Borgesius (2021), p. 20.

[211] GDPR. Article 77 and 78.

[212] EDPB-EDPS. Opinion 5/2021. para 18.

[213] Veale & Borgesius (2021), p. 17.

4.3.4. Human oversight obligation (Article 14)

Article 14 imposes the obligation of human oversight for high-risk AI systems in order to prevent the risk of infringement on fundamental rights.[214] Article 14(1) states that high-risk AI should be developed with "appropriate" human-machine interface tools, which could be overseen by natural persons when using such systems.[215] Such natural persons should fully understand the capacities and limitations of the system, and remain aware of "automation bias".[216] Article 14(5) imposes an extra oversight obligation when using RBS. In this provision, the output generated by RBS should be verified and confirmed by at least two natural persons, otherwise the user cannot take action or make a decision.[217]

4.3.4.1. The strength

This obligation under the AIA contributes to expand the human oversight under the GDPR, in which human intervention only exists if there is automated processing that produces significant effects on the data subject. The GDPR requires that individuals shall not be subjected to solely automated decision making if the result has legal effects. Meanwhile, under the AIA, human oversight applies irrespective of whether or not the system involved is makes decisions automatically making. Moreover, it clarifies specific human oversight requirements, requiring that two natural persons verify the results, rather than the GDPR rules which only forbid solely automated decision making. This obligation is essential to mitigate the accuracy problem of FRT and reduce discrimination.

4.3.4.2. The weakness

Regardless of how the provisions make effort to strengthen oversight for the protection of fundamental rights, two issues arise. Firstly, it is unclear how the confirmation or verification process is to be conducted, which could reduce the human oversight to "two natural persons" that look at the results on a computer. Instead, two persons should be allocated to divide assessment.[218] For instance, one person should be required to sight the identified individual in question rather than only look at the screen.[219]

---

[214] AIA. Article 14(2).

[215] AIA. Article 14(1).

[216] AIA. Article 14(4).

[217] AIA. Article 14(5).

[218] Smuha, et al. (2021), p. 35.

[219] Ibid. p. 35.

Secondly, if there is no basis to deploy FRT, the protective measure of human oversight shall not become the legitimate reason to do so.[220] Allowing machines to make decisions based on data has impact on individuals, groups or the entirety of society.[221] For this reason, high-quality and meaningful human oversight should be used to moderate the adverse influence of FRT, rather than legitimize the use of such technology. Even if FRT has been demonstrated to be proportionate, human oversight can only be used as a means to mitigate risk, not the as an excuse for deploying this system.

The danger of over-reliance on the outputs of a facial recognition system is best evidenced though the system employed by Livonia, used in a skating rink to stop people who have violent behavior from entering the area. A Black teenage girl named Lamya tried to enter the skating rink with friends, despite having never been there, and was refused entry because she was misidentified as someone who was involved in a brawl at the same place.[222] The decision made by the skating rink was based only on the output produced by the facial recognition system used by Livonia, which had this girl at a 97% match. This shows that if the decision-maker merely depends on the output of the facial recognition system, and does not have the technical knowledge to understand how FRT works and to take the limitations into account, negative effects can be caused even in the private sector.

4.3.4.3. Apply this requirement to the cases

The human oversight obligation does not afford much relief for the potential bias in the system used in the supermarket and stadium. In this provision, the result of the identification system should be verified and confirmed by at least two natural persons, otherwise the user of the system will not be able to take action or make a decision using the result. However, merely allocating two security guards in front of one computer to assess if this person on the screen is the same person who is banned from entering the store or stadium, does not provide enough measures to avoid bias.

In view of the above, the protection provided by the mandatory requirements of high-risk AI systems should be strengthened and the open questions these requirements raise need further clarifications.

---

[220] Ibid. p. 36.

[221] EDPB-EDPS. Opinion 5/2021. para 5.

[222] Wimbley (2021).

4.3.5. Standard setting and conformity assessment

To ensure that FRT meet the above requirements, such systems will be subject to stricter conformity assessment procedures in accordance with Article 43 of the AIA.[223] Article 61 also introduced an *ex post* monitoring system for market surveillance, as well as supervision of these systems by competent authorities in Member States. [224]

4.3.5.1. The strength

Standardization is essential to help FRT comply with the regulations, by providing technical solutions.[225] Since these systems are extremely intrusive and could potentially infringe upon fundamental rights, in principle they need to undergo an *ex ante* conformity assessment by a third party.[226] The third-party conformity assessment is more strict than a self-assessment, like other high-risk AI systems need to conduct, which could further enhance legal certainty and public confidence in FRT.[227] In addition, the *ex post* monitoring system would be helpful to avoid potential breaches after the AI system has been put into the market.

4.3.5.2. The weakness

However, this proposed standardization process may lead to inadequate democratic participation for two reasons. Firstly, the detailed standards for FRT are lacking at the EU level. As noted, the requirements in the Proposal are general, while more detailed technical requirements will be mainly specified through European standardization.[228] Hence, the development of detailed standards is essential to the effective implementation and enforcement of the Proposal.[229]

Secondly, the standardization process is industry-led, and therefore lacks democratic oversight.[230] This is because the rule-making power is usually delegated to bodies (ie. CEN/

---

[223] AIA. Article 19 and 43.

[224] AIA. Article 61.

[225] Madiega & Mildebrath (2021), p. 30.

[226] Ibid.

[227] EDPB-EDPS. Opinion 5/2021. para 37.

[228] Smuha, et al. (2021), p. 54.

[229] Ibid.

[230] Madiega & Mildebrath (2021), p. 30.

CENELEC)[231] that are governed by private law.[232] Such a practice is controversial, and its legal ground is increasingly unstable.[233] Another reason is that the public and stakeholders, such as consumer representatives and civil society organizations, often struggle to participate in standardization, due to a lack of resources and relevant knowledge.[234]

In theory, a specific notified body must assess the conformity of high-risk RBIS, while in practice, once there exists a harmonized standard covering these systems, only a self-assessment is required.[235] As the commission wish the harmonized standards to exist before the application of the regulation, the specific notified body for biometric systems may never be established.[236] This self-regulation has been welcomed and complimented by industry.[237] However, such an approach leaves excessive discretion for AI providers and developers, who have major incentives to deploy these systems, which is not enough to protect societal values.[238] Augmented by the imprecise language in the text, this mechanism may result in a derogation for the conformity assessment procedure.[239]

The self-assessment undermines the apparent level of protection and revelation, since it is only an internal inspection without any auditing report for the general public or authority to review.[240] The AI system will only have a "mark" which is attached to deliver the message to the public that it complies with requirements.[241] The reliability of the CE mark[242] has been

---

[231] The European Committee for Standardization (CEN) and the European Electrotechnical Committee for Standardization (CENELEC) are responsible for developing and defining voluntary standards at the European level.

[232] Veale & Borgesius (2021), p. 24-25.

[233] This has been criticized for many years as a result of many reasons, including the lack of democratic supervision, insufficient participation of stakeholders who might be subjected to adverse impact, the lack of appropriate judicial control over harmonized standards.

[234] See note 232.

[235] AIA Article 43(1).

[236] See note 232.

[237] Sébastien (2021).

[238] Kop (2021).

[239] Mökander & Axente,. et al. (2021). p. 20.

[240] Propp & MacCathy (2021).

[241] Ibid.

[242] "CE Marking". The CE Mark refers to the EU conformity marking for regulating the products traded within the European Economic Area.

criticized for many years.[243] Although the providers are required to draft a "declaration of conformity" and hand it to authorities, even the statement of compliance can be withheld from the public.[244] Therefore, the absence of oversight raises concerns, as high-tech companies need to wedge between innovation and social responsibility.[245] They may not act ethically when making decisions related to the design of products that could potentially infringe upon fundamental rights.

Apart from the *ex ante* conformity assessment, the *ex post* monitoring system for market surveillance also remains uncertain. Although the logic behind an *ex post* monitoring system is clear, many practical details need further explanation. For instance, the AIA requires that documentation needs to be kept for a duration which is "appropriate" for the intended purpose of the AI application.[246] Yet it does not mention how long is suitable or whether the provider or the authority is responsible for the decision.[247] There is also a risk of incoherent implementation across the EU, due to the uneven resources and different approaches chosen by Member States, which may lead to inconsistency and potentially weaken the protection of fundamental rights.[248]

4.3.5.3. Apply this requirement to the cases

For the facial recognition systems used in the store and stadium, there will be an *ex ante* conformity assessment. Their systems will undergo a self or third-party assessment, depending on whether the FRT is covered by a harmonized standard. There will also be an *ex post* system for market surveillance and supervision by competent authorities designated by Member States. But as these systems are still being shaped, it is not known if the *ex post* system can offer adequate protection for affected individuals in the future.

In sum, the standardization and conformity assessment are insufficient for the protection of fundamental rights, since the standardization process lacks democratic supervision and the self-assessment will leave discretion for AI providers who seek to put their products into the market. Despite the fact that FRT will be subject to *ex post* monitoring, this does not bring

---

[243] Stuurman & Lachaud (2021).

[244] Ibid.

[245] Nicol (2018).

[246] AIA. Article 20.

[247] Mökander & Axente,. et al. (2021), p. 21.

[248] Smuha, et al. (2021), p. 54.

much relief, as it may cause inconsistency and incoherence in the EU due to the uneven resources and different methods chosen by Member States.

4.4. Summary of gaps in the framework governing artificial intelligence

While the AIA is intended to tighten the use of FRT in order to safeguard fundamental rights, many issues remain under the specific provisions regulating RBS, the general requirements and conformity process governing high-risk AI. These issues include the narrow scope of prohibited FRT, the weak protection toward non-law enforcement use of FRT, the unclear and insufficient approach for compliance requirements, the lack of public oversight over the process of standardization and the excessive discretion of self-assessment. Moreover, there remains uncertainty regarding the interplay of the GDPR and the Proposal.[249]

Thus, it is hard to justify that the AIA will solve issues regarding the use of FRT. The existing legislation has been criticized for the lack of public oversight in governance of FRT, since the development and maintenance of such systems are outsourced to private entities. [250] Yet the same problem also exists in the Proposal. The increasing concerns of FRT that are not sufficiently covered by the current EU regulatory framework are not likely to be solved through the AIA, partly due to the vagueness and complexity in provisions.

Consequently, gap arises as the AIA fails to afford adequate protection for individuals who will be subject to FRT and potentially adversely affected by it. This can also be demonstrated by the case analysis regarding the use of FRT in the supermarket and stadium, where the pre-market requirements are mainly imposed on the providers, and the approaches to public oversight and involvement of affected individuals are lacking.

In conclusion, as an answer to sub-question 3, the Proposal permitted the use of facial recognition systems by private and public actors for safety purposes only if the system complies with pre-market requirements. Identification systems are classified as high-risk AI and therefore subject to more strict obligations before placement into the market. Although there are many requirements that aim to tighten the use of FRT, the gaps arise for issues such as lack of public oversight and meaningful involvement of affected persons. Consequently, the AIA is insufficient to safeguard fundamental rights for people who are exposed to facial recognition systems, especially considering the vulnerable group.

---

[249] Renda, et al. (2021), p. 36.

[250] Ibid.

5. Recommendations to close the gap in the GDPR and AIA to address challenges raised by FRT

As illustrated in sections 3 and 4, both the GDPR and the AIA are insufficient to safeguard fundamental rights impacted by FRT, in spite of their intention to strengthen the requirements of deploying such technology. This section will provide suggestions for data protection regulatory framework and the AIA to make these rules more efficient and clearer, in order to close the gap. Since the AIA is a proposal that is still being developed, this section will give more suggestions for the draft with respect to the specific provisions, compliance requirements and standardization process for high-risk AI, and the relationship between the GDPR and the AI regulation.

5.1. Reduce vagueness and complexity in the GDPR

The proportionality principle is critical to prevent the widespread of FRT by critically evaluating whether private entities could rely on exemptions in order to use FRT for safety reasons in publicly accessible places. Thus, the specific criteria and factors need to be clarified when assessing the necessary and proportionate use of such a system, particularly when it is used in a large crowd, based on the exemptions of the public interest or a court claim. The guidance should be clear about the conditions under which private organizations could deploy FRT for the public interest without disproportionately infringing upon individual rights. This thesis suggested several criteria in section 3.3.3 (see Table 1) when analyzing the two cases, such as the weight given to the consequences to individual rights and seriousness of potential damage, and the presence of adequate risk-mitigation measures.

Even if the private use of FRT has been demonstrated to be necessary and proportionate, other data protection principles also need to be incorporated into the deployment of FRT under the requirement of data privacy by design and by default. Article 25 of the GDPR is a valuable rule to create a mindset for the data controller of consistently putting privacy as a priority when developing system requirements.[251] Thus, data privacy by design and by default should set clear goals and legal incentives for data controllers and engineers in achieving privacy protection goals. [252]

5.2. The Proposal should take a principled approach toward RBS

In order to ensure that the design and deployment of FRT is "legally trustworthy", the AIA needs to adopt a new approach toward RBS.

[251] Bygrave (2017), p. 120.

[252] Ibid.

5.2.1. Expand the scope of prohibited RBS

The Proposal should expand the prohibition on use of RBS for law enforcement purposes beyond "real time" use. Police should be prohibited from accessing private databases except in urgent situations. This way, biometric data collected by private entities, such as the supermarkets and stadiums, may only be shared with law enforcement agencies under the restrictions set out in the Proposal.

The Commission should also consider extending the prohibition to some private actors. If the Commission still decides to allow the use of FRT by private organizations due to justified reasons and conditions, these users should be subject to more meaningful obligations than the current general requirements for all high-risk AI systems.

5.2.2. Private use of RBS needs the same level of protection

The Proposal should justify the necessity of the "two-tier" approach to regulating remote biometric systems that differentiates the systems used by public and private entities. If the Commission cannot give a reasonable justification, they should not overlook the danger posed by private organizations. Considering that FRT is likely to be widespread, leading to chilling effects, the Proposal should reconsider the justifiability of the distinction, and tighten the rules for private use of FRT.

5.3. Ensure an effective framework for compliance requirements and conformity process

Compliance requirements and conformity procedures are critical in addressing the challenges of biometric systems by offering meaningful and effective protection of fundamental rights. However, the current pre-market requirements are complex and ambiguous. In order to increase the effectiveness of the regulatory approach, the Commission should strengthen the protection level of fundamental rights and clarify the remaining questions in the Proposal.

5.3.1. Involve legitimate stakeholders in the risk assessment

The risk assessment would be critical in determining the effectiveness of the requirements and obligations imposed on high-risk systems such as FRT. The risks regarding fundamental rights should be stated explicitly. The Proposal should also be clear regarding what measures are suitable to ensure residual risks and what risks can be regarded as acceptable. Moreover, the risk assessment should be conducted by both the provider and the user, considering where the

AI system will be used.[253] The providers and the users should also communicate to all stakeholders, such as the affected individuals, what level of risk can be considered "acceptable". All of these elements are essential for the protection of fundamental rights, and therefore should not be neglected by the Commission.

5.3.2. Reduce uncertainty in data governance

Data governance is essential to protect biometric data collected and processed by a facial recognition programs. The Commission should lay down specific criteria regarding what is an "appropriate" process for testing a data set against algorithmic bias. For FRT, a large amount of data could improve the overall accuracy of the system but discriminate against specific ethnic groups. Thus, regulatory mechanisms in the AIA need to define fairness in different conditions, and give guidance on how to balance different interests and justify ethical trade-offs.[254]

Furthermore, the high expectations of algorithm development and data set should be broken down into detailed and applicable estimation metrics and industry standards, which is more practical for compliance.[255] Finally, in addition to focusing on accuracy of the data, the Commission should not neglect the integrity of the data. In Article 10(3), requirements on data sourcing and data integrity should be added to confirm the legitimacy of the origins of the data.[256]

5.3.3. Enhance transparency requirements to mitigate bias

The need for transparency is strongly associated with ways to mitigate the risks posed by the use of FRT, especially when it comes to non-discrimination, access to remedies, and effective administration. For this reason, the AIA should ensure that not only commercial users, but also the general public and affected individuals can obtain comprehensive information, so that they can exercise their fundamental rights. The AIA should establish a transparency framework in accordance with the needs of affected individuals.[257] For example, the trade-offs in the algorithmic design need to be disclosed to the public and those impact by FRT.[258]

---

[253] Bergholm (2021).

[254] Mökander & Axente,. et al. (2021), p. 23.

[255] Ibid.

[256] Smuha, et al. (2021), p. 57.

[257] Ibid.

[258] Mökander & Axente,. et al. (2021), p. 24.

Moreover, affected individuals should be able to contest the deployment of FRT using information from AI providers or users. The Proposal should also empower affected individuals to request specific information from both the providers and the users of the AI system. This would enable such affected individuals to use the information they receive to contest the intrusive use of AI systems, especially when the output of the system lead to discrimination and affects other fundamental rights.[259]

5.3.4. Strengthen human oversight obligation

In order to avoid biased decision-making patterns, human oversight should be required in all processes.[260] For high-risk AI, various safeguards should be required to guarantee that individuals' rights, in particular rights related to non-discrimination, are respected.[261] There should be some guidelines to further clarify how to properly evaluate bias and to adopt human oversight measures.

For the specific provision set out in Article 14 (5), which requires the results of RBS to be verified by at least two persons, that confirmation should be based on a separate assessments. Moreover, the Commission should stress that human oversight is not a justification for the use of facial recognition. It should only be used as a means to protect fundamental rights.

5.3.5. Improve standard setting and conformity assessment

Standard development will play an essential role in the effective implementation and enforcement of the Proposal. In order to ensure a meaningful conformity assessment, the draft should enhance democratic participation. The Commission should take measures to ensure that relevant stakeholders, such as consumer representatives and civil society organizations, are sufficiently represented in the standard-setting process.[262] Facial recognition systems must be subject to an external, independent third-party assessments.[263] And this conformity assessment procedure, including the balance between different interests, needs to be disclosed to the public.

---

[259] Ibid.

[260] EDPB-EDPS. Opinion 5/2021. para 59.

[261] Ibid.

[262] Smuha, et al. (2021), p. 40.

[263] Kop (2021).

It should also be clear that even if an AI system complies with the AIA, this does not mean that it also fulfills safeguards set in the GDPR. It is recommended to include an additional requirement to ensure that the AI systems also comply with the GDPR in the conformity assessment, which will help ensure compliance with the principles of accountability.[264]

5.4. Clarify the relationship between the AIA and the GDPR

The relationship between the Proposal and the current data protection legislation should be clarified to enhance the protection of fundamental rights for individuals who are exposed to high-risk AI like FRT.[265] A clear and coherently defined relationship is an essential precondition to support and maintain an environment that encourages innovation and respects human rights.[266]

The AIA and GDPR should supplement each other in setting harmonized rules that regulate the design, development and use of biometric systems, as well as restrictions on certain applications of FRT. In view of fundamental rights, the new rules should not interfere with current regulatory mechanisms in a way that will weaken existing protection standards. This should also include governance by competent authorities.

Although the AIA does include some correspondence with the GDPR, uncertainty and incoherence still exist.[267] The AIA handles facial recognition systems that rely on biometric data, unlike the GDPR. The GDPR requires stricter protection of "special categories of personal data" and holds it to a higher standard of protection by setting important thresholds for data processing, no matter if it belongs to the private sector or a public authority. Yet the Proposal does not provide similar protection. There is also an open question under the AIA regarding whether AI providers could use data collected outside of EU in violation of fundamental rights, for algorithm training.

Therefore, in addition to clarifying the uncertainty, it is essential for the EU commission to strengthen the relationship between the AIA and GDPR to prevent inconsistency and potential conflict. This will not only enhance legal certainty, but also increase the level of protection of

---

[264] Bergholm (2021).

[265] EDPB-EDPS. Opinion 5/2021. p. 3.

[266] Ibid.

[267] Article 10 (5) allows the provider to process social categories of personal data when it is necessary for bias monitoring. Article 29 requires users to conduct a data impact assessment under Article 35 of the GDPR using information obtained under Article 13 of the AIA.

fundamental rights in order to avoid direct or indirect threats to personal data.[268] For instance, since FRT is a type of machine leaning AI, the rights related to automated decision making under Article 22 are essential for data protection. Hence, the right to deletion and correction in accordance with the GDPR should be included in a facial recognition system since the beginning of technical architecture design.[269] Another example is the training of the algorithm. Data subjects should be informed of whether their data is used for such purposes, and their rights regarding restriction of processing[270] and deletion of data[271] should always be ensured.[272]

To conclude, it is important to enhance the connection between the two legislations, considering how little the AIA mentions the GDPR while AI systems rely heavily on personal data.[273] As recommended by the EDPB and EDPS, there should be a statement to confirm that the GDPR is applicable for data processing within the scope of the AIA.[274] By doing this, the data protection framework for FRT will be made more consistent.

6. Conclusion

Regulating facial recognition systems is difficult, as this AI-enabled technology is inherently "opaque", and there exists the tension between private or public entities' interest in enhancing security, and affected individuals' interest in safeguarding their rights.[275] On October 6, 2021 the European parliament adopted a resolution which called for a moratorium on the use of facial recognition identification systems for law enforcement purpose unless certain criteria were fulfilled.[276] [277] The parliament also expressed concern over the police use of private

[268] EDPB-EDPS. Opinion 5/2021. para 57.

[269] Ibid.

[270] GDPR. Article 18.

[271] GDPR. Article 16.

[272] Ibid.

[273] Bergholm (2021).

[274] Ibid.

[275] Wright (2018), p. 651.

[276] European Parliament (2021).

[277] These criteria for such system include that it is used strictly for identifying victims of crime, fully fundamental rights compliant, non-biased, necessary and proportionate. The law also affords safeguards against misuse and democratic supervision.

facial recognition databases.[278] It called law enforcement agencies to disclose whether they are using a private database.[279] Mass biometric surveillance in the private sector also undermines essential fundamental rights such as the right to privacy, non-discrimination and freedom of expression. So far, the EU has not made enough progress preventing the arbitrary use of FRT. The legal framework for facial recognition technology used in the private sector should therefore be stringent in order to protect fundamental rights.

Although the current legislation, the GDPR, is applicable for regulating biometric data, a gap arises as there are many risks, uncertainties and complexity in the implementation of the GDPR. As demonstrated by the two cases from the Spanish and Danish DPAs, without clear guidance in assessing the proportionality of using FRT, different Member States interpret the public interest in different ways. The lack of the guidance will allow the widespread use of FRT in the private sector. Additionally, the GDPR only regulates the controller, while many risks already exist in design and development stages.

Further, the EU commission released the proposed AI regulation, aiming to tighten the use of FRT. The emerging legislation has specific provisions regulating remote biometric systems, and lists a set of pre-market requirements for high-risk AI. However, uncertainty and complicity in the Proposal may undermine the intended protection. Moreover, gaps remain as the Proposal does not seem to take the impact of biometric systems on fundamental rights seriously enough. Under this Proposal, most biometric systems are not required to demonstrate a justification for their use if they comply with rules for high-risk systems. The ineffective approach in many requirements may lead to insufficient protection of fundamental rights. This leads to a biometric-tolerant regime, leaving unreasonable discretion to AI-based FRT providers. Thus, the Proposal does not offer meaningful and effective protection for people whose fundamental rights may be affected by biometric systems.

Without sufficient protection provided by regulatory framework, it is hard to justify the use of FRT simply for convenience or efficiency when it overrides these fundamental rights and potentially causes dystopian reality. The providers and users of FRT ought to justify the legitimate purpose, necessity and proportionality of biometric systems. For this reason, there is a need to bring some changes to the standardization process, especially granting effective participation rights for stakeholders, and making the standardization system more transparent and comprehensive.

---

[278] European Parliament. 2021.

[279] Ibid.

In light of above, this thesis therefore suggests that the GDPR should further reduce the complexity and vagueness of the regulations. There should be clear guidance regarding which factors that must be considered when assessing the proportionality of using FRT.

The AIA should take a principled approach towards remote biometric systems. It should prohibit law enforcement agencies from using private databases and reconsider the "two-tier" approach that differentiates the systems used by public and private entities. In addition to the specific rules toward RBS, the thesis also recommends that the Proposal ensure an effective framework for pre-market requirements and a conformity process. Finally, the relationship between the AIA and the GDPR should be strengthened in order to maintain a more coherent and comprehensive data protection framework for AI systems, and therefore achieve legally trustworthy AI by contributing to the rule of law.

These recommendations consider the importance of democratic supervision and suggest the meaningful involvement of legitimate stakeholders, addressing the real issues with biometric information. The recommendations will be helpful in closing the existing regulatory gaps, affording effective and sufficient protection for individuals who will be subject to this technology. Hopefully, in the near future, with adequate protection provided by a legal framework, we will not live in a dystopian nightmare, where our bodies are reduced to walking barcodes. Instead, FRT will only be used when it is necessary to protect our security.

Table of reference

Legislations

European Union. Charter of Fundamental Rights of the European Union (2012/C 326/02) (26 October 2012) . (CHR)

Council of Europe. Convention for the Protection of Human Rights and Fundamental Freedoms CETS No.5 (3 September 1953). (ECHR)

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)

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, 2021/0106(COD)

Danish Parliament. Danish Data Protection Act. act. no. 502 of 23 May 2018.

Spanish Parliament. Spanish Data Protection Act. Organic Law 3/2018.

Judgments

CJEU Joined Cases C−203/15 and C−698/15 (21/12/2016), Tele2 Sverige v. Post och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others.

A29WP Documents

Article 29 Data Protection Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

EDPB/EDPS Documents

EDPB. Guidelines 3/2019 on processing of personal data through video devices.

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

EU Commission Documents

European Commission, White Paper on Artificial Intelligence, COM(2020) 65 final. 19 February 2020.

The High Level Expert Group set by European Commission, Ethics Guidelines for Trustworthy AI. COM (2019). 8 April 2019.

Secondary Literatures

Books

Handbook on European Data Protection Law, *European Union Agency for Fundamental Rights*, 2018, p.131.

Handbook on Preventing unlawful profiling today and in the future: a guide. *European Union Agency for Fundamental Rights*, 2018.

Renda, Andrea., et al. Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe. 2021, p.43. doi: 10.2759/523404.

Zhao, Wenyi, and Rama Chellappa, eds. Face Processing: Advanced modeling and methods. Elsevier, 2011, p.10-11.

Academic Journals

Aggarwal, Gaurav, et al. "Physics-based revocable face recognition." 2008 IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2008.

Bygrave, Lee A. "Data protection by design and by default: Deciphering the EU's legislative requirements." *Oslo Law Review* 4.02 (2017): 105-120.

Bygrave, Lee A. "Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions." *Version* 2 (2020).

Bygrave, Lee A. "Minding the machine v2. 0: The EU General Data Protection Regulation and automated decision making." Algorithmic Regulation (Oxford University Press 2019, Forthcoming, University of Oslo Faculty of Law Research Paper No. 2019-01 (2019).

Carter, Anthony M. Facing reality: The benefits and challenges of facial recognition for the NYPD. Naval Postgraduate School Monterey CA United States, 2018.

Chen, Y. Amy. "Your Face Is a Commodity, Fiercely Contract Accordingly: Regulating the Capitalization of Facial Recognition Technology through Contract Law." *Notre Dame Journal of Law, Ethics & Public Policy, vol*. 34, no. 2, 2020, p. 501-528.

Christakis, Theodore and Mathias, Becuywe & AI-Regulation Team, Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021, AI-Regulation.com, May 27th, 2021, https://ai-regulation.com/facial-recognition-in- the-draft-european-ai-regulation-final-report-on-the- high-level-workshop-held-on-april-26-2021/

Chun, Sarah. "Facial Recognition Technology: A Call for the Creation of a Framework Combining Government Regulation and a Commitment to Corporate Responsibility." *NCJL & Tech*. 21 (2019): 99.

Colonna, Liane. "Legal Implications of Using AI as an Exam Invigilator." *Faculty of Law, Stockholm University Research Paper* 91 (2021).

Floridi, Luciano. "The European Legislation on AI: a Brief Analysis of its Philosophical Approach." *Philosophy & Technology* (2021): 1-8.

Frantziou, Eleni. "The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Structural Constitutional Principle." *Cambridge Yearbook of European Legal Studies*, vol. 22, 2020, pp. 208–232., doi:10.1017/cel.2020.7.

Fraser, Henry L., and Jose-Miguel Bello y Villarino. "Where Residual Risks Reside: A Comparative Approach to Art 9 (4) of the European Union's Proposed AI Regulation." *Available at SSRN 3960461* (2021).

Fuster, Gloria Gonzalez, and Hielke Hijmans. "The EU rights to privacy and personal data protection: 20 years in 10 questions." (2019)

Greenleaf, Graham. "The 'Brussels Effect'of the EU's 'AI Act'on Data Privacy Outside Europe." (2021).

Hacker, Philipp, and Jan-Hendrik Passoth. "Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond." *From the GDPR to the AIA, and Beyond (August 25, 2021)* (2021).

Hacker, Philipp. "Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law." *Common Market Law Review* 55.4 (2018). Vol.55 (4), p.1143-1185.

Kop, Mauritz. "EU Artificial Intelligence Act: The European Approach to AI." Stanford-Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments, Stanford University, Issue, 2021.

Kosinski, Michal. "Facial recognition technology can expose political orientation from naturalistic facial images." *Scientific reports* 11.1 (2021): 1-7.

Leopold, David A., and Gillian Rhodes. "A comparative view of face perception." *Journal of Comparative Psychology* 124.3 (2010): 233.

Leslie, D. Understanding bias in facial recognition technologies: an explainer. *The Alan Turing Institute*. 2020. https://doi.org/10.5281/zenodo.4050457

Lewis, James A. "How does facial recognition work? A primer."*Center for Strategic and International Studies (CSIS)* (2021).

Liu, Yue. "The principle of proportionality in biometrics: Case studies from Norway." *Computer Law & Security Review* 25.3 (2009): 237-250.

Madiega, Tambiama and Mildebrath, Hendrik. "Regulating Facial Recognition in the EU." *Digital Frontiers Institute*, 30 Sept. 2021, https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

Mendoza, Isak, and Lee A. Bygrave. "The right not to be subject to automated decisions based on profiling." *EU Internet Law*. Springer, Cham, 2017. 77-98.

Mökander, Jakob, et al. "Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI Regulation." *Minds and Machines* (2021): 1-28.

Nativi, Stefano and De Nigris, Sarah, AI Standardisation Landscape: state of play and link to the EC proposal for an AI regulatory framework, EUR 30772 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-40325-8 (online), doi:10.2760/376602 (online), JRC125952.

Nicol, Turner L. "Detecting Racial Bias in Algorithms and Machine Learning." *Journal of Information, Communication & Ethics in Society*, vol. 16, no. 3, 2018, pp. 252-260. *ProQuest*, https://www.proquest.com/scholarly-journals/detecting-racial-bias-algorithms-machine-learning/docview/2130244072/se-2?accountid=14699, doi:http://dx.doi.org/10.1108/JICES-06-2018-0056.

Quintel, Teresa. "The First GDPR Fine in the Country of Openness: Is Sweden Moving towards More Privacy?." *Eur. Data Prot. L. Rev.* 5 (2019): 548.

Rowe, Elizabeth A. "Regulating Facial Recognition Technology in the Private Sector." *Stanford Technology Law Review* 24.1 (2020).

Smuha, Nathalie A. "The eu approach to ethics guidelines for trustworthy artificial intelligence." *Computer Law Review International* 20.4 (2019): 97-106.

Smuha, Nathalie A., et al. "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act." *Available at SSRN* (2021).

Stuurman, Kees, and Eric Lachaud. "Regulating AI. A label to complete the newly proposed Act on Artificial Intelligence." *Available at SSRN 3963890* (2021).

Tangerding, Ellen. Beyond Data Protection: Applying the GDPR to Facial Recognition Technology. University of Twente, 2021.

Taylor, Linnet. "Public actors without public values: legitimacy, domination and the regulation of the technology sector." *Philosophy & technology* (2021): 1-26.

Veale, Michael, and Frederik Zuiderveen Borgesius. "Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach." *Computer Law Review International* 22.4 (2021): 97-112.

Wachter, Sandra, Brent Mittelstadt, and Chris Russell. "Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI." *Computer Law & Security Review* 41 (2021): 105567.

Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. "Why a right to explanation of automated decision-making does not exist in the general data protection regulation." *International Data Privacy Law* 7.2 (2017): 76-99.

Wang, Yilun, and Michal Kosinski. "Deep neural networks are more accurate than humans at detecting sexual orientation from facial images." *Journal of personality and social psychology* 114.2 (2018): 246.

Ward, Angela. "The Impact of the EU Charter of Fundamental Rights on Anti-Discrimination Law: More a Whimper than a Bang?" *Cambridge Yearbook of European Legal Studies*, vol. 20, 2018, pp. 32–60., doi:10.1017/cel.2018.11.

Welinder, Yana. "A face tells more than a thousand posts: developing face recognition privacy in social networks." *Harv. JL & Tech.* 26 (2012): 165.

Woodward Jr, John D., et al. Biometrics: A look at facial recognition. RAND CORP SANTA MONICA CA, 2003.

Wright, Elias. "The future of facial recognition is not fully known: Developing privacy and security regulatory mechanisms for facial recognition in the retail sector." *Fordham Intell. Prop. Media & Ent. LJ* 29 (2018): 611.

Zarra, Antonella, Silvia Favalli, and Matilde Ceron. "Pandemic-Sanctioned AI Surveillance: Human Rights under the Threat of Algorithmic Injustice in the EU." *Available at SSRN 3939747* (2021).

Other Literatures

"AEPD (Spain) - PS/00120/2021 case summary." *GDPRhub*, 26 July 2021, https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS/00120/2021 (AEPD. PS/00120/2021)

Agencia Española de Protección de Datos. 26 July 2021, https://www.aepd.es/es/documento/ps-00120-2021.pdf

Allevate. "How to Measure Facial Recognition Error Rates in Surveillance Applications." 28 Apr. 2020, https://allevate.com/2018/05/10/how-to-measure-facial-recognition-error-rate/#:~:text=In a facial recognition system: a False Positive,person are in fact of the same person.

Bergholm, Jenny. "EDPB-EDPS Opinion: Four Lessons for the AI Regulation and Data Protection." *CITIP Blog*, 10 Sept. 2021, https://www.law.kuleuven.be/citip/blog/edpb-edps-opinion-four-lessons-for-the-ai-regulation-and-data-protection/.

"#BigData: Discrimination in Data-Supported Decision Making." *European Union Agency for Fundamental Rights*, 18 June 2021, https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making.

Castelluccia, Claude and Inria, Daniel Le Métayer. Impact Analysis of Facial Recognition: Towards a Rigorous Methodology. 2020. https://hal.inria.fr/hal-02480647/document

Castro, Daniel. "Are Governments Right to Ban Facial Recognition Technology?" GovTech. May 2019. Accessed November 06, 2021. https://www.govtech.com/products/are-governments-right-to-ban-facial-recognition-technology.html.

CCDCOE. 'CJEU declares general data retention unlawful in Tele2 Sverige.NATO Cooperative Cyber Defence Centre of Excellence.Tallinn. Accessed November 19, 2021. https://ccdcoe.org/incyder-articles/cjeu-declares-general-data-retention-unlawful-in-tele2-sverige/#footnote_3_2991.

"CE Marking." *Internal Market, Industry, Entrepreneurship and SMEs*, https://ec.europa.eu/growth/single-market/ce-marking_en.

Committee on Legal Affairs Working Group on Legal Questions related to the Development of Robotics and Artificial Intelligence, 22 October 2015, European Parliament. https://www.europarl.europa.eu/cmsdata/94927/Minutes_WG_Robotics_Oct.pdf

Dautlich, Marc., et al. "Lessons Learned: Completing a DPIA for an AI Use Case." *Bristows*, 10 Nov. 2020, https://www.bristows.com/news/lessons-learned-completing-a-dpia-for-an-ai-use-case/.

Duren, Erin. “New York School District's Facial Recognition System Sparks Privacy Fears.” *The Guardian*, Guardian News and Media, 31 May 2019, https://www.theguardian.com/technology/2019/may/31/facial-recognition-school-new-york-privacy-fears.

England, Rachel. “Massive Biometric Security Flaw Exposed More than One Million Fingerprints.” *Engadget*, 14 Aug 2019, https://www.engadget.com/2019-08-14-biometric-security-flaw-fingerprints.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAAKGiYVK5OxdRB6YEkP1o4KqE9sS69dSiAUcOT9EZNJGgIz1BhLeXwZOi2MH_D03PiFW0jrf5V7ah0o2yb35FhXf84D7OMd5zvkHcUeVQ_Bpbz2gpoCsaRyF9dzPjFGRfCBqdD9yP3POXjgNpvw0EqaDIIJvpsw5HuqBoXFfwHskm

European Union Agency for Fundamental Rights. “Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement.” 18 June 2019, https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law.

Facial Recognition Market Size & Trends Report, 2021-2028, https://www.grandviewresearch.com/industry-analysis/facial-recognition-market.

Fung, Esther. “Shopping Centers Exploring Facial Recognition in Brave New World of Retail.” *The Wall Street Journal*, Dow Jones & Company, 2 July 2019, https://www.wsj.com/articles/shopping-centers-exploring-facial-recognition-in-brave-new-world-of-retail-11562068802.

Hill, Kashmir, and Krolik Aaron. “How Photos of Your Kids Are Powering Surveillance Technology.” *The New York Times*, The New York Times, 11 Oct. 2019, https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html.

Information Commissioner's Opinion Addresses Privacy Concerns on the Use of Live Facial Recognition Technology in Public Places. *ICO,* 18 June 2021, https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

Lund, Jesper. “Danish DPA Approves Automated Facial Recognition.” *European Digital Rights (EDRi)*, 21 Aug. 2020, https://edri.org/our-work/danish-dpa-approves-automated-facial-recognition/.

Maunder, Dan. “How Brands Are Saving Face: Five Ways Facial Recognition Is Improving Our Lives.” *ITProPortal*, ITProPortal, 10 May 2018, https://www.itproportal.com/features/how-brands-are-saving-face-five-ways-facial-recognition-is-improving-our-lives/.

McGhie, Steffen Nyboe. “Datatilsynet Giver Brøndby Grønt Lys Til Omstridt Overvågning: ‘Dette Er Den Første Tilladelse Af Sin Art.’” *Berlingske.dk*, 14 June 2019, https://www.berlingske.dk/samfund/datatilsynet-giver-broendby-groent-lys-til-omstridt-overvaagning-dette-er.

Office, U.S. Government Accountability. “Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses.” / *U.S. GAO*, https://www.gao.gov/assets/gao-20-522.pdf.

Propp, Kenneth and Mark MacCarthy. “Machines Learn That Brussels Writes the Rules: The EUs New AI Regulation.” *MIAI*, 29 Apr. 2021, https://ai-regulation.com/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/.

Sébastien Louradour, Independent AI Governance Consultant. “What to Know about the EU's Facial Recognition Regulation.” *World Economic Forum*, 23 April 2021, https://www.weforum.org/agenda/2021/04/facial-recognition-regulation-eu-european-union-ec-ai-artificial-intelligence-machine-learning-risk-management-compliance-technology-providers/

Song, Victoria. “In A 'Dangerous And Sinister Step,' London Police Start Using Live Face Recognition Tech.” *Gizmodo Australia*, 24 Jan. 2020, https://www.gizmodo.com.au/2020/01/in-a-dangerous-and-sinister-step-london-police-start-using-live-face-recognition-tech/.

Stolton, Samuel. “LEAK: Commission Considers Facial Recognition Ban in AI 'White Paper'.” *Www.euractiv.com*, EURACTIV, 17 Jan. 2020, https://www.euractiv.com/section/digital/news/leak-commission-considers-facial-recognition-ban-in-ai-white-paper/.

Thales Group. “Facial Recognition: Top 7 Trends (Tech, Vendors, Markets, Use Cases & Latest News).” Last updated: 24 June 2021.https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition.

“Tilladelse Til Behandling Af Biometriske Data Ved Brug Af Automatisk Ansigtsgenkendelse Ved Indgange På Brøndby Stadion.” *Datatilsynet*, https://www.datatilsynet.dk/afgoerelser/tilladelser/2019/maj/tilladelse-til-behandling-af-biometriske-data-ved-brug-af-automatisk-ansigtsgenkendelse-ved-indgange-paa-broendby-stadion. (Datatilsynet decision)

Vincent, James. “AI Experts Say Research into Algorithms That Claim to Predict Criminality Must End.” *The Verge*, The Verge, 24 June 2020, https://www.theverge.com/2020/6/24/21301465/ai-machine-learning-racist-crime-prediction-coalition-critical-technology-springer-study.

Wimbley, Randy. “Black Teen Kicked out of Skating Rink after Facial Recognition Camera Misidentified Her.” *FOX 2 Detroit*, FOX 2 Detroit, 16 July 2021, https://www.fox2detroit.com/news/teen-kicked-out-of-skating-rink-after-facial-recognition-camera-misidentified-her.