The regulatory gap between the law and the use of real-time Facial Recognition Technology by police in the European Union

University: Tilburg University
Master: Law & Technology
Department: LTMS
Author: Renata Delikat
Student number: 2048072
First supervisor: Dr Merel Noorman
Second supervisor: Lucas Jones
Date: February 2021

Table of Contents

Chapter 1: INTRODUCTION

1.1 Background

In the famous dystopian novel by George Orwell, *Nineteen Eighty-four*, the 'Big Brother' government had at its disposal a powerful tool allowing it to observe and listen to each citizen.[1] The terrifying device was called a 'telescreen', and was described as follows:

> *The telescreen received and transmitted simultaneously. Any sound Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live - did live, from habit that became instinct- in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.*[2]

It might seem far-fetched to compare this futuristic dystopian device with the technology our governments use currently. However, with the rapid development of surveillance technology, and facial recognition technology, the idea of being watched at all times, at least in the public places, does not seem so unrealistic.[3] It is already happening in China, where the government is using a system of advanced facial recognition technology in order to surveil and control its

[1] Mark Schreiber, 'Facial recognition technology: what would George Orwell say?' (02 February 2019, thejapantimes) <https://www.japantimes.co.jp/news/2019/02/02/national/media-national/facial-recognition-technology-george-orwell-say/#.XbVjT5NKg6U> accessed 28 October 2019.

[2] George Orwell, *Nineteen Eighty-four* (1949).

[3] Mark Schreiber, 'Facial recognition technology: what would George Orwell say?' (02 February 2019, the Japan Times) <https://www.japantimes.co.jp/news/2019/02/02/national/media-national/facial-recognition-technology-george-orwell-say/#.XbVjT5NKg6U> accessed 28 October 2019.

inhabitants, especially Uighur Muslim population in Xinjiang.[4] The technology is integrated into a vast network of surveillance cameras, and it is watching the members of the minority, keeping records of their everyday lives.[5] In the face of the coronavirus pandemic, the government is strengthening its public surveillance presence all around the country, and facial recognition technologies can now flag people not wearing face masks or recognise an elevated temperature.[6]

We do not need to look as far as China to find examples of such panopticon technologies. Indeed, video surveillance systems, referred to as closed-circuit television (CCTV), are widespread in Europe for many years now.[7] London constitutes a well-known, though hardly the only one, European example of a highly surveilled urban environment, as there are almost 630,000 CCTV cameras (which means that for every 14 people, there is 1 camera).[8] Additionally, reports of the employment of Facial Recognition Technologies ("FRT") by the law enforcement agencies are increasingly common. According to a research by Vice, a database used by the Dutch police for facial recognition technology includes approximately 1.3 million people.[9] In 2017, the German government experimented with real-time automated FRT in Berlin Südkreuz railway station on a group of volunteers.[10] The technology was also tested by the police in the UK, where the use of real-time FRT has been

[4] Paul Mozur, 'One Month, 500,000 Face Scans: How China is using AI to Profile a Minority' (14 April 2019, New York Times) <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> accessed 27 October 2019.

[5] Paul Mozur, 'One Month, 500,000 Face Scans: How China is using AI to Profile a Minority' (14 April 2019, New York Times) <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> accessed 27 October 2019.

[6] Lily Kuo, 'The new normal: China's excessive coronavirus public monitoring could be here to stay' (09 March 2020, theGuardian) <https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay> accessed 10 October 2020.

[7] William Webster, *Video Surveillance: Practices and policies in Europe* (Amsterdam: IOS Press, 2012).

[8] Jonatan Ratcliffe, 'How many CCTV cameras are there in London 2019?' (19 May 2019, CCTV.co.uk) <https://www.cctv.co.uk/how-many-cctv-cameras-are-there-in-london/> accessed 27 October 2019.

[9] 'Dutch police facial recognition database includes 1.3 million people' (22 July 2019, DutchNews.nl) <https://www.dutchnews.nl/news/2019/07/dutch-police-facial-recognition-database-includes-1-3-million-people/> accessed 28 October 2019.

[10] Janosch Delcker, 'Big Brother in Berlin' (13 September 2018, Politico) <https://www.politico.eu/article/berlin-big-brother-state-surveillance-facial-recognition-technology/> accessed 28 October 2019.

met with a substantial outrage. It was followed by reports of inaccuracy of the results of facial recognition scans, which was accompanied by accusations of racial and gender biases.[11]

Surveillance technology is developing at a rapid speed. Face recognition with AI, also capable of identifying people in the real time, might be widespread in our public places soon enough. It may dominate and change our daily lives and lead to the end of privacy outside of our homes.[12] This thesis will identify the gap between the application of real-time FRT used by police to identify individuals in public and the way this technology is regulated in law.

1.2 Problem Statement

The focus of this thesis is the regulation of real-time FRT deployed by police in order to identify individuals in the public places in the European Union. Public places or spaces in this thesis is understood as either indoor or outdoor area to which general public has access, either by right or by invitation.[13] Real-time FRT is relatively new and might bring various risks for the privacy and liberty of individuals. It uses cameras, which are scanning crowds and identifying people in real-time, and then matching the identified faces against a database.[14] It is a prevailing belief among privacy activists that such a use of facial recognition technology without subjects' consent constitutes a gross violation of privacy, and leads to the creation of surveillance states.[15] Big Brothers Watch, a non-profit British civil liberties and privacy campaigning organisation, warns that the employment of this technology means that each passer-by will be scanned and analysed, subjected to a covert biometric identity check, and turned into a 'walking

[11] Kenan Malik, 'As surveillance culture grows, can we even hope to escape its reach?' (19 May 2019, the Guardian) <https://www.theguardian.com/commentisfree/2019/may/19/as-surveillance-culture-grows-can-we-even-hope-to-escape-its-reach> accessed 28 October 2019.

[12] Tonja Bohm, 'Wir mussen Gesichtserkunnung mit KI regulieren - und zwar jetzt' (Microsoft Berlin, 20 February 2019) <https://www.microsoft.com/de-de/berlin/artikel/wir-mussen-gesichtserkennung-mit-ki-regulieren-und-zwar-jetzt.aspx> accessed 28 October 2019.

[13] USLegal, 'Public Place Law and Legal Definition' <https://definitions.uslegal.com/p/public-place/> accessed 28 April 2020.

[14] 'Live facial recognition: introduction' (Big Brother Watch, May 2019) <https://bigbrotherwatch.org.uk/all-campaigns/face-off-campaign/#Intro> accessed 01 October 2019.

[15] 'I.Resist Facial Recognition' (Liberty) <https://www.libertyhumanrights.org.uk/resist-facial-recognition> accessed 01 October 2019.

ID card'.[16] Privacy activists stress that such surveillance might have a 'chilling effect' on the freedom of expression, ultimately posing a threat to democratic freedoms.[17]

The UK constitutes an important example for research of the use of real-time FRT by the police. It is the only state following EU legislation which was conducting real-time FRT trials in the field, using real watchlists.[18] Moreover, in the recent first case on the matter, which attracted worldwide attention, the High Court in Wales ruled on the legality of those trials. Indeed, in September 2019 the Court decided that the use of real-time FRT technology by the South Wales Police is in accordance with British law.[19] However, the Court of Appeal has quashed this ruling in August 2020, deeming the deployment by police force unlawful. The Court based its decision mostly on the fact that the use was not 'in accordance with the law' for the purpose of Article 8(2) of the European Convention of Human Rights (ECHR), as there were fundamental deficiencies in the legal framework on the basis of which the trials were conducted.[20] However, it does not mean that any further use of FRT by police will be unlawful under this judgement – in case the deficiencies would be remedied, the use could be possible. As the Court has rejected as a ground of appeal the issue of proportionality, it seems like the way the technology was used by the South Wales Police would be accepted by the Courts.[21]

Since the case was decided on the basis of the implementation of ECHR and the EU's Directive 2016/680 on data protection in the context of law enforcement, it seems that - provided that there exists a legal basis in the national law - the current legal framework might allow for the employment of real-time FRT. As the potential risks of this technology are believed to be especially high, and its use by the law enforcement agencies might only increase from now on, it appears that there is a regulatory gap between the perception of the effects of

[16] 'Live facial recognition: introduction' (Big Brother Watch, May 2019) <https://bigbrotherwatch.org.uk/all-campaigns/face-off-campaign/#Intro> accessed 01 October 2019.

[17] 'I.Resist Facial Recognition' (Liberty) <https://www.libertyhumanrights.org.uk/resist-facial-recognition> accessed 01 October 2019.

[18] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[19] Jane Croft and Madhumita Murgia, 'UK court backs Welsh police use of facial recognition technology' (Financial Times, 04 September 2019) <https://www.ft.com/content/92d7d5f0-cefb-11e9-99a4-b5ded7a7fe3f> accessed 28 October 2019.

[20] *R (Bridges) v CC South Wales & ors* [2020] EWCA Civ 1058.

[21] *R (Bridges) v CC South Wales & ors* [2020] EWCA Civ 1058.

FRT, including real-time FRT, and the way it is treated in the current legal framework. As the AI technologies are developing rapidly in today's societies, the EU Commission claims to be taking steps to address this gap.[22] Moreover, EDPS head, Wojciech Wiewiórowski, claimed that he will be trying to convince the Commission that all automated recognition technologies in public places should be banned, at least until the technologies are "mature enough".[23]

The European Union is known for its high standards of data protection, and it is said to be already exploring ways to impose a stricter regulation on the use of FRT. Indeed, in its White Paper on AI from February 2020, the European Commission addressed the issue of facial recognition and announced that it will launch an European debate on the specific circumstances justifying use of FRT in public places and on the common safeguards.[24] Moreover, Ursula von der Leyen has declared in her political guidelines that she will seek a legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence.[25] In the light of those developments it is important to examine the risks stemming from the employment of FRT in public places by the police, and assess to what extent the current state-of-law is addressing those risks. The focus of this thesis will lie on real-time application of FRT.

1.3 Research question, existing literature and methodology

The use of FRT, especially real-time application, is a relatively new development in the police sector, thus the available academic literature is scarce.[26] However, in the light of the recent trials in the European Union, several reports discussing the risks of real-time FRT and the legality of such trials were published. Most notable and referred to frequently in this thesis are

---

[22] Mehreen Khan, 'EU plans sweeping regulation of facial recognition' (Financial Times, 22 August 2019) <https://www.ft.com/content/90ce2dce-c413-11e9-a8e9-296ca66511c9> accessed 28 October 2019.

[23] Samuel Stolton, 'EU data watchdog to 'convince' Commission to ban automated recognition tech' (EURACTIV.com, 1 July 2020) <https://www.euractiv.com/section/digital/news/eu-data-watchdog-argues-for-moratorium-on-recognition-technology/> accessed 10 October 2020.

[24] European Commission, 'White Paper: on Artificial Intelligence – A European approach to excellence and trust' (Brussels, 19 February 2020).

[25] Ursula von der Leyen, 'A union that strives for more: My agenda for Europe' (Political Guidelines for the next European Commission 2019-2024) <https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf> accessed 28 October 2019.

[26] Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40 UNSWLJ 121.

Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology by Professor Pete Fussey and Dr Daragh Murray from The Human Rights, Big Data and Technology Project, and European Union Agency's for Fundamental Rights *Facial recognition technology: fundamental rights considerations in the context of law enforcement.* The former focuses on a particular, however prominent, employment by Metropolitan Police and its governance and human rights compliance in the British system.[27] The latter explores the fundamental rights implications of using real-time FRT under legal system of the EU generally.[28] However, there are hardly any sources identifying the potential regulatory gap between the state-of-law in the EU and the risks connected with the deployment of real-time FRT. Therefore, it is important to examine this issue.

The main research question of the thesis is:

To what extent is there a regulatory gap between the current state-of law and the risks of the employment of real-time Facial Recognition Technology (FRT) used by the police to identify individuals in the public places in the EU?

Sub-questions:

1) What is FRT, how does it work, how is it employed in the real-time by the police forces in public places?
2) What are the potential risks to fundamental rights of individuals stemming from the employment of real-time FRT by police in public places?
3) What is the current legal framework at European level that can be applied to real-time FRT used in the public places in the context of police work?
4) What risks to fundamental rights of individuals of the employment of real-time FRT are not (fully) addressed by the current state-of law regulating FRT in the EU?

[27] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[28] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

Thus, the underlying aim of the research is to identify the extent to which the current legal framework is insufficiently equipped to deal with the risks posed by real-time FRT. To achieve this goal, this thesis will focus mainly on doctrinal legal research, taking a critical viewpoint of the risks connected with the employment of FRT in law enforcement context, and addressing the issue through the lens of human rights and human dignity. The main research activity will be based on black-letter analysis of legal documents, and on desk-research of secondary sources. It will consist of the examination of:

- European Convention of Human Rights,
- the EU Charter of Fundamental Rights,
- the EU Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Law Enforcement Directive),
- an analysis of available guidelines, recommendations, case law and academic articles regarding the legal framework.

Moreover, the examination of reports, journalistic and academic articles, books, and blog posts were conducted in order to understand the technology and its potential risks.

1.4 Structure

The second chapter will provide the background knowledge necessary in order to understand the implications of FRT, also its real-time application. It will explain the concept at hand, provide an insight into the functioning of the technology, and discuss the characteristics of biometric data. Moreover, it will explain how law enforcement agencies are employing this technology in public places in their fight against crime in the Member States of the EU and in the UK. Lastly, it will analyse the risks of real-time FRT to the rights of individuals. The third chapter will focus on the current legal regime governing FRT at the European Union level. The fourth chapter will apply the law to the technology at hand, and explore the existing regulatory gap between earlier analysed employment of FRT and its risks, and the current European legal framework governing its employment. Finally, the fifth chapter will be the conclusion, in which the findings will be summarised, and the research question will be answered.

Chapter 2: FACIAL RECOGNITION TECHNOLOGY: THE STATE OF THE ART & ITS POTENTIAL RISKS TO THE FUNDAMENTAL RIGHTS

This chapter will focus on in depth analysis of FRT itself, answering the first and the second sub-questions of this thesis: "what is FRT, how does it work, how is it employed in the real-time by the police forces in public places?", and "what are the risks to fundamental rights of individuals stemming from the employment of real-time FRT by police in public places?". Firstly, it will introduce the concepts of biometric identification and FRT. Furthermore, it will explain how this technology works and how it can be used by the police. Lastly, the analysis of the potential risks of the employment of this technology to fundamental rights of individuals will follow.

2.1 Introduction to Facial Recognition technologies

The verification and identification of individuals using biological information, their unique characteristics, is possible thanks to biometrics.[29] Biometrics is based on "any measurable, robust, distinctive, physical characteristics of an individual that can be used to identify, or verify the claimed identity of that individual".[30] Facial recognition is a part of biometrics technologies, together with, for instance, iris scans and fingerprints.[31] Digital images containing an individual's face are considered personal data and biometric data if an individual can be identified. Moreover, biometric data is considered sensitive personal data.[32]

The importance of facial recognition in the criminal justice systems was already recognised in the first half of the 19th century, when police started storing photographs of

[29] Kanya A Bennett, 'Can Facial Recognition Technology Be Used to Fight the New Way against Terrorism: Examining the Constitutionality of Facial Recognition Surveillance Systems' (2001) 3 NC JL & Tech 151.

[30] John D. Woodward, Katharine W. Webb and others, 'A Primer in Biometric Technology'z in: *Army Biometric Application: Identifying and Addressing Sociocultural Concerns* (RAND Corporation 2001).

[31] Kanya A Bennett, 'Can Facial Recognition Technology Be Used to Fight the New Way against Terrorism: Examining the Constitutionality of Facial Recognition Surveillance Systems' (2001) 3 NC JL & Tech 151.

[32] Article 29 Data Protection Working Party, 'Opinion 2/2012 on facial recognition in online and mobile devices' (22 March 2012).

criminals for their later identification. The automated facial recognition operated by a computer programme became plausible only in the early 1990s thanks to the research of Matthew Turk and Alex Pentland.[33] Since that time, the technology developed significantly and is steadily becoming more sophisticated.[34] The state of the art today achieved almost human level performance, since the first occurrence of deep learning systems in 2014. The deep learning systems driving those innovations are DeepFace, theDeepID, VGGFace, and FaceNet.[35] Moreover, thanks to the advances in image capture devices, such as surveillance cameras, and the amounts of face images online, face recognition has become more significant in the recent years.[36] Nowadays, FRT is used for numerous purposes, most notably in areas of security, social media, commerce and for personal use.[37]

Article 29 Data Protection Working Party defined facial recognition in its Opinion 02/2012 on facial recognition in online and mobile services, as "the automatic processing of digital images which contain the faces of individuals for the purpose of identification, authentication/verification or categorisation of those individuals".[38] In general, FRT operates through complex algorithms which identify faces in images and allow for comparison of different facial images. Taking as an example an algorithm used by South Wales Police during its real-time FRT trials, it was functioning as follows: detecting images of faces, analysing and

[33] Andy Adler and Michael E Schuckers, 'Comparing Human and Automatic Face Recognition Performance' (2007) 37(5) IEEE Transactions on Systems, Man, and Cybernetics 1248.

[34] Andy Adler and Michael E Schuckers, 'Comparing Human and Automatic Face Recognition Performance' (2007) 37(5) IEEE Transactions on Systems, Man, and Cybernetics 1248.

[35] Mei Wang and Weihong Deng, 'Deep Face Recognition: A Survey' (arXiv, 18 April 2018) <https://arxiv.org/pdf/1804.06655.pdf> accessed 01 November 2020, p. 1; Jason Brownlee, 'A gentle introduction to Deep Learning for Face Recognition' (Machine Learning Mastery, 31 May 2019) <https://machinelearningmastery.com/introduction-to-deep-learning-for-face-recognition/> accessed 01 November 2020.

[36] Stan Z Li and Anil K Jain, *Handbook of Face Recognition* (Springer 2011), p. 1.

[37] Sharon Nakar and Dov Greenbaum, 'Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy' (2017) 23 BU J Sci & Tech L 88.

[38] Article 29 Data Protection Working Party, 'Opinion 2/2012 on facial recognition in online and mobile devices' (22 March 2012).

measuring distances between facial features, generating a mathematical representation – a 'biometric template', and then comparing it against a database.[39]

Additionally, it is worth noting that FRT can work either as face verification systems or as face identification systems. Face verification is used for example in the airports for self-serviced immigration, and it entails comparing a query face image against an enrolment face image (or a template).[40] On the other hand, face identification warrants "one-to-many matching"[41], where a query face is compared against many facial images (or templates) in the enrolment database.[42] This thesis will be centred around the latter applications of FRT in the surveillance context by police in the public spaces. In order to answer the research question, it is first necessary to understand the way the technology itself works.

2.2 The components of Facial Recognition technology – the way it works step-by step

This sub-chapter will focus on the analysis of FRT, aiming at explaining the way it operates, and any possible errors that might occur.

2.2.1 The process of Facial Recognition

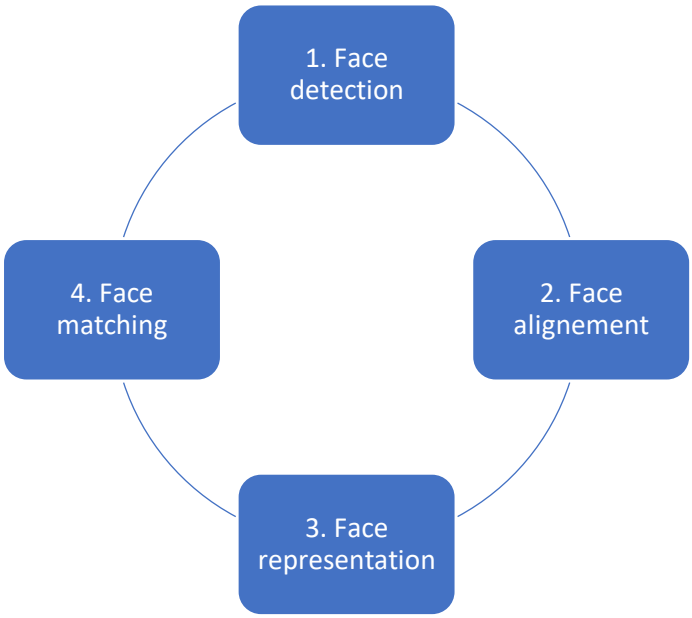
[39] Bethan Davies, Martin Innes and Andrew Dawson, 'An evaluation of South Wales Police's use of automated facial recognition' (Universities' Police Science Institute Crime & Security Research Institute, September 2018), p. 12.

[40] Stan Z Li and Anil K Jain, *Handbook of Face Recognition* (Springer 2011), p. 2.

[41] Stan Z Li and Anil K Jain, *Handbook of Face Recognition* (Springer 2011), p. 3.

[42] Stan Z Li and Anil K Jain, *Handbook of Face Recognition* (Springer 2011), p. 3.

Fig. 1 Face recognition building blocks



[43]

According to the literature, facial recognition consists of inter-related different stages, some of them might take part simultaneously.[44] The building blocks of the technology are usually: face detection, face alignment, face representation, and face matching.[45]

An acquisition of an image, and the subsequent detection of faces are the first essential steps in facial recognition.[46] An image of a face can be acquired for example by a surveillance camera.[47] Such an acquired image is scanned, and the face detector returns the coordinates of a bounding box for faces in the acquired images.[48] After a face has been detected, the next phase is the face alignment[49], in which a face image is adjusted to the canonical coordinates.[50]

---

[43] Daniel Saez Trigueros and Li Meng, 'Face Recognition: From Traditional to Deep Learning Methods' (arXiv, 31 October 2018) <https://arxiv.org/abs/1811.00116> accessed 12 November 2020.

[44] Wen-Yi Zhao, Rama Chellappa and others, 'Face Recognition: A Literature Survey' (2003) 35(4) ACM Computing Surveys 399.

[45] Daniel Saez Trigueros and Li Meng, 'Face Recognition: From Traditional to Deep Learning Methods' (arXiv, 31 October 2018) <https://arxiv.org/abs/1811.00116> accessed 12 November 2020.

[46] Wen-Yi Zhao, Rama Chellappa and others, 'Face Recognition: A Literature Survey' (2003) 35(4) ACM Computing Surveys 399.

[47] Sharon Nakar and Dov Greenbaum, 'Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy' (2017) 23 BU J Sci & Tech L 88.

[48] Daniel Saez Trigueros and Li Meng, 'Face Recognition: From Traditional to Deep Learning Methods' (arXiv, 31 October 2018) <https://arxiv.org/abs/1811.00116> accessed 12 November 2020.

[49] Daniel Saez Trigueros and Li Meng, 'Face Recognition: From Traditional to Deep Learning Methods' (arXiv, 31 October 2018) <https://arxiv.org/abs/1811.00116> accessed 12 November 2020.

[50] Mei Wang and Weihong Deng, 'Deep Face Recognition: A Survey' (arXiv, 18 April 2018) <https://arxiv.org/pdf/1804.06655.pdf> accessed 01 November 2020, p. 2.

After, the next stage is the "face representation".[51] In this step the pixel values of an image are transformed into a template, which is a discriminative and compact feature vector.[52] This stage is crucial for facial recognition[53], and since the development of deep learning it has improved significantly. Deep learning stiches together pixels into a face representation by using multiple layers to "learn representations of data with multiple level of feature extraction"[54], while traditional methods used only one- or two-layer representations.[55]

The last step of the facial recognition process is "face matching".[56] In this phase the templates are compared with those stored, for instance in the database, and the similarity between them is measured for the purpose of identification (or verification).[57] The system calculates a match score measuring similarity between them, and the higher the match score the more likely it is that an individual was recognised. Normally, an application-specific threshold is chosen, and scores above this threshold indicate a match, and below – a non-match.[58] However, errors are possible to occur as a result of the recognition process: either a false positive (the images are matched even though the faces belong to different people), or a false negative (the images are not matched even though the faces belong to one person).[59]

---

[51] Daniel Saez Trigueros and Li Meng, 'Face Recognition: From Traditional to Deep Learning Methods' (arXiv, 31 October 2018) <https://arxiv.org/abs/1811.00116> accessed 12 November 2020.

[52] Daniel Saez Trigueros and Li Meng, 'Face Recognition: From Traditional to Deep Learning Methods' (arXiv, 31 October 2018) <https://arxiv.org/abs/1811.00116> accessed 12 November 2020.

[53] Daniel Saez Trigueros and Li Meng, 'Face Recognition: From Traditional to Deep Learning Methods' (arXiv, 31 October 2018) <https://arxiv.org/abs/1811.00116> accessed 12 November 2020.

[54] Mei Wang and Weihong Deng, 'Deep Face Recognition: A Survey' (arXiv, 18 April 2018) <https://arxiv.org/pdf/1804.06655.pdf> accessed 01 November 2020, p. 2.

[55] Mei Wang and Weihong Deng, 'Deep Face Recognition: A Survey' (arXiv, 18 April 2018) <https://arxiv.org/pdf/1804.06655.pdf> accessed 01 November 2020, p. 2.

[56] Daniel Saez Trigueros and Li Meng, 'Face Recognition: From Traditional to Deep Learning Methods' (arXiv, 31 October 2018) <https://arxiv.org/abs/1811.00116> accessed 12 November 2020.

[57] Article 29 Data Protection Working Party, 'Opinion 2/2012 on facial recognition in online and mobile devices' (22 March 2012); Daniel Saez Trigueros and Li Meng, 'Face Recognition: From Traditional to Deep Learning Methods' (arXiv, 31 October 2018) <https://arxiv.org/abs/1811.00116> accessed 12 November 2020.

[58] Andy Adler and Michael E Schuckers, 'Comparing Human and Automatic Face Recognition Performance' (2007) 37(5) IEEE Transactions on Systems, Man, and Cybernetics 1248.

[59] Andy Adler and Michael E Schuckers, 'Comparing Human and Automatic Face Recognition Performance' (2007) 37(5) IEEE Transactions on Systems, Man, and Cybernetics 1248.

2.2.2 Factors affecting Face Recognition

The general performance of FRT, also when deep learning methods are used (albeit to a lesser extent), depends on a variety of factors. The illumination, facial pose, expression, age span, hair, facial wear, background, camera distance, size of an image and motion may influence the accuracy of matches.[60] Generally, the most important factor influencing the performance of FRT is the similarity of an acquired image with the images enrolled in a database.[61] Another factor influencing FRT performance is the choice of a development set. A development set is the set of images used for the training of algorithms. Through such a set, the algorithms can learn how to detect faces and extract their features. Thus, it is crucial that a development set reflects the conditions under which it will function (from the perspective of the characteristics of individuals and the technical conditions), as it has the power to influence the overall performance of the entire algorithm.[62]

The performance of FRT depends on a variety of factors, and the results are not always accurate. However, the technology is constantly developing and becoming more and more effective[63], with deep learning methods approaching human performance levels.[64] As already indicated earlier, the technology is being implemented in many sectors, including the area of security in the daily work of police.

2.3 The use of Facial Recognition technology by police

[60] Stan Z Li and Anil K Jain, *Handbook of Face Recognition* (Springer 2011), p. 1; Sharon Nakar and Dov Greenbaum, 'Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy' (2017) 23 BU J Sci & Tech L 88; Mei Wang and Weihong Deng, 'Deep Face Recognition: A Survey' (arXiv, 18 April 2018) <https://arxiv.org/pdf/1804.06655.pdf> accessed 01 November 2020, p. 1-3.

[61] Lucas Introna and Helen Nissenbaum, 'Facial Recognition Technology: A Survey of Policy and Implementation Issues' (the Center for Catastrophe Preparedness and Response, 2010) <https://eprints.lancs.ac.uk/id/eprint/49012/1/Document.pdf> accessed 17 January 2020.

[62] Lucas Introna and Helen Nissenbaum, 'Facial Recognition Technology: A Survey of Policy and Implementation Issues' (the Center for Catastrophe Preparedness and Response, 2010) <https://eprints.lancs.ac.uk/id/eprint/49012/1/Document.pdf> accessed 17 January 2020.

[63] Sharon Nakar and Dov Greenbaum, 'Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy' (2017) 23 BU J Sci & Tech L 88.

[64] Mei Wang and Weihong Deng, 'Deep Face Recognition: A Survey' (arXiv, 18 April 2018) <https://arxiv.org/pdf/1804.06655.pdf> accessed 01 November 2020.

FRT is used more and more often by police around the world.[65] The most extreme case of the use of surveillance camera systems with FRT, including real-time recognition, is reportedly in China. Journalists report, among others, that thanks to a surveillance camera system in a city of Guiyang, police is able to locate and identify anyone in a matter of minutes, and also trace the past whereabouts of an individual.[66] However, the precise information about such practices is often difficult to find, due to the lack of transparency, as police departments tend to keep them secret.[67] There is also no official comprehensive overview of the use of FRT in the EU.[68] AlgorithmWatch, a NGO researching algorithmic decision-making processes, published a report in December 2019 which has revealed that the police forces of at least eleven Member States of the EU are using facial recognition; eight plan to introduce it in the coming years; and just two countries (Spain and Belgium) do not allow it.[69]

This sub-chapter will focus on the way real-time FRT was used so far by the police in order to conduct surveillance of individuals in public spaces. The trails of the technology by the UK and some of the European Union's Member States will be discussed.

---

[65] Philip Brey, 'Ethical Aspects of Facial Recognition Systems in Public Places' (2004) 2 Info, Comm & Ethics in Society 97.

[66] Prod. Joyce Liu, 'In Your Face: China's all-seeing state', (BBC News, 10 December 2017), <https://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state> accessed 24 January 2020; Clare Garvie, Alvaro Bedoya and Jonathan Frankle, 'The perpetual line-up' (Georgetown law Center on Privacy & Technology, 18 October 2016) <www.perpetuallineup.org> accessed 26 January 2020.

[67] Angel Diaz, 'New York City Department Surveillance Technology' (Brennan Center for Justice, 4 October 2019) <https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology> accessed 21 January 2020; Nicolas Kayser-Bril, 'At least 11 police forces use face recognition in the EU, AlgorithmWatch reveals' (AlgorithmWatch, 11 December 2019) <https://algorithmwatch.org/en/story/face-recognition-police-europe/> accessed 20 October 2020.

[68] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[69] Nicolas Kayser-Bril, 'At least 10 police forces use face recognition in the EU, AlgorithmWatch reveals' (AlgorithmWatch, 11 December 2019) <https://algorithmwatch.org/en/story/face-recognition-police-europe/> accessed 21 January 2020.

2.3.1 The United Kingdom

Police forces of South Wales, Leicestershire and London's Metropolitan Police were conducting trials of real-time facial recognition in public between 2016 and 2019. Taking as an example London's Metropolitan Police Service, it conducted ten of such trials, using fixed position cameras, either installed in a similar fashion as CCTV cameras (for example in Stratford), or on mobile facial recognition vans. Images obtained through those cameras were streamed in real time to a facial recognition system, which processed the images to detect faces, extract features and analyse them against a 'watchlist', a database of images of wanted persons. In case of a match, an alarm was generated in the control room where the software was controlled by police officers. The software presented them a live image and the image matched from the watchlist, which they could compare and decide whether to stop an individual for a control.[70] According to the available documentation, in case no match was generated, digital signatures were discarded immediately after processing. If a match was generated, it was retained for a 30-day period. Additionally, no database of individuals or their movements was established as a result of the trials.[71] Similar mode of operation was also followed by the South Wales Police, and a simplified visual representation of its forces' operations when employing AFR Locate was included in an evaluation of their use of AFR conducted by Cardiff University[72]:

[70] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[71] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[72] Bethan Davies, Martin Innes and Andrew Dawson, 'An evaluation of South Wales Police's use of automated facial recognition' (Universities' Police Science Institute Crime & Security Research Institute, September 2018), p. 13.

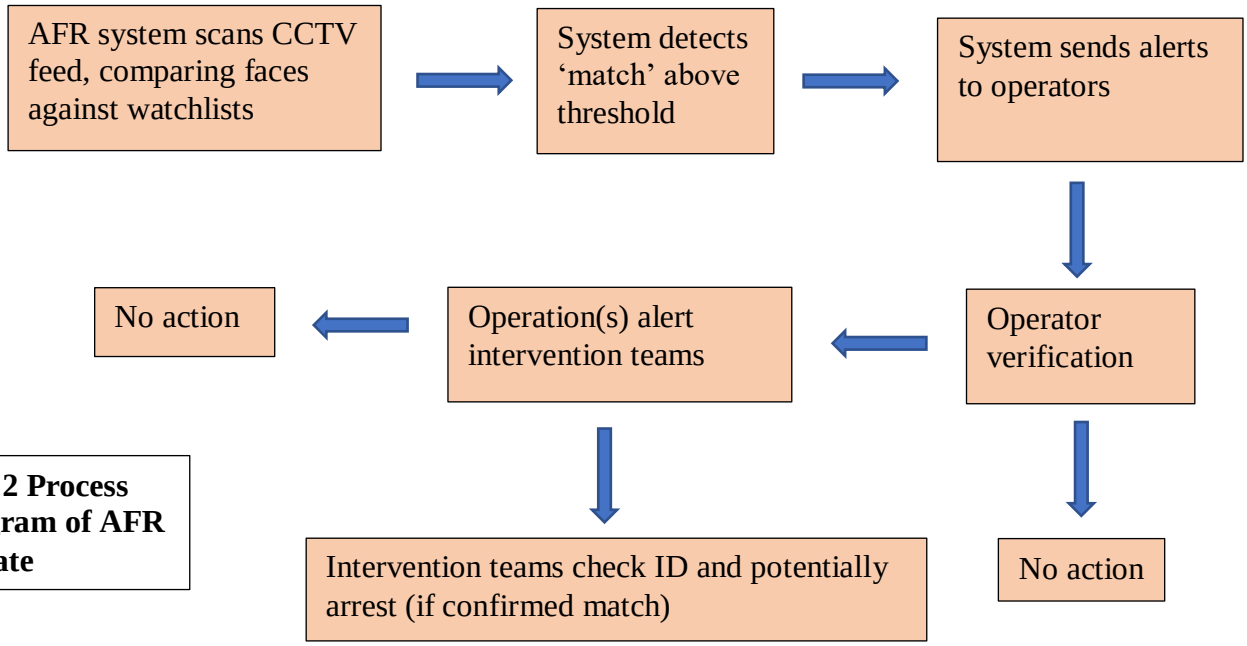


Fig. 2 Process diagram of AFR Locate

[73]

2.3.2 Member States of the European Union

As indicated earlier, the UK is not the only European country testing and having the capacity to use real-time FRT.

In Germany, real-time FRT was tested on a group of 300 volunteers at Berlin's Südkreuz station in 2017 and 2018. The tests included three different cameras and three computer programs.[74] The police issued a statement that a legal basis needs to be enacted in order to commence the legal employment of the real-time FRT in public.[75] Furthermore, in the beginning of 2020 it was reported that Germany's Interior Affairs Minister was planning to use

[73] Bethan Davies, Martin Innes and Andrew Dawson, 'An evaluation of South Wales Police's use of automated facial recognition' (Universities' Police Science Institute Crime & Security Research Institute, September 2018), p. 13.

[74] 'Polizei setzt immer mehr automatische Gesichtserkennung ein, Datenschützer besorgt' (21 March 2018, Heise online) <https://www.heise.de/newsticker/meldung/Polizei-setzt-immer-mehr-automatische-Gesichtserkennung-ein-Datenschuetzer-besorgt-4000106.html> accessed 25 January 2020.

[75] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020, p. 12.

automatic facial recognition at 134 railway stations and 14 airports, however the ministry has not officially confirmed such measures yet.[76]

The police in France conducted a trial of real-time FRT during the carnival in Nice in 2018. The technology was tested on a group of volunteers, whose images were enrolled in a watchlist composed for this purpose.[77] However, the police in France has not been using real-time application of FRT in public, as there is no legal basis in French law.[78]

Regarding other Member States, there is limited information available concerning the possible use or tests of this technology. However, it is clear that at least some of them are interested in using it in the future. This possibility has raised a number of concerns regarding the impact of the technology on fundamental rights of individuals.[79]

2.4 The risks of the employment of FRT to the fundamental rights of individuals

The employment of FRT by the police in public places raises various ethical and practical concerns.[80] This sub-chapter will identify the risks to individuals and their rights of real-time FRT used in public spaces by the police. The potential risks to human rights such as the rights to: privacy, non-discrimination, and freedoms of expression, assembly and association will be analysed. Lastly, the risks of inaccuracy will be explored.

---

[76] Philipp Grull, 'Germany's plans for automatic facial recognition meet fierce criticism' (10 January 2020, Euractiv) <https://www.euractiv.com/section/data-protection/news/german-ministers-plan-to-expand-automatic-facial-recognition-meets-fierce-criticism/> accessed 01 February 2020.

[77] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[78] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[79] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[80] Sharon Nakar and Dov Greenbaum, 'Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy' (2017) 23 BU J Sci & Tech L 88.

2.4.1 Risks to the privacy of individuals

Privacy should be understood as the protection from "a range of kinds of social friction"[81], and as a tool enabling individuals "to engage in worthwhile activities in ways that they would otherwise find difficult or impossible".[82] Even in public places people tend to expect to preserve privacy in their identities. While being in public allows others to see our faces, it does not allow them to identify us and know our background.[83] Anonymity becomes a tool for privacy in public.[84] Indeed, it constitutes an important aspect for individuals, as it assures them that they remain 'nameless', are a part of an undifferentiated crowd, and have the freedom of action.[85] It shields individuals from a potential bias based on their identities and from the danger of reprisal when exercising democratic freedoms.[86]

However, surveillance cameras embedded with facial recognition make an identification of individuals possible, stripping them of the anonymity.[87] Generally, the continuous monitoring was proven to have problematic effects on individuals. First of all, it is making people uncomfortable, leading them to change their behaviour, and to self-censorship. It is an effective tool of social control, pressuring individuals to adhere to social norms. Such control adversely impacts freedom, creativity, autonomy, and self-development.[88] It is said that it results in "a subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines".[89] The issue can be visualised through the prism of the Panopticon, a concept coined by Bentham, and later analysed by Foucault. When daily life is

[81] Daniel Solove, 'A taxonomy of privacy' (2006) 154(3) University of Pennsylvania Law 477.

[82] Daniel Solove, 'A taxonomy of privacy' (2006) 154(3) University of Pennsylvania Law 477.

[83] Mariko Hirose, 'Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology ' (2017) 49 Conn L Rev 1591.

[84] Sharon Nakar and Dov Greenbaum, 'Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy' (2017) 23 BU J Sci & Tech L 88.

[85] Christopher Slobogin, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity' (2002) 72 Miss LJ 213.

[86] The International Justice and Public Safety Network, 'Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field' (30 June 2011) <https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf> accessed 28 April 2020.

[87] Sharon Nakar and Dov Greenbaum, 'Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy' (2017) 23 BU J Sci & Tech L 88.

[88] Daniel Solove, 'A taxonomy of privacy' (2006) 154(3) University of Pennsylvania Law 477.

[89] Julie E Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stan L Rev 1373.

invaded by Panopticon mechanisms, everybody can potentially be under surveillance. It causes people to internalise control, and results in a disciplinary society. Foucault identified a phenomenon connected with the disciplinary society called 'normation', which is a process of creating norms of behaviour. In this process individuals are supposed to conform to a norm, thus creating a universal subject, and any abnormality is deemed deficient and inferior, which in turn leads to de-individualisation.[90]

Additionally, surveillance is much more than targeting specific information. It is about gathering and combining together data about an individual (aggregation). Those pieces of information together can create a comprehensive image about an individual. Moreover, if analysed, the aggregated data might reveal new facts, previously unknown, which would not be concluded from isolated data.[91] Such aggregation unsettles expectations – people do not expect others will know more about them than what they give out. Moreover, it can "increase the power that others have over individuals"[92], and it leads to distortions if used in decision-making as "the data is often reductive and disconnected from the original context in which it was gathered".[93]

All of those negative consequences of monitoring and surveillance are likely to be more pronounced if FRT will be used to surveil public spaces, as people would be aware that they are not anonymous when they are outside. Moreover, individuals' movements within the city could be recorded, aggregated and stored, and perhaps subjected to a further automated analysis, identifying for example unusual pattern of movement, participation at certain events, etc.. Thus, such technology could allow a great intrusion into the privacy of individuals, and far-reaching conclusions regarding their private lives.[94]

2.4.2 Risks to the right to non-discrimination

[90] Masa Galic and others, 'Betham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation' (2017) 30(1) Philosophy and Technology 9.

[91] Daniel Solove, 'A taxonomy of privacy' (2006) 154(3) University of Pennsylvania Law 477.

[92] Daniel Solove, 'A taxonomy of privacy' (2006) 154(3) University of Pennsylvania Law 477.

[93] Daniel Solove, 'A taxonomy of privacy' (2006) 154(3) University of Pennsylvania Law 477.

[94] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

FRT is often accused of being discriminatory and biased towards women and people of colour.[95] Firstly, there were concerns that FRT can be used in a discriminatory way, analogous to traditional concerns regarding policing practices. It might depend on factors such as watchlist composition or the nature of the deployment. [96] The organisation Liberty has brought up the fact that in the UK the technology so far affected mostly people of colour – for instance it was used during the Notting Hill Carnival, large street carnival in London led by the Caribbean community.[97] Moreover, it was employed twice in the London Borough of Newham, which constitutes one of the UK's most ethnically diverse areas.[98] Indeed, a research conducted in the US across 100 police departments concluded that dark-skinned individuals are more likely to be subjected to facial recognition scans than any other ethnicity.[99]

Furthermore, many are concerned that biases are built into FRT.[100] Generally, the discrimination in data-supported algorithmic decision making can be caused by various reasons, and take place during the design, testing, and implementation stages.[101] The evaluations of FRT indicate that the performance between different algorithms varies

[95] 'I.Resist Facial Recognition' (Liberty) <https://www.libertyhumanrights.org.uk/resist-facial-recognition> accessed 01 October 2019.

[96] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[97] 'Notting Hill Carnival Guide' (Time Out, 21 August 2019) <https://www.timeout.com/london/things-to-do/notting-hill-carnival-guide> accessed 25 January 2020; 'I.Resist Facial Recognition' (Liberty) <https://www.libertyhumanrights.org.uk/resist-facial-recognition> accessed 01 October 2019.

[98] 'I.Resist Facial Recognition' (Liberty) <https://www.libertyhumanrights.org.uk/resist-facial-recognition> accessed 01 October 2019.

[99] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 1.

[100] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[101] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

considerably and it is necessary that each is evaluated on an application-by-application basis.[102] As result of performance biases, some systems systematically score higher recognition rates for certain groups over others, especially: "Asians, African-Americans, and other racial minorities over whites".[103] Indeed, a study from 2019 revealed that skin reflectance had the biggest impact on the accuracy of FRT, and it was less accurate for individuals with darker skin.[104] It may result in disproportionate scrutiny over historically marginalized groups.[105]

The biases can creep into the model as a result of an algorithm itself, or/and through the input data used to develop an algorithm.[106] The algorithms could be to some extent enhanced if they were fed with many images, which reflect different groups of people. As the algorithms tend to be mostly developed with data over-representing white men, they have higher recognition rates for white men.[107] Nonetheless, it was revealed that even when the training data was more inclusive, the models still, albeit to a lesser extent, "performed better

---

[102] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[103] Lucas Introna and Helen Nissenbaum, 'Facial Recognition Technology: A Survey of Policy and Implementation Issues' (the Center for Catastrophe Preparedness and Response, 2010) <https://eprints.lancs.ac.uk/id/eprint/49012/1/Document.pdf> accessed 17 January 2020, p. 45.

[104] Joy Buolamwini, 'United States House Committee on Oversight and Government Reform: hearing on Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties' (22 May 2019) < https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-BuolamwiniJ-20190522.pdf> accessed 25 November 2020; Cynthia Cook and others, 'Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems' (2019) 1 IEEE Transactions on Biometrics, Behavior and Identity Science 1.

[105] Lucas Introna and Helen Nissenbaum, 'Facial Recognition Technology: A Survey of Policy and Implementation Issues' (the Center for Catastrophe Preparedness and Response, 2010) <https://eprints.lancs.ac.uk/id/eprint/49012/1/Document.pdf> accessed 17 January 2020, p. 45.

[106] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[107] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

on lighter-skinned than darker-skinned faces, performed better on male-identified faces than female-identified faces, and performed worst on women of color".[108]

Furthermore, the skin colour itself can influence the outcome of biometric matching in facial recognition systems – "reflection of light affects the quality of facial images of very fair-skinned persons, and not enough light affects the quality for very dark-skinned persons".[109] This may result in more false positives among people of colour.[110] Since there is a risk that racial minorities will be subjected to disproportionate scrutiny, the employment of FRT may be as problematic as racial profiling.[111] Generally, biases can result in 'self-fulfilling prophecy', meaning that if a certain group is being stopped more often (for the reason of prejudice), the evidence of criminality is found among such a group more often as well. This in turn reinforces existing biases and perpetrates the idea that stopping people from such a group is an effective way of policing.[112] If people of certain minority are disproportionally targeted, this in turn translates into negative group effects, the deterioration of their relationship with the police – distrust and even hostility.[113]

2.4.3 Risks to freedom of expression, assembly and association

[108] Joy Buolamwini, 'United States House Committee on Oversight and Government Reform: hearing on Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties' (22 May 2019) <https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-BuolamwiniJ-20190522.pdf> accessed 25 November 2020.

[109] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[110] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[111] Lucas Introna and Helen Nissenbaum, 'Facial Recognition Technology: A Survey of Policy and Implementation Issues' (the Center for Catastrophe Preparedness and Response, 2010) <https://eprints.lancs.ac.uk/id/eprint/49012/1/Document.pdf> accessed 17 January 2020.

[112] European Union Agency for Fundamental Rights, *Preventing unlawful profiling today and in the future: a guide* (FRA, 2018).

[113] European Union Agency for Fundamental Rights, *Preventing unlawful profiling today and in the future: a guide* (FRA, 2018).

Using FRT in public places may negatively impact the freedom of expression and freedom of assembly and association. It might lead to a chilling effect, as individuals aware of being observed can refrain from exercising certain democratic rights, fearing the consequences. Even if monitored only in public, a variety of conclusions can be taken about the views and lifestyles of individuals. It could be concluded what kind of people they meet, and to what organizations they belong, also what kind of meetings or events they are attending.[114] In 2018 in the UK, the police used real-time FRT to scan faces of people taking part to a peaceful protest against arms trade, a practice challenged by the activist Edward Bridges.[115] Bridges stated that a van used by police for identification was park opposite the crowd, and "I felt it was there to sort of intimidate people and dissuade them from using their peaceful right to protest".[116] Thus, people attending this protest felt as if they were not anonymous. Anonymity is generally seen as an important part of counterbalancing a chilling effect.[117] Indeed, the police surveillance at political meetings is perceived by participants as: "i) physically and psychologically intrusive, ii) restricting social and political interaction and iii) reducing autonomy. It was also reported to be disruptive of collective political freedoms by reducing internal and external perceptions of legitimacy and safety, creating divisions and deterring participation".[118] Thus, using a technology capable of identifying individuals during peaceful assemblies constitute a factor discouraging from protesting, creating a chilling effect. Even in case of riots, the technology

[114] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[115] *R (Bridges) v CCSWP and SSHD* [2019] EWHC 2341 (Admin).

[116] 'UK privacy activist to appeal after facial recognition case fails' (Aljazeera, 05 September 2019) <https://www.aljazeera.com/news/2019/09/uk-privacy-activist-appeal-facial-recognition-case-fails-190905142953617.html> accessed 01 October 2019.

[117] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[118] Valerie Aston, 'State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives' (2017) 8(1) European Journal of Law and Technology.

may still negatively affect those protesting peacefully next to the more aggressive participants.[119]

2.4.4 Risks of inaccuracy

The inaccuracies of any FRT, also its real-time applications, can lead to situations where innocent persons are misidentified and subjected to undue police scrutiny.[120] The story of a man from Denver from 2014 portrays an example of the consequences of a false positive. Steve Talley was brutally arrested by police in relation to armed bank robberies that he did not commit, based on an FRT match, and was held for two months in a maximum-security pod. A year after his release, he was falsely matched and arrested again. Due to those arrests he had sustained many long-lasting psychological and physical injuries. This story proves that errors made by FRT can have serious consequences for individuals.[121] Thus, the performance of the technology should be carefully considered when deliberating on its possible application in public.

There is a dispute over the way the accuracy of real-time FRT should be determined.[122] The widely cited claim of Big Brother Watch is that FRT is highly inaccurate, and during the trails conducted by the Metropolitan police over 98% matches were false positives.[123] This

[119] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[120] Joy Buolamwini, 'United States House Committee on Oversight and Government Reform: hearing on Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties' (22 May 2019)

[121] Ava Kofman, 'Losing face: how a Facial Recognition Mismatch Can Ruin Your Life' (The Intercept, 13 October 2016), <https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life/> accessed 01 November 2020.

[122] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[123] Big Brother Watch, 'Face off: the lawless growth of facial recognition in UK policing' (2018) 3; Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council)

high percentage was calculated on the basis of *the overall number of matches* generated by the technology against *true positives* (a correct match verified by the officers on the ground).[124] Others evaluating the technology disputed this number, and asserted that instead the technology should be evaluated comparing the *number of faces scanned* against the number of *false positives*.[125] As the technology scans many thousands of faces per hour (precise number is unknow), the number of generated matches, and also the number of false positives, is comparably indeed very small.[126] The US Department of Commerce's National Institute of Standards and Technology (NIST) has conducted in 2018 the largest accuracy test of FRT, with the result of 0,2% of error rates.[127] The results from trials in Germany, where three FRT systems were used on a group of volunteers, also show high accuracy rates. When each was used alone, the average false positive rate was 0,34%. When all of the three systems were used together, the false positive rate was reduced to 0,00018%.[128]

<https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[124] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[125] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[126] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[127] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020, p. 22; Patrick Grother, Mei Ngan and Kayee Hanaoka, 'Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification' (November 2018, NISTIR) <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf> accessed 01 December 2020.

[128] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020, p. 22.

In conclusion, the employment of real-time FRT comes with various risks, and the fact that police either has already been using it or thinks of using it in public to identify individuals makes it necessary to analyse the legal framework governing its possible employment in the EU.

Chapter 3: THE CURRENT LEGAL FRAMEWORK

This chapter focuses on an in-depth analysis of the current legal regime governing the employment of FRT by police in the public places in the European Union. It aims at answering the third sub-question of this thesis: "what is the current legal framework at European level that can be applied to real-time FRT used in the public places in the context of police work?". Currently, the employment of FRT is regulated in law through the rules protecting affected fundamental rights, the threat to which was identified in Section 2.4. Indeed, the human rights framework provides the means to analyse the compatibility of the use of the new technological innovations, such as FRT, with the protections provided for individuals in law. This framework aims at the identification of potential risks, and the protection of individuals from harm that might result from novel, uncertain technologies.[129] When developing new AI-based technologies, the human rights framework must be applied "holistically across the full algorithmic life cycle from conception and design to deployment".[130]

Regarding the structure of this chapter, firstly it will identify and explain the legislation applicable in case the employment of FRT by police. Since the employment of FRT is regulated through the legislation relating to the affected fundamental rights of individuals[131], it is crucial to analyse the rules related to those rights. The rules concerning some of the most important affected rights will be examined, including the right to: privacy, data protection, non-discrimination, freedom of expression and freedom of assembly and of association, an effective remedy, and a principle of good administration.

[129] Lorna McGregor, Daragh Murray and Vivian Ng, 'International Human Rights law as a framework for algorithmic accountability' (2019) 68 International and Comparative Law Quarterly 309.

[130] Lorna McGregor, Daragh Murray and Vivian Ng, 'International Human Rights law as a framework for algorithmic accountability' (2019) 68 International and Comparative Law Quarterly 314.

[131] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

3.1 The applicable law

The relevant pieces of legislation used for the analysis in this chapter will include the EU Charter, the ECHR and the Law Enforcement Directive.

The EU Charter has a limited scope of application, and it does not directly concern the national law enforcement agencies when employing the technology. In accordance with Article 51(1), the EU Charter applies only to the institutions and bodies of the Union, and to national legislators when they are implementing EU law.[132] Thus, the rules granted by the EU Charter will only have an indirect influence on the relevant national laws relating to the employment of FRT through the implementation of EU legislation into national legal systems, such as the implementation of Law Enforcement Directive.

The second piece of legislation relevant for the analysis is the ECHR. While it is enacted by the European Council and not the EU institutions themselves, it is crucial for any discussion involving human rights in the EU. All of the Member States are parties to the ECHR and need to follow its rulings.[133] Additionally, Article 6(3) of the Treaty of European Union asserts that the fundamental rights as guaranteed in the ECHR constitute general principles of EU law.[134] Moreover, Article 52 (3) of the EU Charter declares that "in so far as this Convention contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention".[135] Thus, the rights granted to individuals under the EU Charter should be interpreted taking into account the decisions of the European Court of Human Rights (ECtHR).

The last piece of legislation relevant for the analysis under this chapter is the Law Enforcement Directive. It applies to any activities relating to the processing of personal data wholly or partly by automated means, by competent authorities for "the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public

[132] Charter of Fundamental Rights of the European Union 2012, art. 51(1).

[133] Treaty Office, 'Chart of signatories and ratifications of Treaty 005' (Council of Europe, 25 February 2020) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=16IBVmpg> accessed 25 February 2020.

[134] TEU, art. 6(3).

[135] Charter of Fundamental Rights of the European Union 2012, art. 52(3).

security".[136] Thus, the rules of the Law Enforcement Directive are of paramount importance for police when employing FRT.

3.2 Fundamental rights affected

As explained above, it is the human rights framework that sets the limits to the use of new technologies. Most of these rights are not absolute, and can be subject to limitations, both under the framework of the EU Charter, and the ECHR.[137] Thus, even though FRT can be deemed as interfering with some of the rights, it might still be used if the criteria for the restriction of those rights are met.

This sub-chapter will focus on the analysis of the most important fundamental rights that are affected by the employment of FRT in public places by the police. The relevant legal framework will be analysed in general, and with regard to similar technologies (surveillance). Additionally, the conditions for the limitation of those rights will be discussed.

3.2.1 The Right to Privacy

As shown in the introduction and explained in Section 2.4.1, opponents of the employment of FRT by the police in Europe are first and foremost claiming that this technology infringes their right to privacy.[138] The main rationale underlying the concept of privacy in the European legal tradition is the protection of the inherent dignity of individuals.[139] Indeed, the right to privacy aims at protecting "the autonomy and human dignity of individuals, by granting them a personal sphere in which they can freely develop their personalities, think and shape their

[136] Directive 2016/680/EU, art. 1-2.

[137] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[138] Luana Pascu, 'EU no longer considering facial recognition ban in public spaces' (Biometric Update, 30 January 2020) <https://www.biometricupdate.com/202001/eu-no-longer-considering-facial-recognition-ban-in-public-spaces> accessed 13 February 2020.

[139] James Q Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 Yale LJ 1151.

opinions".[140] As such, it is a prerequisite that allows exercising other fundamental freedoms, for instance the freedom of expression or the freedom of assembly and of association.[141] In the EU, the right to privacy is protected both under Article 8 of the ECHR, and Article 7 of the Charter. Since those two rights are corresponding and the interpretation of ECtHR is relevant for the provision of EU Charter, the focus of this subchapter will lie on Article 8 of the ECHR. The first paragraph of the Article lies out the interests protected under the right, and the second paragraph sets out the conditions under which the right can be limited. The provision reads as follow:

Article 8: Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[142]

3.2.1.1 The scope of the right

Firstly, the scope of Article 8 should be discussed in order to understand the protected interests. Generally, the ECtHR has given an extensive interpretation to Article 8.[143] Even though originally coined as a negative freedom, Article 8 is now also setting positive obligations on the States to protect the privacy of the individuals. With time, the Court has gradually extended

[140] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (FRA, 2018), p. 19.

[141] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (FRA, 2018), p. 19.

[142] ECHR 1950, art. 8.

[143] ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Council of Europe 2019).

the protection of Article 8 to individual autonomy, self-expression, personal development and human flourishing.[144]

In order to invoke Article 8, the complaint in question needs to fall within at least one of the spheres enumerated in the provision, namely: private life, family life, home or correspondence.[145] The Court has not laid down precise rules regarding the interpretation of those dimensions, and usually analyses the concepts on a case-by-case basis.[146] The most relevant notion for the purpose of this thesis (as it includes surveillance)[147] is the dimension of private life, which will be explained below.

The Court tends to interpret the concept of private life broadly. The meaning and scope of this dimension can be inferred from the case-law of the Court.[148] This notion has been applied to a wide range of situations, and the Court in its guidelines divided them into three main categories: (1) physical, psychological and moral integrity; (2) privacy; (3) identity and autonomy.[149] Within the second category, the Court included various issues, among others data protection, right to access personal information, file or data gathering by security services or other organs of the state, and police surveillance.[150] Crucially, the Court does not limit the

[144] Bart van der Sloot, 'Privacy as human flourishing: could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?' (2014) 5 JIPITEC 230.

[145] ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Council of Europe 2019); Ivana Roagna 'Protecting the right to respect for private and family life under the European Convention on Human Rights' (Council of Europe, 2012) <https://www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf> accessed 01 April 2020.

[146] Ivana Roagna 'Protecting the right to respect for private and family life under the European Convention on Human Rights' (Council of Europe, 2012) <https://www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf> accessed 01 April 2020.

[147] ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Council of Europe 2019).

[148] ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Council of Europe 2019); Ivana Roagna 'Protecting the right to respect for private and family life under the European Convention on Human Rights' (Council of Europe, 2012) <https://www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf> accessed 01 April 2020.

[149] ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Council of Europe 2019).

[150] ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Council of Europe 2019).

concept of private life only to the private sphere, and extends to wider social interactions.[151] As held by the Court in *Von Hannover v Germany*: "there is a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life".[152]

3.2.1.2 Privacy in public

As public places are accessible and observable to anybody, the notion of privacy in public may seem counterintuitive to some.[153] However, the public sphere includes a wide range of private interests.[154] The recognition of protection of activities carried out in public by the Court started from asserting that the concept of private life includes also the right to establish and develop relationships and the right to fulfil one's personality.[155] Thus, private life cannot be limited only to an individual's inner circle, and must include wider social interactions, which are happening mostly in public.[156] Such recognition implies that the concept of private life "cannot be approached from a spatial and binary perspective in which an individual would surrender all privacy once he is in the outside world".[157] Indeed, the Court in its case-law "has increasingly suggested that the private life and the public life, the private sphere and the public sphere, and private activities and public activities are so intrinsically intertwined that both are provided protection under the scope of the right to privacy if this is essential to the development

[151] *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Council of Europe 2019), para 65 – 67.

[152] *Von Hannover v Germany* 2012, para 95.

[153] Bert-Jaap Koops, 'Privacy Spaces' (2018) 121(1) W. Va. L. Rev. 611.

[154] Bert-Jaap Koops and others, 'Typology of privacy' (2017) 38 (2) U. Pa. J. Int'l L. 483.

[155] *X v Iceland* 1976, p. 2; Bart van der Sloot, 'Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?' (2014) 5 Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 230, p. 238.

[156] ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Council of Europe 2019), para 65-70; Arthur Laudrain, 'Smart Cities, Technologies, Government Surveillance & Privacy' (Working Paper, Leiden University, Grotius Centre for International Legal Studies, 2019) <https://ssrn.com/abstract=3437216> accessed 01 November 2020, p. 14.

[157] Arthur Laudrain, 'Smart Cities, Technologies, Government Surveillance & Privacy' (Working Paper, Leiden University, Grotius Centre for International Legal Studies, 2019) <https://ssrn.com/abstract=3437216> accessed 01 November 2020, p. 14.

of an individual's public identity".[158] Additionally, in *Von Hannover v Germany* the Court held that activities of purely private nature can also take place when an individual is in public or semi-public places, and suggested that the nature of the activity is more important in the assessment than the location of the activity.[159] Thus, while the interference with the right of privacy can occur in public places, the activity interfered with needs to be of private nature. The Court gave examples of such activities, including "practising sport, out walking, leaving a restaurant or on holiday".[160] One of the important factors in determining the nature of an activity is whether the activity includes a participation in a public event. It suggests that an activity is of a public nature.[161]

3.2.1.3 Private life and the extraction and use of biometric data

Relevant for the purpose of this thesis is also the way the Court treats the extraction and the use of biometric data. The crucial case in that respect is *S. and Marper v the United Kingdom*, where the Court dealt with the issue of the retention of biometric information – fingerprint records and DNA samples.[162] In the case the Court emphasized that the retention of fingerprints interferes with Article 8(1), as fingerprints allow a precise identification and are "capable of affecting […] private life and retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant".[163]

Thus, according to the relevant case law of the Court any processing of biometric data constitutes an interference with private life under Article 8(1) of ECHR. The same reasoning can be applied to facial images matched using FRT, as this technology also allows for extraction of unique personal information and identification of an individual.[164]

3.2.1.4 Limitation of the right

[158] Bart van der Sloot, 'Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?' (2014) 5 Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 230, p. 238.

[159] Mathias Vermeulen, 'Surveille Deliverable D4.7 The scope of the right to private life in public places' (European University Institute, 27 July 2014), p. 33; *Von Hannover v Germany* 2012, para 30 and 110.

[160] *Von Hannover v Germany* 2004, para 61.

[161] *Friend and the Countryside Alliance and others v UK* 2009, para 42.

[162] *S and Marper v UK* 2008.

[163] *S and Marper v UK* 2008, para 84.

[164] *R (Bridges) v CCSWP and SSHD* 2019, para 57.

As indicated in Article 8(2), the right to privacy is not absolute, and it might be subject to limitations if the enumerated requirements for justified interference are met.[165] The first requirement, 'in accordance with the law', refers both to the need for a legal basis for an interference, and to the quality of the law in question, meaning that it needs to be accessible, foreseeable and precise.[166] Secondly, as it regards legitimate aims, the limitation can be introduced only if it is done to achieve one of the enumerated aims: "in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".[167] The last criteria, "necessary in the democratic society", entails the necessity, suitability, and proportionality tests *strictu sensu*.[168] In order to determine if the infringement is necessary in a democratic society, the Court balances the interests of the State against the right of an individual. The necessity itself is understood by the Court as implying "the existence of a 'pressing social need' for the interference in question".[169] Additionally, the Court considers whether the infringement was relevant and proportionate to the legitimate aim pursued.[170] It means that the interference should not go any further than what is strictly necessary to fulfil the aim, thus only the least intrusive measures can be used.[171]

[165] ECHR 1950, art. 8.

[166] George Katrougalos, 'It and the Tension between Privacy and Security: The Case of Surveillance of the Public Sphere' (2011) 8 US-China Law Review 579.

[167] ECHR 1950, art. 8(2).

[168] George Katrougalos, 'It and the Tension between Privacy and Security: The Case of Surveillance of the Public Sphere' (2011) 8 US-China Law Review 579.

[169] ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Council of Europe 2019), p. 12.

[170] ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Council of Europe 2019), p. 12.

[171] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (FRA, 2018), p. 40.

3.2.2 Data protection

The right to privacy and the right to personal data protection are related, however constitute distinct rights.[172] In the European legal framework, data protection is recognised as a separate right, and can be found in Article 8 of the EU Charter. It reads as follows:

Article 8: Protection of personal data

1. *Everyone has the right to the protection of personal data concerning him or her.*
2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
3. *Compliance with these rules shall be subject to control by an independent authority.*[173]

Article 8 of the EU Charter explicitly guarantees the right to data protection and refers to the most important data protection principles. It also ensures that an independent authority will control the implementation of the right.[174] Whenever the personal data is processed, the right of data protection is relevant, irrespective of the impact of such processing on the private life of an individual.[175] Indeed, the CJEU in *Digital Rights Ireland* found an interference with Article 8 merely as the law in question was providing for "the processing of personal data".[176] Thus, the scope of the right to data protection is broader than the scope of the right of privacy.[177] However, this right is not absolute and can be subject to limitations in case the conditions

[172] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (FRA, 2018), p. 18.

[173] EU Charter 2012, art. 8.

[174] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (FRA, 2018), p. 28.

[175] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (FRA, 2018), p. 20.

[176] Case C-293/12 *Digital Right Ireland* 2014.

[177] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (FRA, 2018), p. 20.

discussed in Article 52(1) of the EU Charter are met.[178] Thus, it can be limited in case the law provides for such a restriction, the essence of the right is respected, and in case such a limitation is proportional, necessary and is genuinely meeting the objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[179]

The right to data protection is further elaborated on in the European data protection legislation, the Law Enforcement Directive being the relevant piece of legislation for the purpose of this thesis. First, in order to analyse the application of the Directive to the employment of FRT by the police, it is necessary to analyse the scope, subject-matter and objectives, and relevant definitions.

Generally, in accordance with Article 2 of the Directive, it "applies to the processing of personal data by competent authorities for the purposes set out in Article 1(1)".[180] Personal data was defined in the Directive as "any information relating to an identified or identifiable person".[181] Processing is to be understood as any operation performed on personal data.[182] Competent authority means any public authority competent or any other body or entity entrusted by law to exercise public authority and powers for the purposes for which this Directive applies.[183] The Directive applies to the processing only for "purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".[184] Recital 12 of the Directive provides further insight into the activities which purpose would fall under with the Law Enforcement Directive:

(12) The activities carried out by the police or other law-enforcement authorities are focused mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities without prior knowledge if an incident is a criminal offence or not. Such activities can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. They also include

[178] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (FRA, 2018), p. 36.

[179] EU Charter 2012, art. 52(1).

[180] Directive 2016/680/EU, art. 2.

[181] Directive 2016/680/EU, art. 3(1).

[182] Directive 2016/680/EU, art. 3(2).

[183] Directive 2016/680/EU, art. 3(7).

[184] Directive 2016/680/EU, rec. 29.

maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence.[185]

Furthermore, it is important to define the concepts of 'controller' and 'processor'. Under the Directive, a controller is the competent authority which determined the purposes and means of processing of personal data.[186] On the other hand, a processor is a natural or legal person which processes personal data on behalf of the controller.[187]

Another important concept is the concept of biometric data, which under the Article 10 of the Directive is a special category of personal data encompassing "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".[188] Under this provision, special category of personal data can be processed only if the conditions enumerated in this provision are met. Such processing must be strictly necessary, and subject to appropriate safeguards for the rights and freedoms of the data subject. Moreover it must be either authorized by law, or it must protect the vital interests of the data subject or another natural person, or it must relate to data which are manifestly made public by the data subject.[189] The Article 29 Working Party considered that strictly necessary needs to be understood as "a call to pay particular attention to the necessity principle in the context of processing special categories of data, as well as to foresee precise and particularly solid justifications for the processing of such data".[190] Regarding 'appropriate safeguards', Recital 37 of the Directive provides examples of such possible safeguards: "the possibility to collect those data only in connection with other data on the natural person concerned, the possibility

[185] Directive 2016/680/EU, rec. 12.

[186] Directive 2016/680/EU, art. 3(8).

[187] Directive 2016/680/EU, art. 3(9).

[188] Directive 2016/680/EU, art. 10.

[189] Directive 2016/680/EU, art. 10.

[190] Article 29 Data Protection Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)' (29 November 2017).

to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data".[191]

Further, Article 11 of the Directive provides for a prohibition of a decision based on solely automated processing, including profiling, if such decision produces an adverse legal effect or significantly affects the data subject. 'Solely automated decision-making' means decision made by technological means without human involvement in the decision-making process.[192] Such a decision-making may be allowed only if it is authorised by law, and if suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are ensured.[193] Suitable measures can include the provision of specific information to the data subject, the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision.[194] It is important that the human intervention is carried out by a person who has the authority to change the decision.[195]

Moreover, under the Directive the processing of personal data must be conducted in a way which is (a) lawful and fair (b) following a specific, explicit and legitimate purpose, and (c) complying with the requirements of data minimization, data accuracy, storage limitation, data security and accountability.[196]

Lawful and fair processing

Both Recital 26 and Article 4(1)(a) of the Law Enforcement Directive provide for lawful and fair processing. Recital 26 holds that "any processing of personal data must be lawful, fair and

[191] Directive 2016/680/EU, rec. 37.

[192] Article 29 Data Protection Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)' (29 November 2017).

[193] Directive 2016/680/EU, art. 11(2).

[194] Directive 2016/680/EU, rec. 38.

[195] Article 29 Data Protection Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)' (29 November 2017).

[196] Directive 2016/680/EU, art. 4; European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

transparent in relation to the natural persons concerned".[197] Also Article 4(1)(a) obliges Member States to ensure that personal data is processed lawfully and fairly.[198]

Lawfulness means that there must be a legitimate ground for the processing. Fair processing relates to the relationship between the controller and the data subject, and it entails that a controller must inform the data subjects about the processing and ensure they understand the potential risks stemming from that particular processing.[199] Transparency is thus a crucial element of a fair processing. Transparency is provided for in Article 12 of the Directive – under this provision, the controllers need to take reasonable steps to provide information (the precise list included in Article 13) in a concise, intelligible and easily accessible form, using clear and plain language.[200] The provision of information is crucial for the fair processing, additionally promoting respect for dignity of the individual.[201] The EDPB in its guidelines (albeit relating to the GDPR) clarified that regarding video surveillance in public, it is necessary that warning signs are displayed informing the passers-by about it. The information should allow data subjects to easily recognize the circumstances of the surveillance and to estimate which area is surveilled before entering it, so that they could adjust their behaviour accordingly.[202] This warning sign should also convey the most important information regarding the processing of data, such as the purposes of processing, the identity of controller and the rights of a data

[197] Directive 2016/680/EU, rec. 26.

[198] Directive 2016/680/EU, art. 4(1)(a).

[199] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (FRA, 2018), p. 117.

[200] Directive 2016/680/EU, art. 12(1).

[201] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[202] European Data Protection Board, 'Guidelines 3/2019 on processing of personal data through video devices' (EDPB, 29 January 2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf> accessed 01 March 2020, p. 26.

subject.[203] However, police may still carry out activities such as covert investigations or video surveillance, relying on exceptions provided for in Article 13(3).[204]

Article 13: Information to be made available or given to the data subject

3. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedure

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties

(c) protect public security

(d) protect national security

(e) protect the rights and freedoms of others

Indeed, necessary and proportionate legislative measures, which take into account fundamental rights, can be adopted to delay, restrict or omit the provision of the information in order to achieve one of the enumerated aims.[205]

Specific, explicit and legitimate purpose

Another crucial principle of data protection law is the principle of purpose limitation, which is enshrined in Article 4(1)(b) of the Law Enforcement Directive. The provision states that personal data needs to be "collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes".[206] This principle has two components: the first one is the purpose specification, and the second one is the compatible

[203] European Data Protection Board, 'Guidelines 3/2019 on processing of personal data through video devices' (EDPB, 29 January 2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf> accessed 01 March 2020, p. 26.

[204] Directive 2016/680/EU, rec. 26.

[205] Directive 2016/680/EU, art. 13(3).

[206] Directive 2016/680/EU, art. 4(1)(b).

use.[207] The first component means that the initial purpose of collection needs to be specific, explicitly defined and legitimate. In its opinion on the draft of the directive, Article 29 Working Party stated that 'law enforcement' cannot be considered as one specified, explicit and legitimate purpose.[208] Thus, the authorities when processing personal data need to define the purpose for each processing.

The second component of this rule is a principle of compatible use.[209] Personal data can be processed exclusively for the purposes for which it was collected, unless further processing is compatible with the initial purpose of processing.[210] The compatibility between the purposes needs to be assessed on a case-by-case basis.[211] Moreover, in its opinion Article 29 Working Party was of belief that the further use of data relating to non-suspects should be prohibited. In addition to that the Article 29 Working Party affirmed that "such a restriction should also apply to the processing of sensitive data. Although they proved necessary for the crime for which they were collected, their necessity to the further use of the data should be demonstrated".[212] However, further processing, even if incompatible, can still be allowed under the Directive, if the conditions enshrined in Article 4(2) are met. Thus, such processing is allowed, if the

[207] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (2013), p. 4.

[208] Article 29 Working Party, 'Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' (2015).

[209] Catherine Jasserand, 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle Purpose Limitation' (2018) 4 Eur Data Prot L Rev 152.

[210] Catherine Jasserand, 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle Purpose Limitation' (2018) 4 Eur Data Prot L Rev 152; Article 29 Working Party, 'Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' (2015).

[211] Article 29 Working Party, 'Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' (2015).

[212] Article 29 Working Party, 'Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' (2015), p. 6.

controller is authorized to do so by law, and if such processing is necessary and proportionate to that purpose.[213]

Data minimization, data accuracy, storage limitation, data security and accountability

The principle of purpose limitation is accompanied by requirements of data minimization and the limitation of the retention of data. Data minimization, required in Article 4(1)(c), means that only the data strictly necessary for achieving a specific determined purpose can be processed.[214] It indicates that "a controller should strictly limit collection of data to such information as is directly relevant for the specific purpose pursued by the processing".[215] Moreover, the retention of data needs to be limited - data should be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed".[216] Additionally, data needs to be accurate, and the inaccurate data must be erased or rectified without delay, which constitutes a right of data subjects under Article 16.[217] Furthermore, the security of data constitutes an important issue. According to Article 4(1)(f), personal data should be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures".[218] Indeed, controllers and processors are obliged to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, especially if they are processing special categories of data, such as biometric data.[219] Moreover, the controllers need to implement appropriate measures "to effectively implement data protection principles and to integrate the necessary safeguards to meet the requirements of the regulation and protect

[213] Directive 2016/680/EU, art. 4(2).

[214] Article 29 Working Party, 'Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' (2015), p. 7.

[215] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (FRA, 2018), p. 125.

[216] Directive 2016/680/EU, art. 4(1)(e).

[217] Directive 2016/680/EU, art. 16(1).

[218] Directive 2016/680/EU, art. 4(1)(f).

[219] Directive 2016/680/EU, art. 29.

the right of data subjects".[220] The controllers need to implement such technical measures to ensure that by default only necessary personal data are processed, and that their retention and accessibility is limited.[221]

When deciding on the measures, the data controllers need to take into account: the state of art, the costs of implementation, the nature, the scope, context and purposes of processing, as well as the risks and their severity for the rights and freedoms of data subjects.[222] Such measures include for instance pseudonymisation, in order to protect the data by design.[223] Furthermore, if a type of processing (in particular when using new technologies) is likely to result in a high risk to the rights and freedoms of natural persons, data protection impact assessment (DPIA) needs to be carried out.[224] It is necessary to assess the possible risks and evaluate their legal permissibility.[225] Additionally, the controller or processor should consult the data protection authority (DPA) prior to processing, where "a data protection impact assessment indicated that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, or the type of processing, in particular, where using new technologies, mechanisms or procedure, involves a high risk to the rights and freedoms of data subjects".[226]

3.2.3 Non-discrimination

Another right potentially violated due to the use of FRT in public places by the police is the right of non-discrimination. Generally, discrimination can be divided into direct and indirect one. Direct discrimination takes place where "one person is treated less favourably than another

[220] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (FRA, 2018), p. 183.

[221] Directive 2016/680/EU, art. 20(2).

[222] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (FRA, 2018), p. 183; Directive 2016/680/EU, art. 20(1).

[223] Directive 2016/680/EU, art. 20(1).

[224] Directive 2016/680/EU, art. 27.

[225] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[226] Directive 2016/680/EU, art. 28.

is, has been or would be treated in comparable situation"[227] on the basis of a discriminatory ground. On the other hand, indirect discrimination takes place where a neutral practice puts certain persons at a particular disadvantage compared with others.[228] Non-discrimination provisions are included both in Article 21 of the EU Charter, and Article 14 of the ECHR and Article 1 of the Protocol No. 12 to the ECHR.

Under the EU Charter, Article 21(1) prohibits discrimination on the basis of certain grounds, and provides their non-exhaustive list.[229] Thus, individuals can complain in case the EU law or national laws implementing EU law are discriminatory on the basis of that provision.[230] Discrimination under the EU Charter can occur even if an individual himself/herself was not directly affected by a discriminatory measure.[231] However, it is possible to justify a discriminatory measure in relation to indirect discrimination if there is a legitimate aim and it is achieved in a proportional way.[232]

The right not to be discriminated against is also included in the ECHR, in Article 14 and in the Protocol No. 12 to the ECHR. Article 14 prohibits discrimination on the basis of enumerated grounds (sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status).[233] Unlike Article 21 of the EU Charter, Article 14 of the ECHR is not a freestanding right, and it requires that another fundamental right is infringed together with it.[234] The right not to be discriminated against relates only to "the enjoyment of the rights and freedoms set forth in this Convention".[235] It indicates that the ECtHR can only examine complaints of discrimination in

[227] Council Directive 2000/43/EC, art. 2(2)(a).

[228] Council Directive 2000/43/EC, art. 2(2)(b).

[229] EU Charter 2012, art. 21.

[230] European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law* (Council of Europe, 2018), p. 35.

[231] European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law* (Council of Europe, 2018), p. 43.

[232] European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law* (Council of Europe, 2018), p. 94.

[233] ECHR 1950, art. 14.

[234] European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law* (Council of Europe, 2018), p. 35.

[235] ECHR 1950, art. 14.

case "they fall within the ambit of one of the rights protected by the ECHR"[236], as Article 14 is of an ancillary nature.[237] Thus, the Court can only consider violation of Article 14 as an addition to a potential violation of another right protected by the ECHR, and not simply because certain measure appears to be discriminatory.[238] For instance, the violation of Article 14 would be examined in connection to a claim of violation of Article 6 - the right to a fair and public hearing, if the access to justice was precluded on a discriminatory basis.[239] However, it is the practice of the Court to still examine the claims of violation of Article 14 even if the other right itself (together with which the complaint was raised) was not infringed.[240] Generally, under the ECHR discrimination can be both direct and indirect.[241] However, an applicant must always be able to show that he/she was directly affected by a discriminatory measure concerned.[242] Furthermore, differential treatment, both direct and indirect, is subject to justification, where it pursues a legitimate aim and the means to pursue that aim are proportional. In such a situation a "justified differential treatment will not constitute discrimination".[243]

[236] European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law* (Council of Europe, 2018), p. 29.

[237] ECtHR, *Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No.12 of the Convention* (Council of Europe 2020), p. 6.

[238] European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law* (Council of Europe, 2018), p. 29.

[239] ECtHR, *Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No.12 of the Convention* (Council of Europe 2020), p. 6.

[240] European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law* (Council of Europe, 2018), p. 30.

[241] European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law* (Council of Europe, 2018), p. 53.

[242] European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law* (Council of Europe, 2018), p. 43.

[243] European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law* (Council of Europe, 2018), p. 93.

Additional protection is provided by Protocol No. 12 to the ECHR, which sets out a general prohibition of discrimination.[244] However, not all of the Member States of the EU have ratified this Protocol.[245] Article 1 of the Protocol No. 12 reads as follows:

Article 1: General prohibition of discrimination

1. *The enjoyment of any right set forth by law shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.*
2. *No one shall be discriminated against by any public authority on any ground such as those mentioned in paragraph 1.*[246]

Article 1 of the Protocol No. 12 has a wider scope than Article 14, as it concerns discrimination in relation to any right provided for in law, and any act, omission or practice by public authority.[247] This is a free-standing right, thus it can be applied alone.[248]

3.2.4 Freedom of expression and freedom of assembly and association

Furthermore, some of the identified risks of the employment of FRT relate to the rights of the freedom of expression and freedom of assembly and association. The freedom of expression is protected under Article 10 of the ECHR and Article 11 of the EU Charter. The freedom of assembly and of association is protected under Article 12 of the EU Charter and Article 11 of

[244] ECtHR, *Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No.12 of the Convention* (Council of Europe 2020), p. 9.

[245] Council of Europe, 'Chart of signatures and ratifications of Treaty 177' (Council of Europe, 26 November 2020) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/177/signatures> accessed 26 November 2020.

[246] Protocol No. 12 to the ECHR, art. 1.

[247] European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law* (Council of Europe, 2018), p. 33.

[248] ECtHR, *Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No.12 of the Convention* (Council of Europe 2020), p. 9.

the ECHR. As the meaning and the scope of those rights are the same under those two pieces of legislation, only provisions of the ECHR will be analysed in detail in this section.[249]

The relationship between those two rights is especially close.[250] The Court in *Eva Molnar v Hungary* held that: "one of the aims of freedom of assembly is to secure a forum for public debate and the open expression of protest. The protection of the expression of personal opinions, secured by Article 10, is one of the objectives of the freedom of peaceful assembly enshrined in Article 11."[251] The freedom of expression was described by the Court as "one of the basic conditions for the progress of democratic societies and for the development of each individual".[252] In the opinion of the Court, the importance comes from the fact that this freedom allows for pluralism, which in turn allows for "diverse political programmes to be proposed and debated".[253] Additionally, the protection concerns more than just the content of expressions, encompassing also the means of disseminating them.[254] The Court extends the protection to various means of transmission, also to transmission through demonstrations.[255] Thus, those two rights of freedom of expression and freedom of assembly and association are interconnected, with the Court even suggesting that the freedom of expression might be seen in certain cases (in which the aim of freedom of assembly is the expression of ideas) as a *lex generalisis* in relation to freedom of assembly, which would in such circumstances constitute *lex specialis*.[256] Thus, as the purpose of this thesis is to assess the employment of FRT in public spaces, the focus of this chapter will lie on Article 11 - the right to freedom of assembly. It is because this right is mostly exercised in public, especially in a form of a protest, which is especially prone to the risks associated with the use of FRT.

---

[249] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[250] Toby Mendel, 'Freedom of Expression: a guide to the interpretation and meaning of Article 10 of the ECHR' (Council of Europe, 21 February 2017) <https://rm.coe.int/09000016806f5bb3> accessed 25 March 2020.

[251] *Eva Molnar v Hungary* 2008.

[252] *Handyside v the UK* 1979.

[253] *Centro Europa 7 S.R.L. and Di Stefano v Italy* 2012.

[254] Toby Mendel, 'Freedom of Expression: a guide to the interpretation and meaning of Article 10 of the ECHR' (Council of Europe, 21 February 2017) <https://rm.coe.int/09000016806f5bb3> accessed 25 March 2020, p .6.

[255] Toby Mendel, 'Freedom of Expression: a guide to the interpretation and meaning of Article 10 of the ECHR' (Council of Europe, 21 February 2017) <https://rm.coe.int/09000016806f5bb3> accessed 25 March 2020, p. 6.

[256] *Ezelin v France* 1991.

Article 11 of the ECHR reads as follows:

Article 11: Freedom of assembly and association

1. *Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.*
2. *No restrictions shall be placed on the exercise of these rights other than such as are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others. This Article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State.*[257]

The freedom of assembly is not be interpreted restrictively, and it covers a wide range of peaceful gatherings. An assembly is defined by a common purpose of its participants.[258] The obligation of the Contracting States in relation to the right is to refrain from applying unreasonable restrictions on the right to assembly, protecting an individual from arbitrary interference with the right.[259] The right may include positive obligations as well, in order to secure the effective exercise of the right, such as taking preventive measures to ensure the safety of the citizens and the peacefulness of the gathering itself.[260] This right also can be subject to restrictions pursuant to Article 11(2). Interference does not need to constitute an outright ban, and it can also be caused by other actions of authorities.[261] The restrictions include

[257] ECHR 1950, art. 11.

[258] European Court of Human Rights, 'Guide on Article 11 of the European Convention on Human Rights' (Council of Europe, 31 December 2019).

[259] European Court of Human Rights, 'Guide on Article 11 of the European Convention on Human Rights' (Council of Europe, 31 December 2019).

[260] European Court of Human Rights, 'Guide on Article 11 of the European Convention on Human Rights' (Council of Europe, 31 December 2019).

[261] European Court of Human Rights, 'Guide on Article 11 of the European Convention on Human Rights' (Council of Europe, 31 December 2019), para 47.

measures taken before, during and after an assembly. Restrictions can include enforcement measures, such as crowd-control.[262]

Limits imposed on the right are justified if the requirements of Article 11(2) are met. Firstly, such an interference must be prescribed by law, meaning there needs to be a legal basis for it in domestic legislation, which fulfills the quality of law requirement.[263] Secondly, it must be imposed in order to achieve some legitimate aim, out of those enumerated in the provision: national security or public safety, the prevention of disorder or crime, the protection of health or morals or the protection of the rights and freedoms of others. The prevention of disorder is the most commonly used ground.[264] Lastly, an interference must be considered necessary in a democratic society.[265] The Court in its guidelines stated that: "in considering the proportionality of the measure account must be taken of its chilling effect"[266], meaning of a potential to deter people from participating in assemblies.[267]

3.2.5 The right to good administration and the right to an effective remedy

Besides the prominent fundamental rights affected, those employing FRT also need to take other issues into account. One of such issues is the right to good administration. It is enshrined in Article 41 of EU Charter; however, application of this provision is limited only to the work of the EU institutions, bodies and agencies. Nonetheless, it constitutes also a general principle of the EU law developed by the CJEU, and as such must be considered as a part of the EU law, with which the CJEU must ensure compliance.[268] As a general principle it can be applied to

[262] European Court of Human Rights, 'Guide on Article 11 of the European Convention on Human Rights' (Council of Europe, 31 December 2019), para 51.

[263] European Court of Human Rights, 'Guide on Article 11 of the European Convention on Human Rights' (Council of Europe, 31 December 2019), para 54.

[264] European Court of Human Rights, 'Guide on Article 11 of the European Convention on Human Rights' (Council of Europe, 31 December 2019), para 59.

[265] European Court of Human Rights, 'Guide on Article 11 of the European Convention on Human Rights' (Council of Europe, 31 December 2019), para 63.

[266] European Court of Human Rights, 'Guide on Article 11 of the European Convention on Human Rights' (Council of Europe, 31 December 2019), para 74.

[267] European Court of Human Rights, 'Guide on Article 11 of the European Convention on Human Rights' (Council of Europe, 31 December 2019), para 75.

[268] *H. N. v Minister for Justice, Equality and Law Reform, Ireland, Attorney General* 2014; European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context

actions of all state institutions.[269] The right to good administration includes, among others "the right of an individual to have access to their file and the obligation of any public authority to give reasons for its decisions".[270] Those obligations are crucial for individuals, as the access to files and receiving the reasons for the decisions are also influencing other fundamental rights, such as the right to a fair trial and the right to an effective remedy.[271] Some of the elements of the principle of good administration were translated into the EU data protection law and can be found in the provisions of the Law Enforcement Directive. [272] Indeed, data subjects can rely on Chapter III of the Directive to claim certain rights regarding their data. The rights granted to data subjects include: the right to receive information, the right to access personal data, the right to rectify personal data, the right to erase personal and restrict processing.[273] Firstly, as mentioned in Section 3.2.2, under Article 12 and Article 13 they have a right to receive certain enumerated information (and Article 13(3) allows Member States to restrict it).[274] Secondly, under Article 14 individuals have a right to access certain information relating to their personal

of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020; Eslpeth Berry and others, *EU law: text, cases and materials* (OUP 2015), p. 77.

[269] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[270] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[271] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[272] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[273] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (Council of Europe, 2018).

[274] Directive 2016/680/EU, art. 13(1).

data, for example the categories of data processed.[275] This right is subject to limitations under Article 15 – Member States can adopt measures restricting (wholly or partly) the data subject's right to access data if it is necessary and proportionate for certain enumerated purposes. Those purposes include: avoiding obstructing official or legal inquiries, investigations or procedures, avoiding prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, protecting public security, protecting national security, and protecting the rights and freedoms of others.[276]

The rules connected with the right to good administration constitute a precondition for the exercise of the right to an effective remedy, as it allows an individual to know about his data processing.[277] The right to effective remedy is guaranteed in Article 47 of the EU Charter, and it provides for a right to challenge any measure affecting the rights guaranteed by EU law. The right to compensation is provided for in the Law Enforcement Directive, where Article 56 ensures compensation will be paid by controller or competent authority to "any person who has suffered material or non-material damages as a result of an unlawful processing operation or of any act infringing national provisions adopted pursuant to this Directive".[278]

3.3 Conclusion

This chapter analysed the rights potentially affected by real-time FRT. Firstly, the right to privacy is infringed in case of an interference with private life of an individual. The ECtHR accepted that private life can be infringed in public places, and also in case of any processing of biometric data. However, this right can be limited if conditions of Article 8(2) are fulfilled. Secondly, when processing the data, police must adhere to the Law Enforcement Directive and the relevant data protection principles. Thirdly, there is a general prohibition of both direct and indirect discrimination, however there is a possibility of justification. Fourthly, freedom of expression, assembly and association was discussed, with the focus on the freedom of

[275] Directive 2016/680/EU, art. 14.

[276] Directive 2016/680/EU, art. 15.

[277] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[278] Directive 2016/680/EU, art. 56.

assembly. The states should refrain from applying restrictions on this right. However, it can be limited if the conditions are met. Lastly, the right to good administration and the right to an effective remedy were discussed. They include the right of individuals to have access to their files and be given the reasons for decisions. Additionally, the Law Enforcement Directive provides a number of rights to the data subjects regarding the processing of their data.

This chapter constituted an overview of the legal regime regulating FRT in the context of police work. Now it is necessary to apply this legal framework to the use of real-time FRT.

Chapter 4: THE REGULATORY GAP

The controversy surrounding the employment of FRT is focused on the tension between the notions of security and liberty, and the role of the state in that respect.[279] This chapter will focus on identifying possible regulatory gaps between the current state-of-law and the police's use of real-time FRT identifying individuals in public places and its risks (analysed in Section 2.4). In order to achieve this goal, the last sub-question of the thesis will be answered: "what risks to fundamental rights of individuals of the employment of real-time FRT are not (fully) addressed by the current state-of law regulating FRT in the EU?". Each affected right will be analysed separately, and rules regarding the rights will be applied to the employment of FRT and its risks. Lastly, the identification of the potential gaps in the legislation will follow.

4.1 Right to privacy & Data Protection

4.1.1 Application of FRT to Article 8 ECHR

The employment of real-time FRT by police in public places for the purpose of identification of individuals entails monitoring of public places, facial images acquisition, detecting and extracting facial features and comparing that information with database with facial images, searching for a match.[280] It is first necessary to examine whether such employment of real-time FRT by police falls within the scope of the right to privacy, and whether it infringes this right. Secondly, in case there is an infringement, the possibility for justification of this interference with the right needs to be analysed.

4.1.2.1 Infringement of Article 8(1)

The European Court of Human Rights has never answered the question whether the use of FRT in public infringes Article 8, however its case law concerning surveillance in public places offers some guidance.[281] As explained in Section 3.2.1, the Court in *von Hannover* recognized

[279] Roberto Iraola, 'Lights, Camera, Action - Surveillance Cameras, Facial Recognition Systems and the Constitution' (2003) 49 Loy L Rev 773.

[280] *R (Bridges) v CCSWP and SSHD* 2019.

[281] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council)

that some interactions of individuals in public can fall under the dimension of private life, as long as the activities they engage in are of private nature. Thus, the fact that real-time FRT is used in public does not by itself preclude the fact that private life of an individual might be infringed. Individuals can still expect that their privacy rights will be protected when shopping, walking on the street with a friend, or resting in the park. Moreover, private life considerations can arise when the monitoring by technological means of a public scene results in a systematic or permanent record about an individual.[282] Thus, in case the employment of FRT will result in such a record, Article 8(1) will be infringed.

Additionally, in the opinion of the ECtHR, facial images are crucial for the personal development[283], and constitute "one of the chief attributes of (…) personality"[284] of individuals. Moreover, data derived from FRT constitutes biometric data, as FRT extracts unique information about an individual allowing for his/her identification - just like in case of fingerprints and DNA.[285] Biometric information derived from facial features is precise and unique, and it is of intrinsically private character - regardless of the fact that facial features are seen by everybody.[286] Thus, facial biometric information engages Article 8 of ECHR. Moreover, the fact that data might be retained for a very short period does not affect the application of Article 8: "the application of Article 8 is not dependent on the long-term detention of biometric data"[287], and thus "Article 8 is triggered by the initial gathering of the information".[288] To conclude, the use of FRT in public places to identity individuals constitutes an interference with private life and entails infringement of Article 8(1).

4.1.1.2 Justification of the interference under Article 8(2)

<https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[282] *PG and JH v United Kingdom* 2001.

[283] ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Council of Europe 2019), para. 138.

[284] ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Council of Europe 2019), para. 138.

[285] *S and Marper v United Kingdom* 2008, para 84; *R (Bridges) v CCSWP and SSHD* 2019.

[286] *R (Bridges) v CCSWP and SSHD* 2019; *S and Marper v United Kingdom* 2008, para 84.

[287] *R (Bridges) v CCSWP and SSHD* 2019, para 59.

[288] *R (Bridges) v CCSWP and SSHD* 2019, para 59.

However, real-time FRT can still be used in public if the relevant requirements for justified interference from Article 8(2) are met, as explained in Section 3.2.1.4.

The first criteria, 'in accordance with the law' can be easily met by the Contracting States. It requires them to enact some form of a legal basis allowing the use of real-time FRT in public places by police. However, such legal basis would have to be of high quality, and specify all of the details regarding the employment of the technology in order to be foreseeable and precise.[289] Thus, it must specify whether, when, and how real-time FRT can be used.[290]

Regarding the second criteria: security, the prevention of disorder and crime, and protecting the rights of others are likely to be invoked in order to justify the employment of real-time FRT in the public places by the police.[291]

The third requirement, 'necessary in democratic society', requires to strike a balance between the right of privacy and the aim sought by interference – security and crime prevention. Ulrich Beck has characterized the modern society as a 'risk society', which essentially means that the central concern of governments is prevention and minimization of "risks and hazards systematically produced as part of modernization".[292] Indeed, the protection of individuals against non-state perils, terrorism and criminality in general, constitutes a crucial goal of public interest.[293] In order to provide the feeling of security, it is tempting for governments to curtail the right of privacy of individuals, and introduce pervasive regimes of surveillance.[294] Thus, it is likely that the issue of prevention of crime and security will be identified as a 'pressing social need' and considered important enough to introduce some limitations on the right to privacy. However, any such limitations on the right to privacy would need to be proportional. The High Court in the case *R (Ed Bridges) v CCSWP* (the analysis later deemed appropriate by the Court of Appeal) found that the way the technology was

---

[289] ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Council of Europe 2019), para 15 – 21.

[290] *R (Bridges) v CCSWP and SSHD* 2019, para 84.

[291] ECHR 1950; Daniel Solove, *Nothing to hide: the false tradeoff between privacy and security* (Yale University Press, 2011); Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[292] Ulrich Beck, *Risk society: towards a new modernity* (Sage Publications, 1992).

[293] George Katrougalos, 'It and the Tension between Privacy and Security: The Case of Surveillance of the Public Sphere' (2011) 8 US-China Law Review 579.

[294] Sophie Stalla-Bourdillon et al., *Privacy vs. Security* (SpringerBriefs, 2014).

deployed by the South Wales Police during the trials was fulfilling the criteria of 'proportionality' of Article 8. According to the court, the factors that contributed to deeming the technology proportionate were: transparency, time limit for the use, immediately discarding the Claimant's biometric data after no match was made (thus no retention of data), and not making the data available to any human agent. Moreover, nobody was wrongly arrested, nobody complained about the treatment.[295] Another factor that should be taken into account when assessing proportionality is the degree of errors the technology entails. The balance is between the acceptable number of false positives and the importance of finding individuals from the watchlist.[296] When deliberating on proportionality, the Court in *Bridges* noticed that although there is still a number of challenges when it comes to the performance of real-time FRT, the evidence suggests it can significantly contribute to the work of the police.[297] At the majority of the monitored events, at least one person had been identified and some arrests followed, which according to the Court constitutes an impressive result of the trials.[298] It seems like the current accuracy rates are acceptable to the Court. Furthermore, also the German authorities assessed the rate of false positives that occurred during the trials. The false positive rate when all three FRT systems were employed (0,00018%) was seen as acceptable, however the rate of 0,34% was unacceptable.[299]

Thus, it seems like the level of intrusiveness of real-time FRT as used by South Wales Police would be permissible under Article 8, provided an appropriate legal basis would be enacted. It is possible that courts would deny other specific applications, or allow more intrusive employments, depending on the nature or gravity of the context[300], for example in case of terrorist threats.

---

[295] *R (Bridges) v CCSWP and SSHD* 2019, para 101.

[296] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020, p. 22.

[297] *R (Bridges) v CCSWP and SSHD* 2019, para 106 – 107.

[298] *R (Bridges) v CCSWP and SSHD* 2019, para 104.

[299] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020, p. 22.

[300] *S and Marper v United Kingdom* 2008, para 119.

4.1.2 Application of FRT to Data Protection rules

As discussed in Section 3.2.2, the right to data protection of Article 8 of the EU Charter arises whenever the personal data is processed. Digital images containing a person's face are personal data (as explained in Section 2.1), thus Article 8 applies whenever FRT is used. Furthermore, the Law Enforcement Directive (the conditions for its applicability are analysed in Section 3.2.2) also applies when police forces employ FRT. Police constitutes a competent authority in the meaning of the Directive, and they process facial images for the enumerated purposes – such as crime investigation, prevention and execution of criminal penalties. It includes activities without prior knowledge of the offence. Moreover, police forces employing FRT are also controllers of the personal data. Thus, the Law Enforcement Directive rules need to be abided by police when using real-time FRT.

As facial images are considered biometric data, data processed by FRT is sensitive data under Article 10 of the Directive. Such data can be processed only if it is strictly necessary, which can be interpreted the same as the requirement of 'necessary in the democratic society' under Article 8 of the ECHR.[301] As seen in *R(Bridges) v CCSWP* case, the High Court was of the opinion that if the intrusion is not disproportionate, the use of the technology meets this requirement (the analysis from Section 4.1.1 applies).[302] Moreover, appropriate safeguards need to be implemented by police in order to employ FRT, such as adequate security measures and strict rule on the access of staff of the competent authority.[303] Lastly, such intrusion must be either: authorised by law; aiming at protecting the rights and freedoms of the data subject or another person; or relating to data made manifestly public by the data subject.[304] Member States can adopt a law which would allow such intrusion. Thus, if those requirements are met, FRT can be employed under Article 10.

As processing of facial images by FRT can produce an adverse legal effect or significantly affect an individual (for example it can lead to his or her arrest), a decision based on solely automated processing, without human intervention, cannot be taken. In the context of real-time FRT this issue can be solved by introducing a human contribution. During the trial of FRT by the London MET police, the initial stages of running of the technology were entirely based on automated processing, however when a match was found, the operator (ideally

[301] *R (Bridges) v CCSWP and SSHD* 2019, para 136.

[302] *R (Bridges) v CCSWP and SSHD* 2019, para 99 – 106.

[303] Directive 2016/680/EU, rec. 37.

[304] Directive 2016/680/EU, art. 10.

someone with training) judged the credibility of the match. Then, police officers on the ground conducted identity check.[305] This is sufficient for the prohibition not to apply to the employment of FRT, as the decisions would not be solely based on automated processing. That is, provided that the humans involved do not limit their intervention to a mere 'rubber-stamping' function. So far in all of the trials and deployments envisaged in the EU Member States, the human intervention was ensured, meaning that matches made were flagged to humans who subsequently evaluated then (eliminating many false positives) and had the power to decide whether to take action on the basis of the match.[306]

Lawful, fair and transparent

Transparency is a crucial element of both fair and lawful processing.[307] When employing FRT in public, police can ensure transparency through warning signs, informing passers-by about it and conveying the most important information regarding the processing of data. South Wales Police took steps to inform members of the public about the technology being used, including: advertising the deployment and its location on Facebook and Twitter, displaying large signs on the police vehicles equipped with real-time FRT, and at approximately a 100 radius of cameras, and handing out leaflets in the vicinity of the trial. Further, there was also an information regarding the trials on the police's website.[308] However, the purposes for which real-time FRT is deployed for, such as searching for terrorists or other criminals or suspects, would be most effective if the information about it was not provided to the public. Such limitation of the right

[305] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[306] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[307] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[308] *R (Bridges) v CCSWP and SSHD*, para 39.

to information pursuant Article 13(3) needs to be strongly justified.[309] Under Article 13(4), the Member States are called to adopt legislative measures determining the cases of processing in which the information does not need to be provided pursuant Article 13(3).[310]

Specific, explicit and legitimate purpose

The next principle, the principle of purpose limitation, also applies to data gathered when applying real-time FRT. Indeed, the purposes for each processing of facial images must be strictly determined and explicitly defined.[311] Such purposes could be combating terrorism and other forms of serious crime, "which is the well-established purpose limitation under EU law for law enforcement access to various large-scale EU databases".[312] However, it seems like those purposes are quite general, and could constitute a 'catch-all' phrase used by police whenever they want to use surveillance measures. It possibly defeats the idea behind the purpose limitation, since it might allow surveillance in case there is no imminent threat of crime, or no specific investigation to which the employment of FRT could contribute. The Court of Appeal in *Ed Bridges* case was of an opinion that the terms on which discretionary powers may be exercised should be specified in the relevant legal basis. Indeed, as the policies on the basis of which the technology was used by South Wales Police did not deal with this issue sufficiently, they failed to meet the requirement of the quality of law.[313] Nonetheless, it might be useful if this issue of purpose specification was also addressed at the EU level, by the EDPB, and certain threshold requirements regarding the discretion of police were established for the police forces of all of the EU's Member States.

---

[309] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[310] Directive 2016/680/EU, art. 13(4).

[311] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[312] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[313] *R (Bridges) v CC South Wales & ors* [2020] EWCA Civ 1058.

Regarding the principle of data minimization, only the facial images need to be processed in order to deploy FRT. Furthermore, the period of data retention needs to be specified. Generally, it seems like under those principles data of people who were not matched with a database (so data of non-suspects) should be discarded immediately after no match was made.[314] Similarly, the data of inaccurately matched individuals might need to be immediately erased. Conversely, the data of accurately matched criminals/suspects can be retained, but only as long as it is necessary for the purposes for which they are processed, following Article 4(1)(e). The High Court in the case of *R(Bridges) v CCSWP* considered retention periods established by the South Wales Police as adequate. The police would immediately delete both the facial images that were not matched, and biometric templates, regardless of whether the match was made. Additionally, facial images alerted against were either deleted immediately following the deployment, or within 24 hours. Match report could be retained for up to 31 days.[315] Thus, it is highly likely that such retention period would be considered appropriate for the purpose of running FRT. However, it is possible that the retention could be allowed to last longer, especially if the gravity of the offence or risk is high.[316] Furthermore, in the context of police's employment of FRT, it is necessary that a DPIA is carried out and the DPA is consulted.[317] Such a DPIA needs to properly assess the risks to the rights and freedoms of data subjects, and identify the measures envisaged to address the risks.[318] A DPIA which was carried out in the *Bridges* case was deemed deficient by the Court of Appeal. The reasons for that decision were that the DPIA did not lay down the requirements as to where the technology could be used, as

[314] Article 29 Working Party, 'Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' (2015), p. 6.

[315] *R (Bridges) v CCSWP and SSHD* 2019, para 38.

[316] Article 29 Data Protection Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)' (29 November 2017), p. 5.

[317] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[318] *R (Bridges) v CC South Wales & ors* [2020] EWCA Civ 1058 para 153.

well as to who may be included in a watchlist.[319] Lastly, it is necessary that data is accurate. In its Standard Operating Procedures, the South Wales Police included a stipulation that the images on the watchlists used for real-time FRT purposes need to be of quality. Furthermore, when the match is made, the police collect all of the necessary information to ensure the match is a true positive and the data concerning the confirmed false positives is not stored for longer than 24 hours after the deployment.[320]

The Law Enforcement Directive and its principles introduce a wide range of measures that need to be employed every time personal data is processed. However, if the requirements set therein are satisfied (for instance authorization in law, human intervention, transparency, adequate safeguards and others mentioned above), it is possible that real-time FRT is used by police. The Directive is believed to protect the interests of data subjects sufficiently.

4.1.3 What risks are left unaddressed by the law?

This section will analyse whether the risks to privacy of individuals connected with the employment of FRT by police in public are mitigated by the relevant laws. The risks include aggregation and the issue of self-censorship connected to the chilling effect.

Regarding the issue of aggregation, from *(R) Bridges v CCSWP* judgement of the High Court and its subsequent appeal judgement, together with other cases decided by the ECtHR and the CJEU, it can be deduced that aggregation is highly unlikely to be considered 'necessary in a democratic society'. As explained in Section 2.4.1, aggregation allows for creation of a comprehensive image of an individual and facilitates profiling. In *Digital Right Ireland*, the CJEU found that because traffic and location data if aggregated could create a detailed picture of individuals' private life, it constituted a very serious interference with Article 8 and 7 of the EU Charter.[321] Indeed, aggregation is likely to be seen as posing too grave risks to the privacy of individuals and constitutes an unproportionate intrusion. The measures that preclude aggregation of data consist of those stemming from the principles of data protection, and

[319] *R (Bridges) v CC South Wales & ors* [2020] EWCA Civ 1058 para 129-130.

[320] *R (Bridges) v CC South Wales & ors* [2020] EWCA Civ 1058, ANNEX A para 37 – 38.

[321] European Union Agency for Fundamental Rights, *Handbook on European data protection law* (FRA, 2018); Case C-293/12 *Digital Right Ireland* 2014.

include the short retention period, a limited time of surveillance and a specific purpose for surveillance (such as identification of specific individuals found on the watchlist[322]).

The most problematic risk of the employment of FRT by police in public seems to be an issue of the loss of anonymity and the resulting self-censorship. The very nature and the purpose of FRT entails identification, thus taking away this anonymity.[323] The issue can be to some extent addressed by the requirement of purpose limitation, provided it is not construed as a catch-all phrase, if it limits the identification only to individuals found on the watchlist. It would be helpful if the EDPB issued some sort of guidelines setting a minimum threshold for discretion of police forces regarding the purpose specification. However, it might not be enough to address the chilling effect - it is because it tends to be created even in case the mere awareness of the possibility of surveillance.[324] It seems like only a ban on this technology would fully address the risk of chilling effect, a scenario that might not be accepted by the authorities in the long-term in the increasingly technologically advancing world.[325]

4.2 Non-discrimination

4.2.1 Application of the right to non-discrimination to FRT

Generally, discrimination resulting from employing real-time FRT would be considered as indirect discrimination, as it is a neutral practice not aiming at differentiating among people, however it can put individuals of certain group in a disadvantageous position compared to

[322] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[323] The International Justice and Public Safety Network. ' Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field' (30 June 2011) https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf accessed 28 April 2020.

[324] Neil Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934.

[325] Desara Dushi, 'The use of Facial Recognition Technology in EU law enforcement: Fundamental rights implications' (2020, Global Campus South East Europe) <https://repository.gchumanrights.org/bitstream/handle/20.500.11825/1625/1.GlobalCampus2020_SouthEast_Europe.pdf?sequence=1&isAllowed=y> accessed 11 September 2020.

others.[326] The grounds on the basis of which discrimination is prohibited include the grounds relevant in the case of the employment of FRT technology. Those grounds are race, colour, sex, disability and age (the ECtHR has found that age is included among 'other status').[327]

Regarding the EU Charter, individuals can complain only in relation to the EU law and national law implementing EU law. However, the laws allowing for the employment of FRT by national police would be enacted by national law, and in that case the EU Charter protection would not apply.

Article 14 of ECHR applies in relation to other rights from the Convention. In the context of real-time FRT it can apply together with Article 8, in case "particular individuals are more vulnerable to privacy infringements due to algorithmic bias relating to sex, race, or ethnicity".[328] However, an individual needs to be directly affected by such a discriminatory measure, so only a person whose face was scanned and matched (falsely or not) can claim violation of Article 14 ECHR.

Moreover, Article 1(2) of the Protocol No. 12 applies in case of any discriminatory act, omission or practice by public authority. As the use of real-time FRT by police is a practice of a public authority, it should not be discriminatory. It entails that no other right of the Convention needs to be infringed for the discrimination to be prohibited by the provision. Thus, if the individual is directly affected by the discriminatory use of FRT by police, he/she can claim violation of Article 1(2) of the Protocol No. 12. In conclusion, the protection is provided by Article 14 ECHR and 1(2) of the Protocol 12. Article 14 can be applied together with other articles, and Article 1(2) can be applied alone. However, both provisions can be only applied if a person's face was scanned and matched.

---

[326] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020; European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[327] European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law* (Council of Europe, 2018) 190.

[328] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

4.2.2 What risks are left unaddressed by the law?

The prohibition of discrimination provided for by the Council of Europe requires that the police forces must "take active measures to ensure that neither the LFR [live facial recognition] technology nor its means of deployment violate the prohibition of discrimination. To do so, it is incumbent on those using LFR to understand its shortcomings, and the degree to which they affect issues of bias and discrimination".[329] Since the research into the discriminatory effect of this technology is currently not sufficient, it is necessary that further research into this issue is conducted in order to fully grasp the shortcoming of the FRT in this respect.[330] Nevertheless, any discrimination is prohibited under the relevant legislation at the European level, and the officials need to actively work towards the elimination of discrimination resulting from employing of real-time FRT.

However, the problem lies precisely in the fact that police officers are likely to interpret information in line with their own stereotypes.[331] For example, research suggest that regarding human intervention in case of automated decision making, humans overrule outcomes of the algorithms mostly if it confirms their pre-existing biases.[332] The risk is that mass-scale application of FRT will only support those biases, and may lead to a situation similar to

[329] Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020.

[330] Desara Dushi, 'The use of Facial Recognition Technology in EU law enforcement: Fundamental rights implications' (2020, Global Campus South East Europe) <https://repository.gchumanrights.org/bitstream/handle/20.500.11825/1625/1.GlobalCampus2020_SouthEast_Europe.pdf?sequence=1&isAllowed=y> accessed 11 September 2020.

[331] European Union Agency for Fundamental Rights, *Preventing unlawful profiling today and in the future: a guide* (FRA, 2018).

[332] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

"problematic practices such as racial profiling"[333], and support the creation of 'self-fulfilling prophecy'.[334] This issue is reinforced by the fact that algorithms are often not trained on faces of minorities, and that lighting aspect of images can heavily influence the outcome of FRT application.[335] Thus, since the system is already biased and taking into account the discriminatory potential of FRT, it seems like the general principle of prohibition of discrimination might not be enough to address the problem. It is because only directly affected individuals can claim violation, and it would be difficult for them to actually know and prove that the reason for their arrest or a false positive was the discriminatory effect of the technology. There is a need for a set of comprehensive guidelines addressing all of those nuances influencing the discriminatory potential of the real-time FRT, both relating to the technical aspects of the technology and the human aspects of the officers using it. Thus, it seems like the current rules on non-discrimination do not fully address the risk of discrimination stemming from the use of the technology.

4.3 Freedom of expression, assembly and association

4.3.1 The application of freedom of expression, association and assembly to FRT

An interference with freedom of expression, assembly and association can include any restrictions taken by the authorities. It also can include measures such as crowd-control. As explained above, the employment of FRT by the police during protests deters people from participating in such demonstrations, and constitutes a chilling effect where individuals refrain from lawfully exercising those rights. Therefore, the deployment of FRT during demonstrations constitutes an interference with the right to the freedom of assembly, also the

[333] Lucas Introna and Helen Nissenbaum, 'Facial Recognition Technology: A Survey of Policy and Implementation Issues' (the Center for Catastrophe Preparedness and Response, 2010) <https://eprints.lancs.ac.uk/id/eprint/49012/1/Document.pdf> accessed 17 January 2020.

[334] European Union Agency for Fundamental Rights, *Preventing unlawful profiling today and in the future: a guide* (FRA, 2018), p. 48.

[335] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

right to freedom of expression. However, both of those rights can be restricted if the enumerated requirements justifying interference are met.[336] The Contracting States can introduce national laws on the basis of which such deployments will be conducted. As in the case of the interference with Article 8, FRT can be introduced in order to provide security, to prevent the disorder and crime, and protecting the rights of others. The most problematic criteria in this case would be 'necessary in the democratic society'. The threshold will be especially high regarding the deployment of FRT during the protests and demonstrations.[337]

4.3.2 What risks are left unaddressed by the law?

The main risk in case of freedom of expression, association and assembly connected with real-time FRT deployment is that it creates a chilling effect and deters people from exercising their democratic rights. The chilling effect entails stifling of the development and the exchange of ideas due to the presence or even awareness of surveillance. Indeed, most forms of surveillance seek some form of control over others, influencing or being able to respond to others' behaviour.[338] Thus, chilling effect would take place regardless of any measure ensuring proportionality of the employment of FRT. Indeed, the presence of any kind of surveillance during protest was judged critically by the participants of the assembly, and they considered it to be intimidating, intrusive and restrictive in relation to the right of peaceful gatherings.[339] Additionally, the right to freedom of peaceful assembly, just like freedom of expression, constitute one of the foundations of such a society and are of paramount importance.[340] Taking into consideration the importance of those freedoms to democracy, the chilling effect in that

[336] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[337] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[338] Neil Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934.

[339] Valerie Aston, 'State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives' (2017) 8(1) European Journal of Law and Technology.

[340] European Court of Human Rights, 'Guide on Article 11 of the European Convention on human Rights' (Council of Europe, 31 December 2019).

context might be addressed only through banning the use of real-time FRT, at least during protests.

4.4 The right to good administration and other issues

4.4.1 The right to good administration

The police need to comply with the right to good administration and with the rights enumerated in the Law Enforcement Directive when processing facial images using FRT.[341] However, complying with those rules is likely to be extremely challenging. There are two main issues: the problem of ensuring that potentially a huge number of individuals will have to be informed of the processing of the images of their faces, and also given access to their files.[342] The Member States are likely to adopt measures restricting the right of access of data subjects, pursuing Article 15 of the Law Enforcement Directive, in order to ensure the effectiveness of police work, and restricting the provision of information pursuing Article 13(3). [343] In order to ensure that the right to remedy is still effective even in case individuals are not aware about the processing of their data, it is necessary that independent accountability mechanisms are in place: "a combination of internal and external monitoring bodies, active at different stages of the process (before, during, and after the use of facial recognition technologies)".[344]

[341] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[342] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[343] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

[344] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019)

4.4.2 Inaccuracy and the right to an effective remedy

The issue of inaccuracy is mitigated to some extent in law through the right to an effective remedy and the right to compensation. Individuals can seek damages under the Law Enforcement Directive in case they were falsely matched and suffered some damages.[345] Another element mitigating the issue of inaccuracy is a substantive role of human intervention when approving a match. This contribution ensured that many mistakes are ruled out before approaching a matched person.[346] However, even though the official error rates are quite small[347], inaccuracy still constitutes a problematic aspect of this technology as it has a potential of causing a lot of distress to individuals. Thus, it is important to reduce its potential for mistakes, for example by ensuring data quality and that the training databases are provided with diverse facial images.[348] Additionally, there should be some sort of possibility or even an obligation to correct the algorithm in case someone's face triggers FRT and is stopped on the basis of a false match. It is important so that the mistake is not repeated, and the situation such as in the case of Steve Talley would be avoided. All of those issues should be addressed by authorities in some way, for example through technical guidelines.

<https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020, p. 31.

[345] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020, p. 32.

[346] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020, p. 26.

[347] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020, p. 22; Patrick Grother, Mei Ngan and Kayee Hanaoka, 'Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification' (November 2018, NISTIR) <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf> accessed 01 December 2020.

[348] European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020.

4.5 Conclusion

In conclusion of this chapter, the employment of real-life FRT by police in public places infringes certain fundamental rights of individuals enshrined in the ECHR: the right of privacy, the right not to be discriminated against, and the right to freedom of expression, assembly and association. Additionally, it triggers the application of data protection rules of the Law Enforcement Directive. Moreover, some of the rights guaranteed by the EU law, such as the right to good administration, may be really challenging to fulfil when using real-time FRT in public places. A lot of risks to those rights, identified in Section 2.4 of this thesis, are mitigated by responsible and stringent employment of the technology. However, many risks are still left unaddressed and require more attention by the European Union's watchdogs and regulators.

Chapter 5: CONCLUSION

In today's risk societies surveillance technologies are considered crucial for the work of law enforcement agencies and are seen as indispensable tools in the fight against crime and terrorism. Facial Recognition Technology is becoming increasingly sophisticated and its application in the everyday work of police becomes common. Today's trials of real-time FRT are just a start of the new way of employment of this technology, and soon enough such use may become an ordinary practice, with facial recognition software built into the CCTV cameras network surveilling our streets. Therefore, it is increasingly important to evaluate the present-day regulation of such application of this technology. This thesis researched the extent of a regulatory gap between the current state-of-law and the risks of the employment of real-time FRT by police to identify individuals in the public places in the EU. This question is of a paramount importance, as the literature touching upon the regulation of real-time FRT in the context of law enforcement agencies, let alone any evaluation of its adequacy, is scarce.

Firstly, this thesis outlined the inner workings of FRT. Moreover, it analysed the factors influencing the accuracy of matches, such as the quality of images and the choice of a development set. Furthermore, it addressed the way the technology is being used by the police in the UK and the EU. The EU's Member States that used real-time FRT include France and Germany, which conducted trials on groups of volunteers, and currently are not employing it in public due to the lack of the legal basis to do so.

The second chapter identified risks stemming from the employment of real-time FRT by police to some of the fundamental rights, including the right to: privacy, data protection, non-discrimination, freedom of expression, assembly and association, good administration and effective remedy. In the following chapters (third and fourth), the real-time FRT was analysed from the perspective of the fundamental rights at risk. Indeed, it is mostly the human rights framework that limits the use of FRT. In the third chapter the law at the European level that sets boundaries to the use of FRT along with its real-time application, was analysed. The relevant legal documents are the ECHR, the EU Charter and the Law Enforcement Directive. Outlining this framework was crucial in order to later analyse the kind of deployment that would be allowed under those rules and assess whether such legal application poses any further threats to the liberty of individuals. The fourth chapter applied the law to the use of FRT by police in public places, and assessed whether the law mitigates the earlier identified risks. The analysis in the second, third and fourth chapter was as follows:

1) **The right to privacy and data protection**: The right to privacy was analysed together with data protection rules. The main risks of application of real-time FRT were stripping away the anonymity, leading to the creation of a chilling effect, and negatively affecting autonomy, self-development and individualism. Furthermore, the risk of aggregation of data was brought up. Generally, the relevant rules considerably limit the way the technology can be used. It was concluded that the employment of real-time FRT in public does infringe Article 8 of the ECHR, and its use is only possible if the conditions for justified interference of Article 8(2) are met. Thus, there needs to be a legal basis allowing for such use of the technology, it must be deployed for the purpose of security or the prevention of crime, and it needs to be necessary. The factors that would likely contribute to deeming the use of this technology as meeting this criterion of 'necessary', based on the *R (Ed Bridges) v CCSWP* decision, are: transparency, time limit for the use, limiting the employment to a specific purpose of trying to identify individuals from the watchlist, immediately discarding biometric data if no match is made (thus no retention of data longer than it is necessary), and not making the data available to any human agent. Furthermore, the current accuracy rates are likely to be considered acceptable by the authorities and the courts. However, it is possible that the courts would deny other specific applications, or allow more intrusive employments, depending on the gravity of the context. Furthermore, data protection rules impose further conditions on the use of real-time FRT. Firstly, it is necessary that appropriate safeguards, such as adequate security measures, are implemented when using the technology. It is also of importance that a DPIA is carried out or a DPA is consulted. Additionally, a significant human contribution needs to be introduced when taking a decision based on a produced match. Moreover, transparency of the use should be ensured, and any limitation of transparency needs to be strongly justified.
2) **The right to non-discrimination**: There are two main risks connected with the use of real-time FRT. First is that the technology will be used in a discriminatory way, for example in certain racially diverse neighborhoods. Second is that bias might be built into the technology due to the under-representation of women and people of colour in the development sets, as well as the fact that during the application phase, the lighting can considerably affect the quality of facial images of dark-skinned people. As a result, FRT can be as problematic as racial profiling. Regarding the relevant rules, under Article 14 and Article 1 of the Protocol No. 12 individuals directly affected by a

discriminatory measure on the basis of their race, colour, or sex can claim that their right not to be subjected to the discrimination was violated. Since any discrimination is prohibited, the officials need to work towards the elimination of any biases built into the system or resulting from the employment of the technology.

3) **The right to freedom of expression, association and assembly**: The most prominent risk is the chilling effect, limiting the free flow of opinions and ideas, and discouraging from the right to protest. Generally, the employment of FRT by the police during demonstrations constitutes an interference with the right to the freedom of assembly of Article 11 of the ECHR and Article 12 of the EU Charter, as well as the freedom of expression under Article 10 of the ECHR and Article 11 of the EU Charter. However, the use can be justified, if the criteria for limitation (the same as in the case of the right to privacy) will be met. The threshold for the 'necessary in the democratic society' would be especially high in case of the employment of FRT during protests.
4) **The right to good administration and to an effective remedy**: The technology can be inaccurate, which may lead to arresting a wrong person. Furthermore, the police need to comply with the rule of good administration and the rights enumerated in the Law Enforcement Directive. It includes the right of individuals to have access to their files and be given reasons for the decisions. This is likely to be problematic, since the potentially huge numbers of individuals will have to be informed and provided with different rights. It is probable that those rights will be restricted under the relevant provisions. The right to good administration constitutes a precondition for the exercise of the right to an effective remedy, which provides for a right to challenge any measure affecting the rights guaranteed by EU law.

The last analysis of chapter four was crucial for determining the extent of the regulatory gap, and it aimed at undercovering whether the issues and risks connected with the employment of real-time FRT in public by police would be still present in case of a legal use of the technology:

1) **The right to privacy and data protection:** Generally, there is no threat of aggregation under the current laws – indeed, the short retention period requirement, a limited time of surveillance and a specific purpose for surveillance are enough to tackle the problem. Regarding the purpose limitation, it would be helpful if the EDPB issued some sort of guidelines setting a minimum threshold for discretion of police forces regarding the

purpose specification. Furthermore, the current law does not cover the issue of the potential chilling effect, as it might be created by a mere awareness of the possibility of surveillance. The risk would be only fully addressed by banning the use of the technology altogether, a scenario not likely to be accepted by the authorities in the long-term.

2) **The right to non-discrimination**: The technology seems to be biased towards women and people of color mainly because of the development sets and the issues connected with the lighting. The problem is reinforced by the fact that police officers tend to interpret the information in line with their own implicit biases. The big risk is that any mass-scale application of FRT will only support those biases. There are many nuances when using FRT that need to be identified, named and directly addressed in order to mitigate the problem. It seems like the current rules regarding non-discrimination do not fully address this complex problem, as only the directly affected individuals can exercise the right. The issue is that the individuals would not even know of the discrimination and would not be able to challenge it. Thus, the technology should not be employed unless its discriminatory potential is mitigated. It could be mitigated to some extent by a set of comprehensive guidelines addressing all of those discriminatory nuances, both relating to the technical aspects of the technology and the aspects of the human use. Thus, the right to non-discrimination does not fully address the risk of discrimination.
3) **The right to freedom of expression, assembly and association**: As the risk connected with those rights concerns the creation of the chilling effect, it cannot be adequately addressed by any measures ensuring proportionality of the employment. Taking into account the importance of those freedoms for democracy, only a full ban on the use of the technology, at least during demonstrations, will constitute an adequate response to the problem. As the relevant provision seems to allow employment of this technology in case if the proportionality requirement is fulfilled, it appears that the issue of the chilling effect on democratic freedoms is not fully addressed by the current rules.
4) **Other issues:** Inaccuracy is mitigated to some extent in law through the right to an effective remedy and the right to a compensation, as well through the mandatory human intervention. However, it still constitutes a pertinent problem that is not effectively addressed under current rules. It is crucial to introduce an obligation to correct the algorithm in case of reoccurring mistakes.

While some potential issues are addressed by the law, many by the proportional use of the technology, there are still some risks that remain pertinent. The regulatory gap between the current state of law and the risks stemming from the use of the technology by police in public places of the EU is created where there are issues/nuances unaddressed by the legal rules. First issue is that the rights to privacy, data protection, and freedoms of expression, assembly and association do not address the risk of the chilling effect. It is always created when such surveillance technologies are used, and it affects, among others, self-development and autonomy of individuals, leading to de-individualisation and affecting the free flow of opinions and ideas. The second issue is the risk of discrimination that is not addressed under the current right to non-discrimination, as only the directly affected individuals may claim their right was violated. However, it would be difficult for them to be even aware that their arrest or false matching was due to the discriminatory effects of the technology. Lastly, the issue of inaccuracy is not fully covered in the current law, thus it is necessary that this topic is included in some technical guidelines.

This thesis focused mainly on legal analysis and evaluation of one specific application of FRT: real-time application in public to identify individuals by police. It should be noted that besides this context, this technology is increasingly used by various entities, both private and public, and for different purposes. Narrowing the research only to specific application means that the conclusion of this thesis cannot be directly applied to other uses of FRT by other entities. It is recommended that further research is carried out on this topic. Additionally, European Data Protection Board should provide an opinion or some sort of guidelines on the topic of the use of real-time FRT by police in public, addressing first and foremost the technical shortcoming of the technology.

BIBLIOGRAPHY

1. Primary sources:

1.1 Legislation:

1. Charter of Fundamental Rights of the European Union [2012] OJ 1 326/393
2. Consolidated Version of the Treaty on the European Union [2012] OJ 326/15
3. Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ 180/22
4. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ 2 119/89
5. European Convention of Human Rights 1950
6. Protocol 12 to the European Convention on Human Rights and Fundamental Freedoms on the Prohibition of Discrimination 2000

1.2 Cases:

7. Case C-293/12 *Digital Right Ireland* (2014) ECLI:EU:C:2014:238
8. Case C-604/12 *H. N. v Minister for Justice, Equality and Law Reform, Ireland, Attorney General* (2014) ECLI:EU:C:2012:744
9. *Centro Europa 7 S.R.L. and Di Stefano v Italy* [2012] ECHR 974
10. *Eva Molnar v Hungary* [2008] ECHR 1027
11. *Ezelin v France* [1991] ECHR 29
12. *Friend* and *Countryside Alliance v United Kingdom* [2009] ECHR 2068
13. *Handyside v United Kingdom* (1979) 1 EHRR 737
14. *PG and JH v United Kingdom* [2001] ECHR 550
15. *R (Bridges) v CCSWP and SSHD* [2019] EWHC 2341 (Admin)

16. *R (Bridges) v CC South Wales & ors* [2020] EWCA Civ 1058
17. *S and Marper v United Kingdom* [2008] ECHR 1581
18. *Von Hannover v Germany* (2005) 40 EHRR 1
19. *Von Hannover v Germany* (No. 2) (2012) 55 EHRR. 5
20. *X v Iceland* App no 6825/74 (ECtHR, 1976)

2. Secondary sources:

2.1 Guidelines and opinions

21. Article 29 Data Protection Working Party, 'Opinion 2/2012 on facial recognition in online and mobile devices' (22 March 2012)
22. Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (02 April 2013)
23. Article 29 Working Party, 'Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' (01 December 2015)
24. Article 29 Data Protection Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)' (29 November 2017)
25. Court of Justice of the European Union, 'Relating to the Charter of Fundamental Rights' (CJEU, 17 December 2015)
26. European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence' (Council of Europe, 31 August 2019)
27. European Court of Human Rights, 'Guide on Article 11 of the European Convention on human Rights' (Council of Europe, 31 December 2019)
28. European Court of Human Rights, 'Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No.12 of the Convention' (Council of Europe, 31 August 2020)
29. European Data Protection Board, 'Guidelines 3/2019 on processing of personal data through video devices' (EDPB, 29 January 2020)

<https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf> accessed 01 March 2020

2.2 Books:

30. Ulrich Beck, *Risk society: towards a new modernity* (Sage Publications, 1992)
31. Elspeth Berry and others, *EU law: text, cases and materials* (OUP, 2015)
32. European Union Agency for Fundamental Rights, *Handbook on European data protection law* (FRA, 2018)
33. European Union Agency for Fundamental Rights, *Preventing unlawful profiling today and in the future: a guide* (FRA, 2018)
34. European Union Agency for Fundamental Rights, *Handbook on European non-discrimination law* (Council of Europe, 2018)
35. Stan Z Li and Anil K Jain, *Handbook of Face Recognition* (Springer, 2011)
36. George Orwell, *Nineteen Eighty-four* (1949)
37. Daniel Solove, *Nothing to hide: the false tradeoff between privacy and security* (Yale University Press, 2011)
38. Sophie Stalla-Bourdillon and others, *Privacy vs. Security* (SpringerBriefs, 2014)
39. John D. Woodward, Katharine W. Webb and others, 'A Primer in Biometric Technology' in: *Army Biometric Application: Identifying and Addressing Sociocultural Concerns* (RAND Corporation 2001)

2.3 Reports:

40. European Union Agency For Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 27 November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 24 February 2020
41. Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019, Economic & Social Research Council) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-

ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 24 January 2020

42. The International Justice and Public Safety Network. 'Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field' (30 June 2011) <https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf accessed 28 April 2020 > accessed 21 April 2020
43. Mathias Vermeulen, 'Surveille Deliverable D4.7 The scope of the right to private life in public places' (European University Institute, 27 July 2014)

2.4 Journals:

44. Andy Adler and Michael E Schuckers, 'Comparing Human and Automatic Face Recognition Performance' (2007) 37(5) IEEE Transactions on Systems, Man, and Cybernetics 1248
45. Valerie Aston, 'State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives" (2017) 8(1) European Journal of Law and Technology
46. Kanya A Bennett, 'Can Facial Recognition Technology Be Used to Fight the New Way against Terrorism: Examining the Constitutionality of Facial Recognition Surveillance Systems' (2001) 3 NC JL & Tech 151
47. Philip Brey, 'Ethical Aspects of Facial Recognition Systems in Public Places' (2004) 2 Info, Comm & Ethics in Society 97
48. Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 1
49. Julie E Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stan L Rev 1373
50. Cynthia Cook and others, 'Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems' (2019) 1 IEEE Transactions on Biometrics, Behavior and Identity Science 1.

51. Masa Galic and others, ‘Betham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation’ (2017) 30(1) Philosophy and Technology 9
52. Mariko Hirose, 'Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology' (2017) 49 Conn L Rev 1591
53. Lucas Introna and Helen Nissenbaum, ‘Facial Recognition Technology: A Survey of Policy and Implementation Issues’ (the Center for Catastrophe Preparedness and Response, 2010) https://eprints.lancs.ac.uk/id/eprint/49012/1/Document.pdf accessed 17 January 2020
54. Roberto Iraola, 'Lights, Camera, Action - Surveillance Cameras, Facial Recognition Systems and the Constitution' (2003) 49 Loy L Rev 773
55. Catherine Jasserand, 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle Purpose Limitation' (2018) 4 Eur Data Prot L Rev 152
56. George Katrougalos, 'It and the Tension between Privacy and Security: The Case of Surveillance of the Public Sphere' (2011) 8 US-China Law Review 579
57. Bert-Jaap Koops, ‘Privacy Spaces’ (2018) 121(1) W. Va. L. Rev. 611
58. Bert-Jaap Koops and others, ‘Typology of privacy’ (2017) 38 (2) U. Pa. J. Int’l L. 483
59. Arthur Laudrain, ‘Smart Cities, Technologies, Government Surveillance & Privacy’ (Working Paper, Leiden University, Grotius Centre for International Legal Studies, 2019) <https://ssrn.com/abstract=3437216> accessed 02 April 2020
60. Bridget Mallon, 'Every Breath You Take, Every Move You Make, I'll Be Watching You: The Use of Face Recognition Technology' (2003) 48 Vill L Rev 955
61. Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40 UNSWLJ 121
62. Lorna McGregor, Daragh Murray and Vivian Ng, ‘International Human Rights law as a framework for algorithmic accountability’ (2019) 68 International and Comparative Law Quarterly 309
63. Julian Murphy, ‘Chilling: the Constitutional Implications of Body-Worn Cameras and Facial Recognition Technology at Public Protests’ (2018) 75(1) Wash. & Lee L. Rev. Online
64. Sharon Nakar and Dov Greenbaum, 'Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy' (2017) 23 BU J Sci & Tech L 88
65. Neil Richards, ‘The Dangers of Surveillance’ (2013) 126 Harvard Law Review 1934

66. M Selvapriya and J Komala Lakshmi, ‘Face Recognition Using Image Processing Techniques: A survey’ (2014) 3(12) International Journal of Engineering and Computer Science
67. Christopher Slobogin, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity' (2002) 72 Miss LJ 213
68. Wen-Yi Zhao, Rama Chellappa and others, ’Face Recognition: A Literature Survey’ (2003) 35(4) ACM Computing Surveys 399
69. Bart van der Sloot, ‘Privacy as human flourishing: could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?’ (2014) 5 JIPITEC 230
70. Daniel Solove, ‘A taxonomy of privacy’ (2006) 154(3) University of Pennsylvania Law 477
71. James Q Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 Yale LJ 1151

3. Other sources:

72. I.Resist Facial Recognition' (Liberty) <https://www.libertyhumanrights.org.uk/resist-facial-recognition> accessed 01 October 2019
73. Big Brother Watch, ‘Face off: the lawless growth of facial recognition in UK policing’ (2018) 3
74. Tonja Bohm, 'Wir mussen Gesichtserkunnung mit KI regulieren - und zwar jetzt' (Microsoft Berlin, 20 February 2019) <https://www.microsoft.com/de-de/berlin/artikel/wir-mussen-gesichtserkennung-mit-ki-regulieren-und-zwar-jetzt.aspx> accessed 28 October 2019
75. Jason Brownlee, ‘A gentle introduction to Deep Learning for Face Recognition’ (Machine Learning Mastery, 31 May 2019) https://machinelearningmastery.com/introduction-to-deep-learning-for-face-recognition/ accessed 01 November 2020
76. Joy Buolamwini, ‘United States House Committee on Oversight and Government Reform: hearing on Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties’ (22 May 2019) <https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-BuolamwiniJ-20190522.pdf> accessed 25 November 2020.

77. Fabio Chiusi, ‘Automating society: Italy’ (AlgorithmWatch, 29 January 2019) <https://algorithmwatch.org/en/automating-society-italy/> accessed 25 January 2020
78. Council of Europe, ‘Chart of signatures and ratifications of Treaty 177’ (Council of Europe, 26 November 2020) < https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/177/signatures> accessed 26 November 2020
79. Jane Croft and Madhumita Murgia, ‘UK court backs Welsh police use of facial recognition technology’ (Financial Times, 04 September 2019) <https://www.ft.com/content/92d7d5f0-cefb-11e9-99a4-b5ded7a7fe3f> accessed 28 October 2019
80. Janosch Delcker, 'Big Brother in Berlin' (13 September 2018, Politico) <https://www.politico.eu/article/berlin-big-brother-state-surveillance-facial-recognition-technology/> accessed 28 October 2019
81. Angel Diaz, ‘New York City Department Surveillance Technology’ (Brennan Center for Justice, 4 October 2019) <https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology> accessed 21 January 2020
82. 'Dutch police facial recognition database includes 1.3 million people' (22 July 2019, DutchNews.nl) <https://www.dutchnews.nl/news/2019/07/dutch-police-facial-recognition-database-includes-1-3-million-people/> accessed 28 October 2019
83. Desara Dushi, ‘The use of Facial Recognition Technology in EU law enforcement: Fundamental rights implications’ (2020, Global Campus South East Europe) https://repository.gchumanrights.org/bitstream/handle/20.500.11825/1625/1.GlobalCampus2020_SouthEast_Europe.pdf?sequence=1&isAllowed=y accessed 11 September 2020
84. Clare Garvie, Alvaro Bedoya and Jonathan Frankle, ‘The perpetual line-up’ (Georgetown law Center on Privacy & Technology, 18 October 2016) www.perpetuallineup.org accessed 26 January 2020
85. Patrick Grother, Mei Ngan and Kayee Hanaoka, ‘Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification’ (November 2018, NISTIR) <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf> accessed 01 December 2020
86. Philipp Grull, ‘Germany’s plans for automatic facial recognition meet fierce criticism’ (EURACTIV.de, 10 January 2020, Euractiv) <https://www.euractiv.com/section/data-

protection/news/german-ministers-plan-to-expand-automatic-facial-recognition-meets-fierce-criticism/> accessed 01 February 2020

87. Tom Jackman, 'Axon rolls out the next level of police technology: live-streaming body cameras' (Washington Post, 19 February 2020) <https://www.washingtonpost.com/crime-law/2020/02/19/axon-rolls-out-next-level-police-technology-live-streaming-body-cameras/> accessed 01 March 2020
88. Nicolas Kayser-Bril, 'At least 10 police forces use face recognition in the EU, AlgorithmWatch reveals' (AlgorithmWatch, 11 December 2019) <https://algorithmwatch.org/en/story/face-recognition-police-europe/> accessed 21 January 2020
89. Mehreen Khan, 'EU plans sweeping regulation of facial recognition' (Financial Times, 22 August 2019) <https://www.ft.com/content/90ce2dce-c413-11e9-a8e9-296ca66511c9> accessed 28 October 2019
90. Lily Kuo, 'The new normal: China's excessive coronavirus public monitoring could be here to stay' (09 March 2020, theGuardian) https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay accessed 10 October 2020.
91. 'Notting Hill Carnival Guide' (Time Out, 21 August 2019) <https://www.timeout.com/london/things-to-do/notting-hill-carnival-guide> accessed
92. 'Live facial recognition: introduction' (Big Brother Watch, May 2019) <https://bigbrotherwatch.org.uk/all-campaigns/face-off-campaign/#Intro> accessed 01 October 2019
93. Ursula von der Leyen, 'A union that strives for more: My agenda for Europe' (Political Guidelines for the next European Commission 2019-2024) <https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf> accessed 28 October 2019
94. Prod. Joyce Liu, 'In Your Face: China's all-seeing state', (BBC News, 10 December 2017), <https://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state> accessed 24 January 2020
95. Kenan Malik, 'As surveillance culture grows, can we even hope to escape its reach?' (19 May 2019, the Guardian) <https://www.theguardian.com/commentisfree/2019/may/19/as-surveillance-culture-grows-can-we-even-hope-to-escape-its-reach> accessed 28 October 2019

96. Toby Mendel, 'Freedom of Expression: a guide to the interpretation and meaning of Article 10 of the ECHR' (Council of Europe, 21 February 2017) <https://rm.coe.int/09000016806f5bb3> accessed 25 March 2020
97. Paul Mozur, 'One Month, 500,000 Face Scans: How China is using AI to Profile a Minority' (14 April 2019, New York Times) <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> accessed 27 October 2019
98. 'Polizei setzt immer mehr automatische Gesichtserkennung ein, Datenschützer besorgt' (21 March 2018, Heise online) <https://www.heise.de/newsticker/meldung/Polizei-setzt-immer-mehr-automatische-Gesichtserkennung-ein-Datenschuetzer-besorgt-4000106.html> accessed 25 January 2020
99. Luana Pascu, 'EU no longer considering facial recognition ban in public spaces' (Biometric Update, 30 January 2020) <https://www.biometricupdate.com/202001/eu-no-longer-considering-facial-recognition-ban-in-public-spaces> accessed 13 February 2020
100. Jonatan Ratcliffe, 'How many CCTV cameras are there in London 2019?' (19 May 2019, CCTV.co.uk) <https://www.cctv.co.uk/how-many-cctv-cameras-are-there-in-london/> accessed 27 October 2019
101. Ivana Roagna 'Protecting the right to respect for private and family life under the European Convention on Human Rights' (Council of Europe, 2012) <https://www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf> accessed 20 April 2020
102. Mark Schreiber, 'Facial recognition technology: what would George Orwell say?' (02 February 2019, thejapantimes) <https://www.japantimes.co.jp/news/2019/02/02/national/media-national/facial-recognition-technology-george-orwell-say/#.XbVjT5NKg6U> accessed 28 October 2019
103. Samuel Stolton, 'EU data watchdog to 'convince' Commission to ban automated recognition tech' (EURACTIV.com, 1 July 2020) https://www.euractiv.com/section/digital/news/eu-data-watchdog-argues-for-moratorium-on-recognition-technology/ accessed 10 October 2020
104. Treaty Office, 'Chart of signatories and ratifications of Treaty 005' (Council of Europe, 25 February 2020) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=16IBVmpg> accessed 25 February 2020

105. Daniel Saez Trigueros and Li Meng, 'Face Recognition: From Traditional to Deep Learning Methods' (arXiv, 31 October 2018) <https://arxiv.org/abs/1811.00116> accessed 12 November 2020

106. 'UK privacy activist to appeal after facial recognition case fails' (Aljazeera, 05 September 2019) <https://www.aljazeera.com/news/2019/09/uk-privacy-activist-appeal-facial-recognition-case-fails-190905142953617.html> accessed 01 October 2019

107. USLegal, 'Public Place Law and Legal Definition' https://definitions.uslegal.com/p/public-place/ accessed 28 April 2020

108. Mei Wang and Weihong Deng, 'Deep Face Recognition: A Survey' (arXiv, 18 April 2018) <https://arxiv.org/pdf/1804.06655.pdf> accessed 01 November 2020

109. William Webster, 'Video Surveillance: Practices and policies in Europe' (Amsterdam: IOS Press, 2012)