Facial Recognition Technology: Lawfulness of Processing under the GDPR in Employment, Digital Signage and Retail Context

University: Tilburg University
Master: Law & Technology
Author: Kübra Güven
ANR: 949443
Student number: 2005268
First supervisor: Dr B. Zhao
Second supervisor: Dr Emre Bayamlıoğlu

15 January 2019

Table of Contents

CHAPTER 1: INTRODUCTION

> *"The movements of expression in the face and body, whatever their origin may have been, are in themselves of much importance for our welfare. They serve as the first means of communication between the mother and her infant; she smiles approval, and thus encourages her child on the right path, or frowns disapproval. We readily perceive sympathy in others by their expression; our sufferings are thus mitigated and our pleasures increased, and mutual good feeling is thus strengthened. The movements of expression give vividness and energy to our spoken words. They reveal the thoughts and intentions of others more truly than do words, which may be falsified"*. [1] – Charles Darwin, 1872

1.1 Background

Imagine yourself buying your usual groceries in the supermarket, not using any bank card, but instead paying via a system that scans your face and connects it to your bank account. After the shopping, you would go to your home, where your face provides automatic access to the building and opens doors for you. Everything works perfectly until the doorbell rings, and you find a bunch of police officers waiting for you. They arrest you because your face has been falsely connected to an armed bank robbery.

This scenario is not mere fantasy. The unfortunate truth is that a similar but much more sinister scenario has already happened twice to a man named Steve Talley.[2] He was brutally beaten by the police while being arrested for armed bank robberies, and he spent months in jail. He finally got his life back on track after a public defender got him released. The wrongful charges were dismissed until he was arrested again based on another facial mismatch. Steve Talley faced serious psychological and physical consequences because his face was falsely matched to the face of an armed bank robber.

This example depicts the necessity of strengthening the regulatory approach to the use of facial recognition technology ("FRT"), as this technology is increasingly being integrated into our societies and lives. Its use can be biased and inaccurate,[3] and false matches can have life-changing consequences, as proven by the story of Steve Talley.

[1] Charles Darwin, '*The expression of the emotions in man and animals*', (1872), p. 384

[2] Ava Kofman, '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 1 January 2019

[3] Katharine Schwab, 'Facial Recognition Systems Are Even More Biased Than We Thought' (*Fast Company*, 13 February 2018) , https://www.fastcompany.com/90160327/facial-recognition-systems-are-way-more-biased-that-we-thought ; Don Reisinger, (*Fortune*, 26 July 26 2018), 'Amazon's Facial Recognition Linked the Faces of 28 Members of Congress to Mugshots' http://fortune.com/2018/07/26/amazon-facial-recognition-mugshots/ Accessed 1 January 2019

We can assume that law enforcement departments are collecting and using facial data, and in this context the legal grounds would revolve around public security. However, closed-circuit television ("CCTV") systems are not always government-owned. This means that data is being collected by private entities motivated by an economic interest in selling information to governments. The question here is, how trustworthy are these private entities, and how can we know they are not selling this data for other purposes? An example of the risk of data breaches can be found in the events of the Cambridge Analytica scandal.[4] In this case, the most obvious purpose for collecting personal data would be commercial purposes, which brings us to the difficult issue of advertisement companies collecting data for monetisation. This topic will be tackled more in depth in the discussions below.

Many mobile phone applications use FRT for customer verification. For example, Master Card is preparing to launch a FRT payment app in Australia.[5] As part of the contract terms, all customers will give their biometric data and the legal ground for the collection would therefore be contractual. However, what if the owner of this data sells this sensitive personal data to another company, such as an advertising company? Alternatively, what if law enforcement requests this data from a private entity? In this case, the consent of the customer was given for one specific purpose – the use of the application. Therefore, if a transfer of this information happens, it will be an unlawful transfer because the customer's consent for one specific purpose is being abused. In this case, what are the safeguards to protect the citizens from this risk? In the state-of-the-art, we would not even know of unlawful transfers of personal data.

The root of all these issues lies in the slow pace of law making, compared to the development of technologies. In the United States, the National Telecommunication and Information Administration tried to create a code of conduct with all the industry representatives and privacy advocates in 2013.[6] This code of conduct was supposed to be the go-to guide for companies using FRT. However, after 16 months, privacy advocates declared their withdrawal from the negotiations.[7] Their concerns were about the privacy rights of individuals, and one of the primary characteristics of FRT is the loss and violation of privacy. These automated systems do not give any freedom of choice to their consumers. According

[4] Alex Hern and David Pegg, 'Facebook fined for data breaches in Cambridge Analytica scandal ' (*The Guardian*, 11 July 2018) < https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal> Accessed 1 January 2019

[5] Justin Lee, 'MasterCard to launch facial recognition payment app in Australia'(*Biometric Update*, 9 February 2017) <http://www.biometricupdate.com/201702/mastercard-to-launch-facial-recognition-payment-app-in-australia> Accessed 1 January 2019

[6] National Telecommunications and Information Administration, 'Privacy Multi-stakeholder Process: FRT' United States Department of Commerce Publication, (17 June 2016) <https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology > Accessed 1 January 2019

[7] Justin Brookman , 'CDT Withdraws from the NTIA Facial Recognition Process' (*CDT*, 16 June 2015) <https://cdt.org/blog/cdt-withdraws-from-the-ntia-facial-recognition-process/ > Accessed 1 January 2019

to privacy advocates, to uphold the right to privacy, people should be able to control who has access to their sensitive data and how this data will be stored or shared.[8] In this case, the data is created based on personal characteristics. The user or customer can change their password or even their name, but facial data cannot be easily changed.

As a result, facial data has more value than other biometric data. At the same time, it is one of the least protected forms of data and subject to unrestricted collection. Privacy advocates argue that the facial recognition should only be available with a consumer's permission. However, industry stakeholders were not able to agree on this topic.[9] In reality, companies never needed to ask permission for collecting facial data. Negotiations continued for 16 months, but no progress was made on the consumer's right to privacy. In the current situation, people cannot walk down a public street without fear of being tracked by companies.

There are numerous ethical and moral issues with private companies collecting and monetising facial data. It is argued that our privacy needs to be respected and our faces should not become mere means to make us recognisable to advertisers. In addition, FRT is at the centre of a full data ecosystem comprised of multiple entities collecting facial data to sell to advertisers, which increases the risk of cybercrimes and data breaches. One example could be data about skin tone or the earlobes, which are recognised by the technology and then sold to cosmetic and beauty companies for advertisement purposes. This leaves the data of individuals scattered among many privately owned databases. When security breaches happen, facial data can be leaked to other parties who abuse data for illegitimate purposes like identity theft. This leaves individuals vulnerable to cybersecurity risks such as identity theft, fraud, and blackmail.

It appears that biometric data is clearly sensitive data, and facial data is a branch of that sensitive data. In the data protection framework, all the measures and risks are the object of a higher degree of protection. The regulation of biometric data and its collection and use are increasingly of vital importance. Considering the vast scope of facial recognition and its potential to continue developing, the state-of-the-art makes it clear that we should specifically regulate the use of FRT. Private companies should not be able to gather the most sensitive and valuable of our personal data.

For all these reasons, it becomes imperative to strengthen the data protection approach for the use of facial recognition technology in the commercial context and return the control of facial data to individuals.

[8] Privacy advocates statement on NTIA facial recognition process , (16 June 2015) Available at <https://www.dropbox.com/s/g7cdhl66p5um7dn/Privacy%20advocates%20statement%20on%20NTIA%20facial%20recognition%20process%20-%20FINAL.pdf?dl=0> Accessed 1 January 2019

[9] Lauren C.Williams, 'Facial Recognition Is the New Normal, Even When Your Face is Covered'(*Think Progress*, 23 June 2015) https://thinkprogress.org/facial-recognition-is-the-new-normal-even-when-your-face-is-covered-5a4d6e78cc54/ Accessed 1 January 2019

1.2 Problem Statement

The focus of this thesis is to assess the lawfulness of processing facial data when it is used with FRT for the purpose of categorisation under the General Data Protection Regulation 2016/679 (“GDPR”). The different regulatory approaches of the GDPR for three different contexts and the related privacy concerns will be analysed.

The Article 29 Data Protection Working Party (“the Article 29 WP”) in its Opinion 03/2012 emphasizes that “biometrics allow for automated tracking, tracing or profiling of persons and as such their potential impact on the privacy and the right to data protection of individuals is high”.[10] It is necessary to elaborate and underline that FRT is being integrated into online and mobile services and used for identification, authentication/verification, and categorisation of human beings. When the face of an individual is captured, with or without their awareness, this data is transmitted to a server for further processing. However, facial data is dissimilar to other biometric data types in that the face reveals further information about an individual. Human faces can be used to obtain information about ethical origin, religion, or health.[11] The Article 29 WP stresses that this type of information must be considered a special category of personal data that requires higher protection.[12]

Additionally, The Article 29 WP provides “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”.[13] According to the guideline, profiling is done when your personal aspects are being evaluated in order to make predictions about you, even if no decision is taken. For example, if a company or organisation assesses your characteristics (such as your age, sex, height) or classifies you in a category, this means you are being profiled.[14] This definition of profiling means that when a CCTV uses FRT and recognises an individual’s face, three facts come into play: that individuals can be a target without realizing that the technology is being used, that their face may reveal further information about themselves, and lastly, that individuals can be a target of profiling.

With this legal basis, the problem about FRT is that this technology is gathering information about individuals. There are specific requirements (in the GDPR) needed for lawful processing,[15] and these do not apply to how FRT collects data.

[10] Article 29 Data Protection Working Party, ‘Opinion 03/2012 Developments in biometric technologies’, p.3.

[11] Article 29 Data Protection Working Party, ‘Opinion 02/2012 on Facial recognition in online and mobile services’, p.4.

[12] Ibid., p.5.

[13] Article 29 Data Protection Working Party, ‘Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679’

[14] Ibid., p.7.

[15] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (27 April 2016), Art. 6 Lawfulness of processing.

Privacy and data protection concerns derive from the fact that facial detection and recognition software is increasingly being integrated into digital systems equipped with some type of video sensors, often used in modern cities. This leads to a declining amount of privacy in public, including the workplace, retail stores, and public spaces like railway stations, stadium, and schools.

Digital displays and screens ("digital signage") equipped with video sensors and video surveillance systems, also known as CCTV, are slowly colonising every space, private and public. The core of privacy concerns associated with these systems resides in the fear that we will soon be unable to walk, work, or pursue private activities without being identified and profiled, and having our facial data collected by unknown data controllers and/or processors.

1.3 Central Research Question and Sub-Questions

While FRT is increasingly used and is gaining a hegemonic status for identification purposes, it is a relatively deregulated field, which has led to a variety of fragmented privacy practices and policies. Various legal grounds can form the basis of facial recognition as a means of categorisation in the contexts of employment, digital signage, and the retail sector. Therefore, it is necessary to assess the way that the GDPR allows such data collection and uses and how its regulatory approach is shaped in these three contexts.

Central Research Question:

Are the GDPR's legal grounds suited for facial recognition technologies, and what are the GDPR's various regulatory approaches to tackle facial recognition as a means of categorization in the contexts of employment, digital signage, and retail?

Sub-questions:

1. What is FRT? How does facial recognition work as a means of categorisation and what risks are there in these common use-cases?
2. What are the legal grounds under the GDPR when FRT is used in the employment, digital signage, or retail contexts?
3. What are the GDPR's various regulatory approaches to tackle facial recognition as a means of categorization in the contexts of employment, digital signage, and retail?

1.4 Significance

Three scenarios have been chosen for this thesis, because of their prevalence in the private sector. Also, when using FRT in a commercial context, the applicability of legal grounds under the GDPR can be considered a grey area. The use of FRT in employment context is an area where clearer boundaries are determined. Comparing these contexts will be informative to establish how facial data can be better protected in the commercial context.

FRT in digital signage is already widely used and the market is expected to continue to grow fast. Many people don’t know that digital signage can include FRT and it might conflict with their privacy expectations. In this context some of the problems include that it’s impractical for data controllers to ask consent and it’s a very public use case of FRT. FRT in retail stores shares the same problems, but the use is more focused on profiling the customers and their preferences.

The benefits of choosing these three contexts come from the fact that FRT is an emerging technology and it is important to know how it challenges the rules of the GDPR by its features and how the GDPR is applied in these three contexts. Comparing different contexts shows where the boundaries are, and why the boundaries can be different for employers compared to companies as well as the level of protection can be different for employees compared to customers. This will also show how the emergence of FRT is changing people’s expectations of privacy in retail stores and in public places with digital signage. Lastly, FRT is approaching workplaces and companies are getting more interested in monitoring their employees and their working environment as FRT is offering economic benefits for its users.

1.5 Research Methodology and Limitations

This analysis will focus on doctrinal legal research to address the research questions.[16] The thesis will investigate developments in the field of facial recognition technology, use of this technology for categorization purposes of individuals, and the possible misuses enabled by this technology. A critical viewpoint will be taken regarding the general risks and privacy risks that FRT has created. The legal research will examine the legal framework of European Data Protection, focusing on the most relevant legal instruments. The main focus of this thesis is to provide a thorough analysis of the General Data Protection Regulation 2016/679 and the Article 29 WP opinions.

To clarify the legal status of the Article 29 WP opinions and their influence in legal practice: The Article 29 WP is assembled under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.[17] The Article 29 WP has 28 members and consists of one regulator from each EU Member State and one member from The European Commission as a representative. The Article 29 WP is an independent European advisory body and they examine data protection and privacy related matters. The Article 29 WP publishes materials in their website, such as opinions, working documents, letters. It is important to note that these materials reflect the view of Article 29 WP, and not the view of European Commission. The Article 29 WP opinions are non-binding materials, however, it provides guidance, which carries legal weight for data protection and privacy

[16] Kharel, Amrit, “Doctrinal legal research is analytical study of existing laws, related cases and authoritative materials as a whole, on some specific matter.”, (*Doctrinal Legal Research*, 26 February 2018). Available at SSRN: <https://ssrn.com/abstract=3130525 or http://dx.doi.org/10.2139/ssrn.3130525>, p. 4.

[17] As explained in the first page of Article 29 WP opinions.

practitioners. These opinions are taken into consideration by the EU courts and Data Protection Authorities. Lastly, when the GDPR came into force, the Article 29 WP became European Data Protection Board which has increased legal powers on data protection and privacy related matters.

Relevant literature, such as news articles, academic and journal articles, decisions, case-law, recommendations, the Article 29 WP's advisory opinions, websites, blog posts, reports, and books will be examined to reveal the state of the technology and its problematic uses, as well as data protection risks and issues of FRT when it is used in the employment, digital signage, and retail contexts. The doctrinal legal research will be used to gather relevant facts, to identify and analyse legal issues and risks, to find and analyse case law, and to arrive at a conclusion based on an analysis of the main issues found during the research.[18]

It should be noted that other laws and regulations than GDPR are also applicable to FRT such as contract law, e-commerce law, employment law, and so on. These other laws are not included within this scope of the discussion.

1.6 Overview of Chapters

Chapter 2 explores the history and development of FRT by using a few examples from the state-of-the-art and illustrates the step-by-step process of facial data gathering. Chapter 2 will lay out the biometric characteristics of facial data and elaborates on how FRT is used as a means of categorisation as well as the risks associated with FRT. In addition, FRT in employment, digital signage, and retail contexts will be introduced. Chapter 3 will focus on examining the legal grounds under the GDPR for FRT in these common use-cases. Chapter 3 will also include analysis and reflections of the GDPR's regulatory approach for the analysed cases. Chapter 4 will be the conclusion, in which the research is summarised and the conclusions and answers to the research questions will be presented.

[18] Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' (*Deakin Law Review*, 2012) 17(1), p. 83-119.

CHAPTER 2: WHAT IS FACIAL RECOGNITION TECHNOLOGY?

This chapter aims to describe the relevant aspects of FRT and to explain "How does facial recognition work as a means of categorisation and what risks are there in these common use-cases?" This chapter explains the origins, history, and development of FRT. This chapter also showcases how some of the currently most advanced FRT systems work. Third, this chapter highlights the biometric characteristics of the related data and the privacy risks that come with processing biometric data. Facial recognition technology as a means of categorisation is closely examined and general risks of the use of FRT are described.

2.1 Origins and Development of Facial Recognition Technology

The Handbook of Face Recognition by Stan Z. Li and Anil K. Jain explains how technological development has enabled FRT to develop:

> Wide availability of powerful and low-cost desktop and embedded computing systems has created an enormous interest in automatic processing of digital images and video in a number of applications, including biometric authentication, surveillance, human-computer interaction, and multimedia management. Research and development in automatic face recognition follow naturally.[19]

The work of Stan Z. Li and Anil K. Jain provides insight into the origins of FRT and how it was achieved, and how it has developed. The development has taken almost 60 years, as the development of advanced computing was a precondition for FRT. Thus, the history of FRT is as old a vision as the computer.[20] Even though there are other types of biometric data, facial data has a special importance. One of the reasons for this is that facial recognition is the primary method of personal identification for humans.[21]

Many would point to Woodrow Wilson Bledsoe as the pioneer of FRT because of his contributions to artificial intelligence and pattern recognition.[22] Bledsoe published a report called *A Facial Recognition Project* in January 1963. He established a system that could distribute photos of faces by manual use of a tablet and called it RAND.[23] This system was able to record the geo-coordinates of different facial features including the inside corner of the eyes, the nose, the hairline, and the mouth. This data could be added to a database. Even

[19] Huang, T., Xiong, Z., & Zhang, Z, 'Face recognition applications. Handbook of Face Recognition' (2011) <https://doi.org/10.1007/978-0-85729-932-1> p. 617-638

[20] Ibid.

[21] O'Connor, Sean, 'Biometrics and Identification after 9/11' (2002) SSRN Electronic Journal. 10.2139/ssrn.299950.

[22] Alex Pentland and Tanzeem Choudhury, 'Personalizing Smart Environments : Face Recognition for Human Interaction'(8 October 1999), Available online: <http://hd.media.mit.edu/tech-reports/TR-516.pdf > Accessed 1 January 2019

[23] Woodrow Wilson Bledsoe, 'A Facial Recognition Project Report', (January 1963), Available online: <https://archive.org/details/firstfacialrecognitionresearch> Accessed 1 January 2019

though the technology was only able to find similar pictures from the database, it was an essential first step for FRT.

In 1973, Takeo Kanade of Kyoto University, Japan published his PhD thesis[24] and outlined one of the earliest face recognition technologies.[25] Although Kanade's achievement was radical for the technology, it did not take off. In the 1970s, Goldstein, Harmon, and Lesk were able to improve the efficiency of the manual face recognition system. They used 21 specific individual markers as well as lip thickness and hair colour to identify faces automatically.[26] However, even with Bledsoe's system, the biometrics still needed to be computed manually.

In 1988, Sirovich and Kirby began to apply linear algebra to the problem of facial recognition, which later became known as the Eigenface approach.[27] The Eigenface approach began as an examination of the low-dimensional portrayal of facial images. Sirovic and Kirby were able to display their feature analysis on an assemblage of facial images that could be designed using a blend of essential features.[28]

Kanade, Turk, and Pentland broadened the Eigenface approach by exploring how to catch faces within images.[29] A method of distinguishing faces from crowded environments was presented by Matthew Turk and Alex Pentland in 1991[30]. This was the beginning of real-time facial identification and led to the first occurrence of automatic face recognition. In the same year, the National Institute of Standards and Technology[31] and The Defence Advanced

[24] Takeo Kanade, (23 May 1974), 'Picture processing system by computer complex and recognition of human faces' Available online: <https://repository.kulib.kyoto-u.ac.jp/dspace/bitstream/2433/162079/2/D_Kanade_Takeo.pdf > Accessed 1 January 2019

[25] Yana Welinder, (Santa Clara High Technology Law Journal , 2013) 'Facing Real-Time Identification in Mobile Apps &amp: Wearable Computers' page. 94 Available online: <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1577&context=chtlj > Accessed 1 January 2019

[26] Alex Pentland and Tanzeem Choudhury, (8 October 1999), 'Personalizing Smart Environments : Face Recognition for Human Interaction' Available online: <http://hd.media.mit.edu/tech-reports/TR-516.pdf > Accessed 1 January 2019

[27] Ibid.

[28] Ibid.

[29] M Turk, 'A Random Walk through Eigenspace' [2001] IEICE Transactions on Information and Systems.Available online: < http://cs.ucsb.edu/~mturk/pubs/TurkIEICE2001.pdf > Accessed 1 January 2019

[30] Yana Welinder, (Santa Clara High Technology Law Journal , 2013) 'Facing Real-Time Identification in Mobile Apps &amp: Wearable Computers' page. 94 Available online: <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1577&context=chtlj > Accessed 1 January 2019

[31] Official website of the National Institute of Standards and Technology, Available online:< https://www.nist.gov/> Accessed 1 January 2019

Research Projects Agency (DARPA)[32] presented a FRT called FERET, and use the program started in 1993.[33] The primary purpose of the project was to create a database of facial images. The underlying purpose was to encourage the use of this technology in the private market – more specifically, the commercial facial recognition market.

In 2000, the National Institute of Standards and Technology (NIST) created the Face Recognition Vendor Test (FRTV),[34] which was constructed to provide independent government evaluations of facial recognition systems. The reason for the FRTC was to create commercially available prototype technologies. After 2010, Facebook started to include FRT as a function that helped to identify people.[35] On a daily basis, "more than 350 million photos are uploaded" to Facebook, [36] which are tagged using a face recognition system. Today's face recognition methods commonly start with an examination of "training images" of previously known persons to measure their facial characteristics.[37] These measurements are collected in a database. After this collection, the FRT can use this data to recognise that face in new photos. People can upload new pictures to the database, and the facial recognition system will be able to recognise that individual.[38]

2.2 Facial Recognition Systems

One of the most basic features of humankind is recognising each other by our faces. The idea of "face recognition by computer" has always been a subject of interest for scientists and researchers.[39] With FRT, computers are now able to identify people from their faces. A system called "DeepFace" has filled the majority of the gaps in the most popular criterion in unconstrained face recognition. With all of its recent developments, FRT is now at the border

[32] Official website of Defense Advanced Research Projects Agency, Available online:< https://www.darpa.mil/> Accessed 1 January 2019

[33] Face Recognition Technology (FERET) Explanation of the project, Available online : <https://www.nist.gov/programs-projects/face-recognition-technology-feret> Accessed 19 November 2018

[34] Face Recognition Vendor Test (FRVT) Explanation of the project, available online : < https://www.nist.gov/itl/iad/image-group/feret-face-recognition-technology-documents> Accessed 1 January 2019

[35] Nicholas Jackson, (The Atlantic, 16 December 2010), 'Facebook Will Start Using Facial Recognition Next Week' Available online: < https://www.theatlantic.com/technology/archive/2010/12/facebook-will-start-using-facial-recognition-next-week/68121/> Accessed 1 January 2019

[36] Internet.org. 'A focus on efficiency: A whitepaper from Facebook, Ericsson and Qualcomm' (13 September 2013.). Retrieved May 20, 2015 Available online:< https://www.parool.nl/rest/content/assets/1368f07e-16b8-415d-bd3a-a4046f2fa9bd > p.7 Accessed 19 November 2018

[37] Yana Welinder, 'Facing Real-Time Identification In Mobile Apps & Wearable Computers'.Available online :< https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=https://www.google.nl/&httpsredir=1&article=1577&context=chtlj > Accessed 1 January 2019

[38] Ibid.

[39] Alex Pentland and Tanzeem Choudhury, 'Personalizing Smart Environments: Face Recognition for Human Interaction' Available online: <http://hd.media.mit.edu/tech-reports/TR-516.pdf > Accessed 1 January 2019

of human-level efficiency. The DeepFace system is trained to divide large datasets of faces acquired from a community, and it can exceed the existing system with only minimal adaptation.

Additionally, the system has the capability of producing extremely compact facial representations. With social media applications and websites, enormous numbers of photos have been uploaded to databases. This data has been collected by search engines, and consists of a variety of material such as photos and videos that contain facial data. The massive amount of data and constantly increasing resources have empowered the use of more capable statistic models, which have improved the stability and power of computer recognition systems.

To explain in a more detailed manner, there is more than one way of recognising the face of a person using FRT. This recognition can be made through a picture, a video, or directly from a camera. The steps may vary depending on the way the system is being used, but generally in modern FRT, the sub-process consists of four stages.[40]

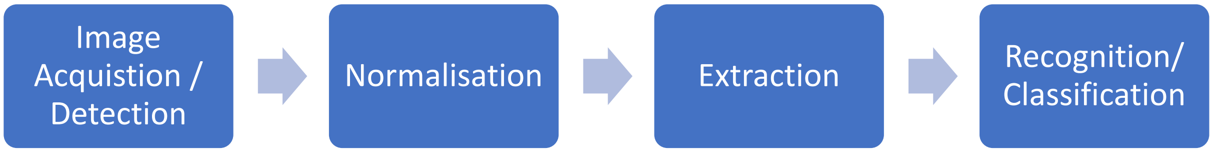

Figure 1 Steps of facial recognition

Processing or capturing the face of a person and then converting it to a digital form is called the image acquisition step.[41] After the image acquisition step, the presence of a face is detected. In the face detection step, the image is processed, and the face is highlighted. After the detection of the face, marker spots are normalised. The normalisation of the picture might include rotating or arranging the colour classification.[42] In the next step, the detected face will be isolated and turned into distinctive data from the digital image that represents an individual. In the extraction phase, groups of facial features are collected in a reference template for other comparisons in the future. If the capturing process is the first time that the system "sees" a person, their data is enrolled in the database.[43] In the last step, the captured human face will be compared to the existing database in search of a match to identify the

[40] Yaniv Taigman and others, 'DeepFace: Closing the Gap to Human-Level Performance in Face Verification'.Available online : <https://www.cs.toronto.edu/~ranzato/publications/taigman_cvpr14.pdf > Accessed 1 January 2019

[41] Selvapriya.M , Dr.J.KomalaLakshmi, (International Journal Of Engineering And Computer Science, Volume 3 Issue 12 December 2014) Available online : <https://www.ijecs.in/index.php/ijecs/article/download/1662/1538/> Accessed 1 January 2019

[42] Ibid., p.4.

[43] Article 29 Data Protection Working Party, ' Opinion 02/2012 on Facial Recognition in Online and Mobile Services' , p. 2.

individual. Another purpose of comparing the face is the categorisation of the person based on their gender, age, and mood.[44]

2.3 Biometric Characteristics of Facial Data

The use of human characteristics with the purpose of identification is increasing every day. This raises privacy concerns about the protection of the data, as it is biometric data and requires a high level of protection. As mentioned above, the Article 29 WP in Opinion 03/2012 indicates that biometric data "allows for automated tracking, tracing or profiling of persons and as such their potential impact on the privacy and the right to data protection of individuals is high".[45]

There are physical and physiological features of persons that are consistent in facial data. The face has certain physical characteristics. With facial expression analysis, the technology is available for analysing these physical characteristics.[46] The uniqueness of the face is not replicable, and specific images can contain sensitive information, especially if the face image allows the person to be identified. Because of this sensitivity, there should be privacy-preserving techniques to protect the faces of individuals.

The face or a digital image of a person can be considered a special category of personal data. Especially if the detection of the face is used in further processing such as facial expression analysis, this data must be considered sensitive data.[47]. Thus, FRT is a way to collect both sensitive and biometric data. Lastly, the risks that are derived from the process of FRT relate to the type of processing used. Facial recognition should not be involved in unlawful processing. Because of this, the lawful grounds must be determined within the regulations. All of the faces that have been collected through CCTVs end up in a database, and each face is captured from many different angles. This database provides many opportunities for tracking, categorising, profiling, or tracing. Thus, the potential threat to privacy and the right to data protection require safeguards.

[44] Article 29 Data Protection Working Party, 'Opinion 02/2012 on Facial Recognition in Online and Mobile Services', p.2.

[45] Article 29 Data Protection Working Party, 'Opinion 03/2012 Developments in Biometric Technologies', p.3.

[46] Jang, E. H., Park, B. J., Park, M. S., Kim, S. H., & Sohn, J. H. (2015). Analysis of physiological signals for recognition of boredom, pain, and surprise emotions. Journal of physiological anthropology, 34(1), 25. Available online: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4490654/ > Accessed 1 January 2019

[47] Article 29 Data Protection Working Party, 'Opinion 02/2012 on Facial Recognition in Online and Mobile Services' , p. 4.

2.4 Facial Recognition Technology as a Means of Categorisation

Facial recognition technology is used by many different actors in many different ways and for different purposes.[48] One of these purposes is FRT as a means of categorisation, which is the focus of the legal analysis in this thesis. Biometric categorisation has explained in the Article 29 WP opinion on developments in biometric technologies as:

> The categorisation of an individual by a biometric system is typically the process of establishing whether the biometric data of an individual belongs to a group with some predefined characteristic in order to take a specific action. In this case, it is not important to identify or verify the individual but to assign him/her automatically to a certain category. For instance, an advertising display may show different adverts depending on the individual that is looking at it based on the age or gender.[49]

As we can see, categorisation means that facial data is detected and assigned to a category with pre-defined criteria, such as age, gender, or even mood.[50] It is important to stress that it is not necessary to have an enrolment process for categorisation purposes.[51] This means that the technology does not require the input of biometric data, so it can be used on a mass of people, as the technology has the ability to capture data automatically.

As explained above, the processing of biometric data involves three different processes: enrolment, storage, and matching.[52] The first contact of a biometric system with a person initiates the enrolment phase.[53] This allows the biometric system to extract biometric data from an individual, and the system links this data to that person. In most cases, the enrolment phase requires interaction with a person, for example, fingerprinting. This interaction requirement provides an opportunity for an individual to have a fair notification of processing.[54] However, if biometric data is extracted from a CCTV with facial recognition functionality, then it is possible to enrol an individual's facial data without their knowledge or consent.[55]

[48] Article 29 Data Protection Working Party, 'Opinion 02/2012 on Facial recognition in online and mobile services', p.2

[49] Article 29 Data Protection Working Party 'Opinion 3/2012 On Developments in Biometric Technologies', p. 6.

[50] Article 29 Data Protection Working Party,Opinion 02/2012 on Facial Recognition in Online and Mobile Services', p.2

[51] Article 29 Data Protection Working Party 'Opinion 3/2012 on developments in Biometric Technologies', p 5.

[52] Ibid.

[53] Ibid.

[54] Ibid.

[55] Ibid.

After all this processing, an entire personalised profile of a person can be created by FRT software and stored in databases. This could be used against these individuals.[56] Profiling in commercial use is an outcome of FRT as a means of categorisation. This can have a negative impact on people's lives and can cause misinterpretations of the person due to biased categorisations. Concordantly, it is a common practice that people are denied a service based on face discrimination as customers that are enrolled in different databases.[57]

2.5 Risks of the Use of Facial Recognition Technology

There might not be any problems when FRT is used to scan the face of a single person. However, this one piece of information can have a more significant impact when it comes together with a massive amount of other relevant information. In an article about profiling, M. Hildebrand says that "profiling is not about data but about knowledge", and introduces a new concept of inductive knowledge, defined as "correlations between data in databases that can be used to identify and represent a human and non-human subject […] or the applications of the profiles to individuate and represent a subject or to identify a subject as a member of a group or category". [58] Such correlations may not seem like anything to the data subject, even though the processing might continue without their consent.

In his paper *Taxonomy of Privacy*, Daniel J. Solove explains about data aggregation and creation of profiles. An example of this could be when a face is combined with a database for categorisation purposes, and an individual profile is then created to match the face. In other words, "the whole may become greater than the parts".[59] In this way, information that cannot be derived from a single face may be revealed by analysing a massive amount of facial data from many individuals. Thus, when FRT is used for categorizing people, this analysis will provide a way of profiling people according to their mood, behaviours, and interests. Solove indicates that once a profile has been created for a person through their data, it is likely to be used against that person.[60] Aggregation can increase the "power" that data collectors have over the people who have been profiled. Individuals might not know that they

[56] Lewinski Peter and others, 'Face and Emotion Recognition on Commercial Property under EU Data Protection.' Psychology & Marketing, Wiley Periodicals 729-746. Available at, https://onlinelibrary.wiley.com/doi/abs/10.1002/mar.20913 - accessed 18 November 2018

[57] Mathew Wall, 'Is facial recognition tech really a threat to privacy?' (*BBC Technology*, 19 June 2015) Available at, https://www.bbc.com/news/technology-33199275 Accessed 1 January 2019

[58] Hildebrand M, 'Profiling from data to knowledge the challenges of a crucial technology [2006] 30(9) Datenschutz und Datensinchercheit. Available at <https://pdfs.semanticscholar.org/c0a1/aa843e812925127dfb8f9540089e1a0a72b5.pdf>, p.1, Accessed 1 January 2019

[59] Solove Daniel, 'A Taxonomy Of Privacy' [2006] 154(3) University of Pennsylvania Law Review Available at<https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf> p. 506 Accessed 1 January 2019

[60]Ibid., p. 507

are involved in profiling. Nor do they always understand what is involved and what the consequences of this process are.[61]

Profiling of individuals can have critical impacts on their lives when they are treated differently or with bias, especially in legal situations. Furthermore, the extracted facial data can be given or stolen for abuse or misuse.

Installing surveillance systems inside a company office might create profiling risks for employees if a CCTV camera is using FRT to collect biometric characteristics of the employees. The most relevant applicable case is in the employment context: the performance assessment of an employee can be predicted by FRT. This type of an activity would allow profiling by the employer, and this type of a profiling can affect an employee's working life and cause him/her to be fired.

The use of FRT in the commercial field is likely to lead to profiling of customers by their preferences and behaviour while shopping. Automated facial recognition systems will analyse "shopping experiences to track the routes and habits of the customers, and along with this particular ability also emerges the capability of profiling to deliver targeted advertising to the customers".[62] Furthermore, the profile of the customer can be connected to their social networking profiles such as Facebook and Instagram to allow more detailed analysis of patterns. With this final touch, all types of different information and even the tiniest details about the individual come together. This creates an individually detailed image of a person and their tastes, friendships, reactions, and habits.[63]

An example of the risk of profiling for customers are highlighted in the paper, "A Review of the Data Broker Industry", in which a data broker sells the profiles of consumers to financial companies.[64] The paper indicates that the consumer does not have any knowledge about this purchase, nor have they given any permission. The profiles of the customers are categorised by titles such as "rural and barely making it", "ethnic second-city strugglers", and "tough start: young single parents". The data also carries a scoring system evaluating subjects'

[61] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016\679, p.5

[62] Article 29 Data Protection Working Party, Opinion 3/2012 on developments in Biometric Technologies, p. 23

[63] Mathew Wall, 'Is facial recognition tech really a threat to privacy?' (BBC Technology, 19 June 2015) Available at, https://www.bbc.com/news/technology-33199275 Accessed 1 January 2019

[64] United States Senate, Committee on Commerce, Science, and Transportation. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller, December 18, 2013. Available at < https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf > Page ii of the Executive Summary and 12 of the main body of the document. – Accessed 1 January 2019

financial vulnerability.[65] This kind of unknown processing and the resulting categorisation leads to questions such as how this type of processing can be transparent or in the knowledge of the individual. To identify people like this without their informed consent may raise privacy concerns and risks.

In the commercial field use, with facial images collected in a non-consensual way and shared after profiling with others for further use, or even images collected with consent but repurposed, for example, sold to interested third parties, such as insurance companies.[66]

The private sector is using FRT to gather as much as information as possible in order to acquire customers and maximise their profits. Biometric characteristics are strongly connected to an individual as they carry that person's unique identifiers.[67] A facial recognition system is different and riskier than other biometric systems because the enrolment stage of the collection of other types of biometric data requires human interaction in order to extract the data, but FRT can perform the extraction mostly without the data subject's knowledge.[68] This means that the data subject's expectation of privacy, in many relevant occasions, especially the three to be discussed below, that the data subject has is higher, which makes FRT more intrusive to personal privacy than other biometric systems.

We are increasingly surrounded by cameras and being anonymous while walking in public has already become a privilege. This situation could be acceptable for the sake of public security. However, what started with recognising individuals in public for detecting criminals has reached the point where it does not uphold sufficient privacy for the general public. First, the most unique part of our body has been made a template and held in millions of databases, without us knowing who has it or for what reason. This intrusion is continuing to advance deeper as it tries to analyse characteristics and emotions for categorisation purposes.

In order to demonstrate the common use-cases of FRT as a means of categorisation, the use of this technology will be introduced in the employment, digital signage, and retail contexts.

2.6 Common Use-Cases of Facial Recognition Technology as a Means of Categorisation

The Article WP29 opinion on developments in biometric technologies states that many biometric technologies "allow for automated tracking, tracing or profiling of persons, and as such their potential impact on the privacy and right to data protection of individuals is

[65] Ibid.

[66] David Fulton, (Information- Age, 11 May 2018) 'How facial recognition could save insurance companies billions' Available online: < https://www.information-age.com/how-facial-recognition-could-save-insurance-companies-billions-123472478/ > Accessed 1 January 2019

[67] Article 29 Data Protection Working Party, Opinion 3/2012 on developments in Biometric Technologies, p. 2

[68] Ibid., p.5.

high".[69] The data that is collected by FRT can be used to derive profiles.[70] Data subjects should be able to access their profiles generated by FRT.[71] The problem with FRT profiling is its impact on the privacy and data protection of individuals, especially in these three contexts explained below.

2.6.1 Facial Recognition Technology in the Employment Context

Facial recognition for categorisation purposes could be used in the employment context. Its use in the workplace might create negative consequences for an employee:

> With the capabilities given by video analytics, it is possible for an employer to monitor the worker's facial expressions by automated means, to identify deviations from predefined movement patterns (e.g. factory context), and more.[72]

For example, a company might use a CCTV surveillance system by which movements of employees are detected in order to provide employee data to the company's Human Resources ("HR") department. The cameras are used to share images of employees with a facial recognition system that predicts the likely age, gender, and mood of the employees for the company's database. Data from FRT and other multimodal factors can change the way the employee works to improve employee productivity by reflecting the employee's predicted profile.[73] The HR department could use FRT to assess the performance or suitability of an employee by categorising the mood of the employee. Imagine a hotel receptionist whose job description is to be welcoming, happy, hospitable, and enthusiastic towards customers. The HR department would be interested in assessing the suitability of the receptionist by assessing the moods and reactions of the receptionist and their customers. If the employee's mood is categorised as angry or irritated when interacting with customers, or if the customer's mood is negative after the interaction, this would signal poor performance and unsuitability of the employee for the job. This could lead to decisions negatively affecting the situation of the employee.

Such a scenario is especially problematic because the accuracy of FRT cannot be completely guaranteed.[74] In companies where such systems would be used, the employee would be at constant risk of the FRT making incorrect categorisations of the employee's mood. Instances like this should always be safeguarded by human supervision to prevent automated decisions

[69] Ibid. p 3

[70] Article 29 Data Protection Working Party, Opinion 3/2012 on developments in Biometric Technologies, p.10

[71] Article 29 Data Protection Working Party, Opinion 3/2012 on Developments in Biometric Technologies, p.14

[72] Article 29 Data Protection Working Party, Opinion 2/2017 On Data Processing at Work, p. 19

[73] Yasin Yilmaz, Alfred O. Hero (3 August 2015) "Multimodal factors enable a powerful means of clustering based on a diverse set of observations.", https://arxiv.org/abs/1508.00408 Accessed 1 January 2019

[74] Article 29 Data Protection Working Party, Opinion 3/2012 on developments in Biometric Technologies, p.18

concerning individuals from being made based purely on profiles derived from the data collected by FRT.[75]

Employee-monitoring software is becoming more common. One such software is produced by Resolution View, a software company that provides software for tracking employees' working hours. What makes this software different from other working hour trackers is that this software uses facial recognition technology to track the number of hours the employees are working.[76] Resolution view timeclock software combines video analytics with facial recognition to prepare a report to show how many hours each employee has worked. The report is not based only on login and logout hours, but also on video analytics that provide detailed information. In relation to this thesis, this software is marketed to companies by promises that the software proves how many hours employees really worked, and what they really did during the working hours. The software promises to prevent fraud by employees who might just show themselves as working instead of actually working. The software also promises to combat wage and hour lawsuits, which have been skyrocketing.[77]

Companies are able to collect employee data due to their contract-based relationship, as it is stipulated in the contract. Software that uses FRT offers higher efficiency and lower costs. Companies are having a hard time declining promising offers from this software, especially when classic HR department performance analyses are turning to data-driven performance analyses.[78] With FRT software, the "opportunity" for more data-driven performance analyses can be only a click away, and reveal all the information a company would need.

2.6.2 Facial Recognition Technology in Digital Signage

Facial recognition technology in electronic advertising boards, digital signage, and billboards is a recent trend that has emerged in the field of FRT.[79] Even the famous Piccadilly Circus Billboard in London has been equipped with FRT, which is integrated to hidden cameras that detect the faces of passers-by and assess their ages, genders, and moods in order to tailor

[75] Ibid.

[76] Ben Virdee-Chapman, (Kairos, 26 May 2016) '5 Companies Using Facial Recognition to Change The World' <https://www.kairos.com/blog/5-companies-using-facial-recognition-to-change-the-world> Accessed 1 January 2019

[77] Lydia DePillis, (The Washington Post, 25 November 2015) <https://www.washingtonpost.com/news/wonk/wp/2015/11/25/people-are-suing-more-than-ever-over-wages-and-hours/?utm_term=.41b15d00b126> Accessed 1 January 2019

[78] Bernard Marr, (2018, 1st Edition). 'Data-Driven HR: How to Use Analytics and Metrics to Drive Performance' Available online : <https://books.google.nl/books?id=rSRTDwAAQBAJ&pg=PA5&source=gbs_selected_pages&cad=3#v=onepage&q&f=false >, p.2 Accessed 1 January 2019

[79] Ben Virdee-Chapman, (Kairos, 26 May 2016) '5 Companies Using Facial Recognition to Change The World' <https://www.kairos.com/blog/5-companies-using-facial-recognition-to-change-the-world> Accessed 1 January 2019

personalised advertisements to them.[80] The global market for digital signage was $19.61 billion in 2016, and it is expected to grow to $32.84 billion by 2023.[81] The size and growth of the market clearly shows that advertising boards generate value for companies and that they will only become more common in the future. This might be concerning in the case that companies equip more and more of these boards with FRT, which is likely to lead to infringements of individuals' privacy rights and a lower expectation of privacy. [82]

Companies commonly use digital signage for marketing and analysis of their advertising audiences. Digital signs are equipped with a screen on which ads and marketing messages are displayed. They also have sensors that collect data from bystanders. The data is then used to evaluate how the observers react and respond to the advertisements. The data is collected and analysed by software that uses FRT.[83] Digital signage electronic screens are generally placed in public areas (e.g. streets, airports, and shopping malls). These screens or billboards are commonly used to display advertisements to people who walk past them. Such digital signage is usually connected to the Internet and is capable of measuring the reactions and demographics of the audience.

The Irish Data Protection Commissioner ("The Irish DPC") has published a press release concerning digital advertisement screens in public places.[84] Many privacy campaigners have expressed concerns about the intrusiveness of this technology.[85] The Irish DPC answers these concerns and makes a distinction between facial detection and FRT. Regarding the use of FRT in digital signage, the Irish DPC says that "the technology being used does not involve the recording, analysis, matching, profiling or storage of personally identifiable data". For

[80] Tom Cheshire (SKY News, 18 October 2017) ' Piccadilly Circus lights facial detection system 'incredibly intrusive'' <https://news.sky.com/story/piccadilly-circus-lights-facial-detection-system-incredibly-intrusive-11087020 > Accessed 1 January 2019

[81] Press Releases, Digital Signage Market worth 32.84 Billion USD by 2023, The report "Digital Signage Market by Product < https://www.marketsandmarkets.com/PressReleases/digital-signage.asp> Accessed 1 January 2019

[82] Buckley, Ben & Hunter, Matt. (2011). Say cheese! Privacy and facial recognition. Computer Law & Security Report. 27. 10.1016/j.clsr.2011.09.011. Available online: <https://www.researchgate.net/publication/251544161_Say_cheese_Privacy_and_facial_recognition> p. 4

[83] Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria - 21 dicembre 2017 [7496252]. Section 2 <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252> Accessed 1 January 2019

[84] The Irish Data Protection Commissioner, 'Press Release on the use of Facial Detection Technology in Advertising'' (15 May 2017)Available online: < https://www.dataprotection.ie/documents/Facialdetection.pdf> Accessed 24 November 2018

[85] Sean Hargrave (The Guardian , 17 August 2016) https://www.theguardian.com/media-network/2016/aug/17/facial-recognition-a-powerful-ad-tool-or-privacy-nightmare> Accessed 1 January 2019

this reason, the Irish DPC states that the data controllers have so far been adequately complying with data protection rules.[86]

As another example, in an Italian data protection case,[87] in which digital signage was installed in a train station, the Italian Data Protection Authority (DPA), *Garante*, examined how exactly software using FRT functions. In this case, the software in question was created by a private company called Quividi.[88] This software analyses the data collected by the video sensors in digital signs. The software uses FRT to determine when a human face comes in view of the digital sign; detects the time spent in front of the screen; derives the gender, age, and distance from the screen based on the facial characteristics of the observer; and evaluates the observer's appreciation of the advertisement. The software by Quividi collects, processes, and stores data for each face that is detected by the video sensor in the digital sign. For each face, a data set containing many different types of information is stored. The data that is collected includes a sequential number for the data set, the ID of the collecting digital sign, the date and time when the face was detected, the time that the face spent in front of the sign, the time the observer paid attention to the sign, the gender of the observer, the approximate age of the observer, the average distance from the sign, and an estimation of the observer's facial expression quantified as happiness in a scale from one to five. The data that is collected is encrypted and stored centrally in order to perform further statistical analysis comparing the happiness of the observer to the advertisements shown.[89]

In Quividi's software, biometric data such as facial images are stored in the RAM memory of the individual digital signs for long enough to perform analysis on a particular face. This analysis lasts only a few tenths of a second, after which the data is immediately overwritten by new data that the sensor collects. Thus, the facial data is never permanently stored in the hard drive of the digital signage, nor is the data transmitted outside the digital sign or sent to any Quividi system.[90] As a result, the use of digital signage was found compliant by data protection authorities.

[86] The Irish Data Protection Commissioner, 'Press Release on the use of Facial Detection Technology in Advertising'' (15 May 2017)Available online: < https://www.dataprotection.ie/documents/Facialdetection.pdf> Accessed 24 November 2018

[87] Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria - 21 dicembre 2017 [7496252]. Available online: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252> section 2, Accessed 1 January 2019

[88] Website of the Quividi. < https://quividi.com/> Accessed 1 January 2019

[89] Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria - 21 dicembre 2017 [7496252]. Available online: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252> section 2 Accessed 1 January 2019

[90] Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria - 21 dicembre 2017 [7496252]. Online: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252 p. 3

2.6.3 Facial Recognition Technology in the Retail Store Context

In the retail store context, the use is different from the use of public digital signage in the sense that retailers can use electronic screens but also the CCTVs in stores to gather data on customers with FRT. In this way, a retailer can analyse the preferences of the customer and predict their point of view towards a product from their facial expressions. Up to this point, predicting a customer's view is the same as what digital signage is doing. However, in the retail context, there are possible ways to identify the customer. Retailers also have a higher interest in gathering facial data through FRT to collect information for profiling and identifying individual customers.[91]

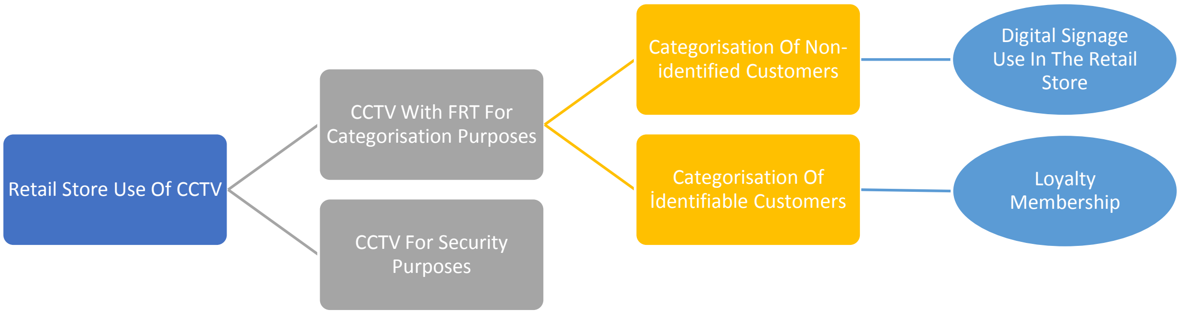
Retail Store Use Of CCTV
CCTV With FRT For Categorisation Purposes
CCTV For Security Purposes
Categorisation Of Non-identified Customers
Categorisation Of İdentifiable Customers
Digital Signage Use In The Retail Store
Loyalty Membership

Figure 2 Current practices for the use of CCTV cameras in retail stores:

As an example of this, some companies are already using FRT to gather biometric data to recognise "loyalty members" in their stores by linking the biometric data to an identifiable database.[92] One of such companies, Cali Group, is using FRT in their AI-enabled self-ordering kiosks to identify loyalty members. Cali Group does this by obtaining and storing a "unique digital fingerprint of the face" using their facial recognition software and comparing it to their database to identify the individual and determine whether he or she is a loyalty member.

John Miller, the CEO of Cali Group, summarises the reasoning behind the use of FRT as follows: "Face-based loyalty significantly reduces the friction associated with loyalty program registration and use. Further, it enables a restaurant chain like CaliBurger to provide a customised, one-on-one interactive experience at the ordering kiosk".[93] In recent years, there has been a growing interest in integrating FRT into the shopping experience.

[91] Farinella G.M., Farioli G., Battiato S., Leonardi S., Gallo G. (2014) Face Re-Identification for Digital Signage Applications. In: Distante C., Battiato S., Cavallaro A. (eds) Video Analytics for Audience Measurement. VAAM 2014. Lecture Notes in Computer Science, vol 8811. Springer, Cham, page 2

[92] Bryan Pearson, (Forbes, 15 March 2018) <https://www.forbes.com/sites/bryanpearson/2018/03/15/3-ways-retailers-can-use-facial-recognition-to-express-better-experiences/#794793541766> Accessed 1 January 2019

[93] Rick Ferguson, (RetailWire, 9 January 2018), 'Facial recognition software comes to loyalty'< https://www.retailwire.com/discussion/facial-recognition-software-comes-to-loyalty/ > Accessed 1 January 2019

Multinational foodstuffs producer Kraft has planned since 2011 to install face-scanning kiosks in supermarkets to recognise the age and gender of customers and give them tailored suggestions.[94] Similarly, Adidas has experimented with digital walls in stores to advertise shoes based on the gender and age of shoppers.[95]

In the retail store context, FRT is used as a means of categorisation to understand "emotions, attention and different psychological states" through facial modelling.[96] The purpose is to analyse customer preferences directly and to create a customer profile. As explained in section 2.4 in a detailed way, in the first stage, the facial features are detected, and the data is processed through a normalisation phase, which accounts for lighting, distance, and other variables common to images. After that, FRT analyses the person's psychological features. Facial recognition technology allows the person to be recognized, and with the use of software, this processing of personal data reveals the emotions and preferences of the individual.

Finally, the software creates a profile of the consumer by analysing their facial expressions. But, the purposes of understanding the behaviour of a customer go one step further. As the next step, the profile aims to influence the customer's preferences using different layers of marketing segmentation.[97] After that, the customer receives advertisements personalised for their preferences.

Currently, these companies are already using FRT for the purposes of identifying "loyalty members" and monitoring the facial expressions, age and gender of the customers in the store. But privacy experts are afraid that this data will be linked to databases or social networking sites, which will lead to identifying individuals and showing them targeted marketing based on their shopping behaviour.[98] This will lead to more data being collected from individuals and a further loss of privacy.

[94] Shan Li and David Sarno (Los Angeles Times, 21 August 2011) 'Advertisers start using facial recognition to tailor pitches' <http://articles.latimes.com/2011/aug/21/business/la-fi-facial-recognition-20110821> Accessed 24 November 2018

[95] Kashmir Hill, (Forbes, 1 September 2011) 'Kraft To Use Facial Recognition Technology To Give You Macaroni Recipes' <https://www.forbes.com/sites/kashmirhill/2011/09/01/kraft-to-use-facial-recognition-technology-to-give-you-macaroni-recipes/#6ccf03bc5390> Accessed 1 January 2019

[96] Cootes, T., & Taylor, C. (2000). Statistical models of appearance for computer vision. Technical report, University of Manchester, Wolfson Image Analysis Unit, Imaging Science and Biomedical Engineering. University of Manchester. Available at: < http://www.face-rec.org/algorithms/aam/app_models.pdf > Accessed 1 January 2019

[97] Kamenskaya, E & Georgy, Kukharev. (2008). 'Recognition of psychological characteristics from face', p,3 Available online: <https://pdfs.semanticscholar.org/b85f/c769fe5624fa1402d23f6e1cc45f555d635b.pdf> Accessed 1 January 2019

[98] Buckley, Ben & Hunter, Matt. (2011). Say cheese! Privacy and facial recognition. Computer Law & Security Report. 27. 10.1016/j.clsr.2011.09.011. Available online: <https://www.researchgate.net/publication/251544161_Say_cheese_Privacy_and_facial_recognition> p. 4

This chapter outlined the history, origins and developments of FRT. The main focus of the chapter was on FRT as a means of categorisation and the risks and potential misuses of FRT. In conclusion, it can be seen that FRT in the employment context for categorisation purposes enables many opportunities for employers. Moreover, the technology is already being used with commercial purposes in digital signage and retail stores. However, these use-cases of FRT for categorisation purposes include many risks, such as profiling, - especially if the data subject is identified- and raise data protection and privacy concerns which need to be resolved.

CHAPTER 3: LEGAL GROUNDS UNDER THE GDPR

This chapter aims to answer the second and third research questions. The second research question focuses on finding out "What are the legal grounds under the GDPR when FRT is used in the employment, digital signage, or retail contexts?" The third research question focuses on examining "What are the GDPR's various regulatory approaches to tackle facial recognition as a means of categorization in the contexts of employment, digital signage, and retail?"

3.1 Processing of Facial Data under the GDPR

As the Article 29 WP states, "facial recognition is the automatic processing of digital images which contain the faces of individuals for identification, authentication/verification or categorisation of those individuals".[99]

The GDPR determines the conditions for legally processing personal data and establishes six different legal grounds for the lawfulness of processing under Article 6 of the GDPR.[100] Processing must fulfil one of the legal grounds in Article 6, as these grounds are an exhaustive list of lawful processing.[101] The grounds include consent, the performance of a contract, compliance with a legal obligation, vital interest, public interest, and legitimate interest.

Facial data falls under the scope of Article 9 of the GDPR regulating biometric data, and because of the inherent risks of biometric data, explicit consent of the individual is required before the processing of digital images for facial recognition can be started.[102]

While this is the general rule, in some cases, the data controller may have to perform the first stages of the facial recognition process for evaluation purposes.[103] For the first steps of operations such as image acquisition, face detection, and comparison, the data controller might have a separate legitimate ground that complies with data protection rules. For example, it might be in the legitimate interest of the data controller.[104] In such cases, the data

[99] 'Article 29 Data Protection Working Party,Opinion 02/2012 on Facial Recognition in Online and Mobile Services', p. 2

[100] Regulation (Eu) 2016/679 Of the European Parliament and Of The Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (27 April 2016)

[101] Custers, Bart and Ursic, Helena, Worker Privacy in a Digitalized World under European Law (January 2018). Comparative Labour Law & Policy Journal, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3179425, p. 333-334

[102] Article 29 Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services, p. 5

[103] Ibid.

[104] Ibid.

controller might perform the first stages of facial recognition, however, “data processed during these stages should only be used for the strictly limited purpose to verify the user’s consent and should, therefore, be deleted immediately after”.[105]

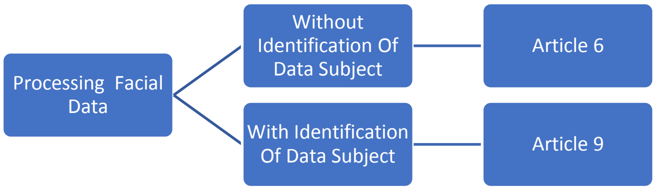
Processing Facial Data
Without Identification Of Data Subject
With Identification Of Data Subject
Article 6
Article 9

Figure 3 Distinction of legal grounds for processing facial data under the GDPR

At the same time, verifying the user’s consent might be a challenge in the case of FRT for categorisation purposes, because the enrolment stage is the stage where a data controller has the opportunity to inform the data subject about the processing, as it is indicated in Section 2.4. It constitutes the first contact for the data subject, during which the data subject can be informed about the data processing activity and asked for consent. In most scenarios of obtaining biometric data, enrolment requires data subject’s involvement.[106] However, “it is not necessary for a categorisation system to have an enrolment process”.[107] Additionally, “the image and/or reference template may be stored as a record for later comparison”[108] without the knowledge or consent of the data subject. This means that categorisation can be done without the person being informed. This feature of the technology also presents a challenge for data controllers trying to obtain a legal ground for their processing activities.

In order to provide a more specific analysis, the legal grounds for using FRT under the GDPR will be analysed in three concrete contexts: employment, signage, and retail stores. These examples will be used so that a more detailed picture can be provided regarding whether the present major regulations can address the problematic risks affiliated with these deployments of FRT.

3.2 Legal Grounds for FRT in the Employment Context

The legal grounds for FRT in the employment context have been well-evaluated by the Article 29 WP due to the vulnerable position and the need for protection of employees. In some of the related guidance on CCTVs in the workplace, the Article 29 WP has provided legal advisory opinions on the video surveillance of workers and the processing of image data in the employee-employer relationship. According to the Article 29 WP Opinion 8/2001 on the processing of personal data in the employment context, “data protection requirements apply to the monitoring and surveillance of workers [through] … video camera data”.[109]

[105] Article 29 Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services, p. 5
[106] Article 29 Data Protection Working Party, Developments in biometric technologies, opinion 3/2012, p. 5
[107] Article 29 Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services, p. 2
[108] Ibid.
[109] Article 29 Working Party Opinion 8/2001 On The Processing Of Personal Data In The Employment Context, p. 3

Furthermore, in the employment context, consent, the performance of a contract, and legitimate interest are the relevant legal grounds for processing personal data. However, because in the employment context FRT using biometric identification would aim to identify the data subject, the processing falls under Article 9 and requires the explicit consent of the employees. In contrast, if only facial detection were used for categorisation purposes, then the performance of a contract and legitimate interest could be applied due to the non-biometric nature of the data. Due to the strict approach of GDPR in the employment context, the legal grounds for both FRT using mere facial detection and FRT using biometric identification will be examined.

One of the legal grounds in the employment context is consent. According to the Article 29 WP opinion on developments on biometric technologies, "consent in the employment context has to be questioned and duly justified".[110] The opinion states that employers cannot rely on consent as a legal ground in the first place but instead should seek another legitimate ground to justify processing biometric data of employees. Moreover, the Article 29 WP indicates that if there is a less intrusive way to achieve the purpose of the processing activity, the employer should use it. The employer should always seek a non-biometric avenue for gathering data if possible.[111]

In addition, the opinion declares that "consent is only valid when sufficient information on the use of biometric data is given".[112] Because of the unique and universal characteristics of biometrics, valid consent is the crucial requirement for processing biometric data.[113] Article 4 (11) of the GDPR defines consent and indicates that:

> 'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action signifies agreement to the processing of personal data relating to him or her.[114]

Thus, in order to be valid, consent needs to meet the requirements indicated in the definition.

Consent being "freely given" is one of the requirements of valid consent and relies on the freedom of the data subject, as expressed in the Article 29 WP Opinion on the definition of consent:

> As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.[115]

[110] Article 29 Data Protection Working Party, Opinion 3/2012 on developments in Biometric Technologies, p.11
[111] Ibid.
[112] Ibid.
[113] Ibid.
[114] Article 4(11) of the GDPR
[115] Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, Adopted on 28 November 2017, p. 6

But in the employment context, the employee is arguably not in a position that she/he can freely consent to the processing activity without feeling compelled to consent or without being afraid of negative consequences. The Article 29 WP Opinion 8/2001 on the processing of personal data in the employment context strengthens this argument by stating that consent cannot be accepted as valid and freely given when the employer is involved in monitoring the worker's behaviour over time.[116] In the case that a company uses FRT to recognise an employee, the biometric characteristics of the data would require explicit consent from that employee. Categorisation might be used to identify the employee and to categorise their mood into pre-defined criteria. However, neither scenario can rely on employee consent.

As can be seen from the strict limitations mentioned above, consent in the employment context is a problematic topic due to the imbalance of power between the employer and the employees. Because of this imbalance, applying consent as a legal ground to process identifiable facial data of the employees requires special circumstances and is normally prohibited by the GDPR. The Article 29 WP has published many opinions due to the delicate nature of the topic and has examined the limits of consent in the employment context.[117] With their opinions, the Article 29 WP has explicitly drawn the boundaries of GDPR in the employment context without leaving much room for interpretation as also discussed in Section 2.6.1.

For the reasons mentioned above, consent per se is not a sufficient ground for the use of FRT in the employment context in general. If FRT were used only for categorisation purposes, then due to the lack of an identification element of the data, performance of a contract and legitimate interest could be used instead. Subsequently, these two legal grounds will be analysed to see whether an employer can seek another legal ground in order to process the biometric data of employees using FRT.

Performance of a contract can be another legitimate ground to process personal data by using FRT in the employment context. Article (6) (b) of the GDPR indicates that “processing is necessary for the performance of a contract to which the data subject is a party”.[118] Moreover, Recital (44) points out the important elements of the article as being that “processing should be lawful where it is necessary in the context of a contract”. The opinion gives guidance on how this “necessity” should be determined and explains that:

[116] Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, p. 6

[117] Article 29 Working Party Opinion 8/2001 On the Processing of Personal Data in The Employment Context p. 5; Article 29 Data Protection Working Party Opinion 2/2017 On Data Processing at Work; Article 29 – Data Protection Working Party Working Document on The Surveillance of Electronic Communications in The Workplace

[118] Article 6 of the GDPR

> The provision must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller.[119]

For instance, processing the bank account information of an employee to pay their salary is one of the valid uses of the performance of a contract as a legal ground.[120] At this point, the purpose limitation principle and assessment of necessity have to be connected to examine the rationale of the *performance of a contract* legal ground.[121]

After presenting the criteria to assess the necessity of data processing activity for the performance of a contract, the Article 29 WP opinion states that "video-surveillance of employees more clearly constitute processing that is likely to go beyond what is necessary for the performance of an employment contract".[122] Any data processing activity that aims to provide further information about the employee should be considered outside the scope of what is necessary for the performance of a contract, even if it would be only limited to face detection. Thus, a scenario that aims to categorise employees using CCTV cameras is extreme. It cannot be interpreted as "genuinely necessary" for the performance of a contract, and therefore this cannot be used as a legal ground in the employment context.

The third and last related legal ground for the employment context is the legitimate interest of the controller. Article 6(1)(f) of the GDPR defines this legal ground as:

> Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.[123]

According to the Article 29 WP Opinion 06/2014 on the notion of legitimate interests of the data controller, in order to determine the legitimate interest of the controller, Article 6(1)(f) requires a "balancing test" whereby the legitimate interests of the controller must be balanced with the interests and fundamental rights of the employee.[124] The outcome of this balancing test concludes whether the legitimate interest can be accepted as a legal ground for lawful processing.[125] The opinion elaborates on the concept of interest and explains that interest of the controller is related to the purpose of the controller.[126] According to recital 47 of the GDPR the legitimate interest requires data controllers to consider the reasonable expectations

[119] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller, p.16
[120] Ibid.
[121] Ibid. p. 17
[122] Ibid.
[123] Article 6(1)(f) of the GDPR
[124] Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller, p. 9
[125] Ibid.
[126] Ibid., p. 24

of data subjects and to provide protection for the fundamental rights and freedoms of these subjects.[127]

> The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects *do not reasonably expect further processing*.[128]

To apply this criterion to CCTV in the workplace environment, an employee would not reasonably expect further categorising by FRT. CCTV systems with FRT can disclose data regarding an employee and the employee would not expect to be sorted into pre-defined categories.

The Article 29 WP provides a list of examples that shows the most common contexts for the legitimate interest of the controller.[129] The only example on this list for data processing activities at workplace is "employee monitoring for safety or management purposes".[130] Thus, in the employment context, the legitimate interest of the employer is accepted if it is related to safety or management purposes, which means it would be acceptable for an employer to install CCTV cameras for safety reasons. For example, in the case of Köpke v. Germany[131], a shop assistant was subjected to covert video surveillance at the workplace. The cameras were installed by the employer and a private detective agency. The reason for the installation of these cameras was that the employer suspected the applicant of manipulating the company accounts. After inspection by the detective agency, the employer claimed that there had been theft and ended the contract of an employee without notice. The court declared that "there had not been any other equally effective means to protect the employer's property",[132] and after the balancing test, the court dismissed the employee's case and ruled that the employer had a legitimate interest in installing the cameras. Additionally, the Article 29 WP declares that the purpose of avoiding unlawful conduct has been ruled permissible in some jurisdictions[133] (i.e. The case of Bershka in the Constitutional Court of Spain[134]).

To summarise, the legitimate interest of the employer is acceptable only for safety and management purposes. In situations such as potential a fraud in the workplace, the balancing test would protect the interest of the employer. However, because CCTV systems create covert surveillance in the workplace, and for reasons other than safety, they cannot be placed

[127] Ibid.; Recital 47 of the GDPR.

[128] Recital 47 GDPR emphasis added.

[129] Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller, p.25

[130] Ibid.

[131] *Köpke v Germany*, App no. 420/07 (ECHR, 5 October 2010)

[132] Ibid.

[133] Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, p. 19, footnote 19.

[134] Victor Bescós, (Pragma International, 24 January 2018) Dismissal with Video Surveillance as Supporting Evidence, Has it Changed Case-law?<'http://pragma.international/article/dismissal-with-video-surveillance-as-supporting-evidence-has-it-changed-case-law> Accessed 1 January 2019

without a valid legal ground. Moreover, in the employment context, cameras with FRT will likely fail the balancing test, as they are not strictly necessary and proportionate.[135] The interests or fundamental rights and freedoms of the employee would make the interest illegitimate, unless there is a clearly necessary purpose behind installing CCTV.

Lastly, the Article 29 WP has published an opinion relevant to cameras with FRT in the workplace, in which they explicitly examine monitoring of the facial expressions of employees at work.[136] The opinion highlights the disproportionality of the use of FRT in the employment context:

> With the capabilities given by video analytics, it is possible for an employer to *monitor the worker's facial expressions by automated means*, to identify deviations from predefined movement patterns (e.g. factory context), and more. This would be *disproportionate to the rights and freedoms of employees*, and therefore, generally *unlawful*. The processing is also likely to involve profiling, and possibly, automated decision-making. Therefore, employers should refrain from the use of facial recognition technologies. There may be some fringe exceptions to this rule, but such scenarios cannot be used to invoke a general legitimation of the use of such technology.[137]

In conclusion, categorising employees using FRT embedded in CCTV cameras or applying predictive analyses cannot rely on performance of a contract as it is not strictly necessary. Thus, there are no legal grounds for FRT to be used for the sole purpose of categorisation in the workplace. The use of CCTV cameras with FRT in the workplace is strictly regulated under GDPR and the Article 29 WP has explicitly declared that the use of such technology would be disproportionate in the employment context. Facial recognition processing cannot rely on any legal grounds to be lawful, and the use of FRT must be avoided in the workplace due to high risks to the fundamental rights and interests of the employees.

3.3 Legal Grounds for FRT in Digital Signage

As mentioned above, the Article 29 WP opinion on the legitimate interest of the data controller provides guidance on how to carry out the balancing test and how legitimate interest should be interpreted. Unlike in the employment context, in the context of consumer-business relations, the interpretation of "interest" is much broader. While explaining the concept of interest, the Article 29 WP defines the legitimate interest of the data controller as "the economic interest of a company to learn as much as possible about its potential customers so that it can better target advertisement about its products or services".[138] Following the concept of interest, the Article 29 WP provides a non-exhaustive list for the most common contexts in which the legitimate interest of data controller can be relied upon. There are two different examples in that list, which refer to marketing purposes. The first is

[135] Article 29 Data Protection Working Party, Opinion 2/2017 On Data Processing at Work, p. 23
[136] Article 29 Data Protection Working Party, Opinion 2/2017 On Data Processing at Work, p. 19
[137] Ibid.
[138] Article 29 Data Protection Working Party Opinion 06/2014 On the Notion of Legitimate Interests of The Data Controller, p. 24

"conventional direct marketing and other forms of marketing or advertisement", and the second is "processing for research purposes (including marketing research)".[139]

It can be said, especially for marketing purposes, that if there is research being conducted behind the marketing purpose, the legitimate interest would likely survive the balancing test. However, the GDPR changes its approach if monitoring activities are used for marketers to gain more information about their customers:

> However, this does not mean that controllers would be able to rely on Article 7(f) *to unduly monitor the on-line or off-line activities of their customers*, combine vast amounts of data about them from different sources that were initially collected in other contexts and for different purposes, and create - and, for example, with the intermediary of data brokers, also trade in - c*omplex profiles of the customers' personalities and preferences without their knowledge,* a workable mechanism to object, let alone informed consent. Such a profiling activity is likely to present *a significant intrusion into the privacy of the customer*, and when this is so, the controller's interest would be overridden by the interests and rights of the data subject.[140]

This indicates that the legitimate interest of the controller in the marketing context is limited and that this limitation is a safeguard for customers. Because of the nature of digital signage, asking for consent from passers-by is highly impractical. Thus, for marketing purposes, the most relevant legal ground for digital signage under the GDPR is the legitimate interest provided by Article 6. Article 9 relating to biometric data does not usually apply as it requires consent, and acquiring explicit consent for digital signage remains impractical for both the data controllers and data subjects. Facial recognition processing in digital signage usually relies on facial detection and does not involve the identification of data subjects based on their faces. Facial recognition technology in digital signage categorises data subjects to general demographics and analyses their reactions to tailored advertisements.[141]

The Italian DPA, *Garante*, decided a case on digital signage in which promotional devices called totems were installed at the Milano Centrale railway station.[142] The issue in the case was that people complained that the totems used recognition and facial tracking technology. It was found that the totems detected human faces, measured the time spent looking at the ads on the screen, categorised the data subjects by their gender and age, and analysed their

[139] Article 29 Data Protection Working Party Opinion 06/2014 On the Notion of Legitimate Interests of The Data Controller, p. 25

[140] Ibid., p. 26 emphasis added.

[141] Farinella G.M., Farioli G., Battiato S., Leonardi S., Gallo G. (2014) Face Re-Identification for Digital Signage Applications. In: Distante C., Battiato S., Cavallaro A. (eds) Video Analytics for Audience Measurement. VAAM 2014. Lecture Notes in Computer Science, vol 8811. Springer, Cham, page 2

[142] Installazione di apparati promozionali del tipo "digital signage" (definiti anche totem) presso una stazione ferroviaria - 21 dicembre 2017 [7496252] Available online:<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252> Accessed 1 January 2019

facial expressions.[143] The data collector Grandi Stazioni Retail s.p.a. stated that the data was collected, encrypted, and processed for the purpose of statistical analysis. The Italian DPA, *Garante* decided that the data processing used adequate safety measures, such as data minimisation, lawfulness, and proportionality, to comply with the Italian Privacy Code.[144]

One of the deciding factors in the case was that Grandi Stazioni Retail did not use FRT involving biometric identification. Instead, "facial detection" was used, which does not identify the face of the specific data subject through biometric data. Another important fact was that the facial data was stored only for a few tenths of a second at most, and immediately deleted afterwards.[145] However, The Italian DPA required Grandi Stazioni Retail to be more transparent about the data processing and ordered it to put a notice next to the totems and to provide more detailed information on their website. The Italian DPA required periodic monitoring of the proper functioning of the devices at least every six months as a security measure.[146] As a result, the Italian data protection authority, *Garante*, declared that the usage and data processing of digital signage was lawful. It can be generalized that if there is research purpose behind the marketing purpose, the legitimate interest would likely survive the balancing test and a valid legal ground for FRT in digital signage would be obtained.

Lastly, the Article 29 WP opinion indicates that "what can be considered as a legitimate interest can also change over time, depending on scientific and technological developments, and changes in society and cultural attitudes".[147] This statement can be interpreted in two ways – either it leaves a possible legal ground open for future advanced marketing strategies, or there shall be more limitations and controls of such use when the privacy risks are on the rise due to technology advances.

3.4 Legal Grounds for FRT in Retail Stores

In the context of retail stores, there are two relevant legal grounds for processing facial data, which apply depending on the way that FRT is used. First, if the retail store uses FRT without

[143] Ellen O'Brien, (Data Guidance, 1 February 2018) 'Italy: Garante's decision on digital signage "correctly balances parties' interests" '< https://www.dataguidance.com/italy-garantes-decision-digital-signage-not-easy-one/ > Accessed 1 January 2019

[144] Installazione di apparati promozionali del tipo "digital signage" (definiti anche totem) presso una stazione ferroviaria - 21 dicembre 2017 [7496252] Available online:<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252>

[145] Installazione di apparati promozionali del tipo "digital signage" (definiti anche totem) presso una stazione ferroviaria - 21 dicembre 2017 [7496252] Available online:<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252>

[146] Ellen O'Brien, (Data Guidance, 1 February 2018) 'Italy: Garante's decision on digital signage "correctly balances parties' interests" '< https://www.dataguidance.com/italy-garantes-decision-digital-signage-not-easy-one/ > Accessed 1 January 2019

[147] Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller, p. 25

identifying the individual and only use facial cues to detect the mood or interest of the customer, then it falls under the same ground as digital signage, which is "legitimate interest" as provided by Article 6 (f) of the GDPR. But in retail stores where such cameras are installed, there should be a prominent notice, so that a consumer may choose whether to step in or not. Walking into a retail shop after seeing a prominent sign would indicate the acceptance of being monitored in the shopping environment. Second, if the retail store uses FRT to identify an individual, then the consent of the data subject would be needed, as is stated in Article 9 of the GDPR. The main difference between retail stores and digital signage is the element of identification. In this section, the use of FRT in retail stores with and without identification of the customer will be explained and requirements of consent will be analysed in the scenario of loyalty programs. Retail stores can obtain consent in different ways. Considering the different approaches in the market, some retail stores are asking consent for the use of FRT jointly with their loyalty membership programs.[148]

Retail stores are also using digital signage in their stores. In such cases, they can rely on the legitimate interest of the data controller provided that they do not use biometric recognition and take adequate safeguards to comply with the GDPR. It is important to note that the non-identification of data subjects should be guaranteed by safeguards that are indicated in the GDPR, not only by the claims of the data controllers themselves. Only by following these regulations can it be assured that FRT does not create a risk of profiling for an individual and is less intrusive of privacy.

Another example of FRT in the retail store context is that of loyalty programs. Many stores have loyalty programs, and FRT can be used to identify each loyalty member and each customer. The store needs to obtain consent from all customers that they want to identify with FRT. For a retail store, the most convenient time to obtain consent from customers is when they are registering as a loyalty member. With these loyalty programs, the companies can offer their services with added features such as recognising loyalty members and letting them pay with their faces. However, the requirements of valid consent must be met when asking customers to register to loyalty programs with FRT features. Then the question is raised: is consent a valid legal ground for such use of FRT?

When a client casually enters a shop, does that constitute explicit consent? The client might be considered to be giving consent by entering the shop after reading a prominent notice on the front door. Applying this case to our context, if the retail store is using CCTV with FRT for categorisation purposes without identification of the data subjects, then categorisation purposes might be legitimate, as the retailer can apply legitimate interest.

[148] Rick Ferguson, (RetailWire, 9 January 2018), 'Facial recognition software comes to loyalty' < https://www.retailwire.com/discussion/facial-recognition-software-comes-to-loyalty/ > Accessed 1 January 2019>

Following this question, the requirements for consent will be analysed to determine whether it can be used as a legal ground to process customer data with FRT also for categorisation purposes in retail stores.

If a store means to identify the customer – no matter what the purpose – then the use of FRT falls under Article 9 instead of Article 6 of the GDPR. With retail companies and restaurants, there is usually an additional element of identifying the customer through biometric data to build a profile of the data subject's shopping habits and to link customers to their database and to provide membership benefits.[149]

Article 9 of the GDPR prohibits the processing of biometric data for uniquely identifying data subjects unless "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes".[150] Thus, a company may only identify the customer using biometric data after receiving an explicit consent from their customer.

Explicit consent is open to interpretation because it is not always apparent which conditions should be fulfilled to acquire it validly. In general, consent needs to be freely given, informed, specific, and it should be unambiguous.[151] Moreover, consent should be obtained with a statement or by an explicit affirmative action from the data subject, and it needs to signify the agreement to related data processing activity.[152]

Article 42 implies that if a data subject does not have an authentic or free choice or is not able to refuse giving consent without any damage, then consent cannot be accepted as freely given. Furthermore, the Article 29 WP, Opinion 15/2011 on the definition of consent indicates that to accept the existence of freely given consent, the data subject should be able to exercise a "real choice" without any deception or threat of negative consequences.[153] The context of the written declaration should ensure that the data subject can understand the extent of consent.[154] The language for the declaration should not obscure the context from being understandable, and the data subject should be able to see the data controller's intent for the data.[155]

It should be also noted that if the retail store aims to gain their customers' consent to identify them using FRT with categorisation purposes, it is the retailer's responsibility to obtain this consent in the right way from data subjects. In the case of loyalty membership programs, one of the concerns is whether the data subjects are freely and explicitly giving their consent to

[149] Farinella G.M., Farioli G., Battiato S., Leonardi S., Gallo G. (2014) Face Re-Identification for Digital Signage Applications. In: Distante C., Battiato S., Cavallaro A. (eds) Video Analytics for Audience Measurement. VAAM 2014. Lecture Notes in Computer Science, vol 8811. Springer, Cham, p. 2

[150] Article 9 (2) (a) GDPR

[151] Article 4 (11) of the GDPR

[152] Ibid.

[153] Ibid.

[154] Recital 42 of the GDPR

[155] Ibid.

these companies or whether the customers feel obliged to consent in order to get regular service.

One of the requirements of freely given consent is that data subject should have the option of choosing not to consent. The data subject should have an option to still get equivalent service. For example, customers should have choices other than loyalty membership. They should not necessarily have to become a loyalty member to get service. It can be said that customers have free choice when they can shop and get regular service without registering as loyalty members.

However, it should be considered if the data subject understands the scope of the context to which she or he is consenting. As Solove argues, individuals do not have enough knowledge to assess the result of their consent.[156] A problem that customers often have is that they do not read privacy statements or the terms and conditions to which they are consenting.[157] For this reason when companies are asking for declaration of explicit consent, the purposes of the processing should be clearly presented, easily understandable, and the language should avoid any kind of complexity.

This situation in practice cannot be ignored. An excellent example of why customers cannot see the broad scope of the context of consent is in the kiosks with AI-enabled technology. As was mentioned in Section 2.6.2, Cali Group uses FRT in their AI-enabled self-ordering kiosks. In such a scenario, customers cannot foresee what kind of data AI can glean from a customer's face. Recital 42 provides guidance on how a declaration of consent, pre-formulated by the controller, should be presented to the data subject. Recital 32 indicates that “Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her” [158]

In the example of the use of FRT in a retail store, for example, the customer can be informed via a visualised privacy statement. Data flows can be illustrated, and the extraction process of FRT can be shown using visualisation techniques. The company might even show it as a cartoon, which would serve nicely. It would guarantee that the customer would have more information on the process if a video were used compared to traditional privacy statements.

[156] Daniel J. Solove, ‘Privacy Self-Management and the Consent Dilemma’ [2013] Harvard Law Review 1880-1886

[157] Phil Lee (FieldFisher, 12September 2016) ‘The nuance of "accepting" vs. "reading" a privacy policy’ https://privacylawblog.fieldfisher.com/2016/the-nuance-of-accepting-vs-reading-a-privacy-policy , David Berreby,(The Guardian, 3 March 2017) ‘Click to agree with what? No one reads terms of service, studies confirm’ <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print > Accessed 1 January 2019

[158] GDPR Recitals 42 and 32

Recital 32 implies that such information can be provided in electronic form, like on a website. However, there are also some arguments on the lawfulness of granting consent by electronic forms. Phil Lee addresses this concern in his article, stating that the difference between accepting and reading a privacy policy is quite challenging.[159] Moreover, he points out that if no one reads privacy policies, it means that there is no meaningful consent being given.

The Article 29 WP Opinion 15/2011 on the definition of consent addresses the quality, accessibility, and visibility of information.[160] The quality of the information means that "an average user should be able to understand it". In that sense, the subject's understanding of the process makes the consent informed. Thinking of the abilities of FRT, it is uncertain how the average user can understand what the technology will extract from their faces. Are they informed that from their face, the company will analyse their preferences about products? Obtaining consent with a single click should not be the way to obtain consent for such a privacy-intrusive technology. Either way, the procedure of obtaining consent must not leave any doubt about the intentions of the data subject.

In the imbalanced consumer-businesses relationship, the consent requirement is not considered as often as it needs to be. Consumers consent the use of their data without knowing what they are creating for the controller – a profile of the customer that is not accessible to them. In that sense, when the loyalty member consents for identification from their face, the company gains the ability to create a profile of the customer. The data that they can gather is not only the face, but also customers' habits, reactions and preferences. In such scenarios, consumers might end up giving up their facial data without understanding the full implications of their consent. Considering current practices, it is quite challenging to ensure that customers are providing consent within these boundaries.

If a retail store is identifying the customer, consent cannot be accepted as explicit with just entrance to the store that has a prominent notice on the front door. However, if a retail store acquires consent together with a loyalty program, and the consent is explicit, freely given, informed and unambiguous the consent can be accepted as valid. But as discussed, the companies have to overcome the high standards of acquiring valid consent, especially in guaranteeing that the consent is informed and specific, which is difficult to achieve in practice given the features of FRT and the possible uses of facial data for categorisation purposes.

[159] Phil Lee (FieldFisher, 12September 2016) 'The nuance of "accepting" vs. "reading" a privacy policy' <https://privacylawblog.fieldfisher.com/2016/the-nuance-of-accepting-vs-reading-a-privacy-policy> Accessed 1 January 2019

[160] Article 29 Data Protection Working Party, Opinion 15/2011 On the Definition of Consent, p.20

3.5 Analysis and Reflections of GDPR’s Regulatory Approach in the common use-cases

After explaining the use of FRT for categorisation purposes and analysing the relevant legal grounds of the GDPR, this part, aims to analyse what are the GDPR’s various regulatory approaches to tackle facial recognition as a means of categorization in the contexts of employment, digital signage, and retailing. Second, this part aims to discuss how to best tackle existing issues under the GDPR’s legal framework related to the current problems and risks arising from the use of FRT. In order to see how protection of data subjects and their right to privacy could be improved, different approaches in different contexts will be analysed and explained.

In order to answer the third sub-question of what are the GDPR’s various regulatory approaches to tackle facial recognition as a means of categorization, three different contexts have been analysed to investigate the possible legal grounds in these three concrete contexts. The legal grounds in the employment context do not allow employers to use FRT for categorisation purposes. Even though FRT does not identify the employee, the legitimate interest and performance of a contract grounds fail the balancing test, as we have shown. Therefore, such a use-case of FRT does not fulfil the criteria of lawful processing. When we analysed digital signage, legitimate interest did provide lawful legal ground for data processors, but only if the data subject is not identified and the extracted data is deleted just after processing. Lastly, in the retail context, two different legal grounds allow data controllers to apply processing activities. One is consent, and the other is a legitimate interest, if the identification feature is not used – similar to digital signage. However, obtaining consent for the identification of a customer still needs further justification due to the privacy-intrusiveness of the technology.

In the context of digital signage, it can be said that the rules of the GDPR have to be applied on a case-by-case basis to each use-case and application of FRT. The case by Italian DPA Garante, which concerned digital signage in a railway station, is an excellent example of this. In that case, the data processing was lawful, but only because the application was very privacy friendly, collected a minimum amount of data, did not store data any longer than was absolutely necessary, and did not identify individuals. This does not mean that all uses of FRT in digital signage are GDPR compliant. Companies using or planning to use FRT in digital signage should conduct a DPIA and carefully consider the different requirements and principles set out in the GDPR to ensure that their processing is lawful.

In the context of employment, there is a barrier for obtaining consent from an employee. The rationale for the barrier is the imbalanced relationship between an employer and an employee. However, in the retail context, this protection disappears if the data subject turns into a customer. Customers do not enjoy the same protections that employees do regarding their rights to privacy. In the past, businesses were only selling goods. If you paid the price of the good, the contract was completed between parties. Now, customers are not paying just with their money, but also with their personal data by helping businesses “to enhance customer experience” through their research. The protection in the employment context shows that if the data subject wants to be protected properly, regulators can restrict the powerful party from violating the rights of "the weaker party", as is happening in the employment context. However, if the employee turns into a customer, the approach to protecting the weaker party changes significantly, and consent can be used as a legal ground.

All in all, the safeguards and interpretations of the law by data protection authorities are stricter for employer-employee relationships, clearly favouring the employees and protecting their freedoms and fundamental rights. However, the protection of data subjects is less strict in commercial context. More problems may arise in the future, as companies will likely introduce different business strategies to enhance customer experiences. At this point, the way that consent will be obtained is essential in order to start any data processing activity of customers. Data protection authorities should not let businesses run their data analytics on customers without constraints. Companies shouldn't be putting the burden on data subjects who have to consent to the data processing activities in order to get regular service. The strict regulatory approach protects employees well and that protection should also be provided to customers. Regulators have adapted a different level of protection for data subjects in commercial and employment contexts, and it can be said that the GDPR could protect some data subjects, especially customers, better.

As discussed in Section 3.2, employers can ask consent from their employees, but it is not valid because of the imbalanced relationship between them. But it can be argued that in a commercial context, there can be a similar imbalance between customers and large companies, because of the difference in resources and the leverage that companies have over customers. This might be the case especially with large companies that have monopolies over certain markets. Unfortunately, if a data subject is a customer, the regulatory approach is less strict and benefits the companies more than it protects the customers.

Legal Grounds for Facial Recognition as a Means of Categorization				
	Categorization Without Identification of Data Subject Article 6 of the GDPR			Categorization with Identification of Data Subject Article 9 of the GDPR
	Consent	**Performance of a contract**	**Legitimate interest**	**Explicit consent**
Employment context	No	No	No	No
Digital signage context	Yes	No	Yes	No
Retail stores context	Yes	No	Yes	Yes

Figure 4 Legal Grounds for Facial Recognition as a Means of Categorisation

The first reflection is based on the Article 29 WP's approach to different contexts. As has been discussed in Section 3.2, FRT is appropriately regulated in the employment context.

The Article 29 WP explicitly declares that the use of such an intrusive technology is disproportionate. From this reasoning, we can derive improvements to the two other troublesome areas of digital signage and retail stores. The privacy problems in these two contexts can also be solved with the guidance and reasoning of the Article 29 WP. The rules that restrict the use of FRT in the employment context should also apply to commercial purposes so that the facial data of customers would have increased protection.

The second reflection is about privacy by design. As was indicated in Section 2.4, due to the biometric sensitivity of facial data, privacy-preserving techniques should protect individuals from being the target of CCTVs. De-identification is one of the procedures that prevent the connection between the person and the information from being established.[161] This would improve protections, and as a consequence, make data more untraceable and safer, which is another option to avoid the risk of FRT. Privacy by design solutions provide promising results. De-identification software such as D-ID[162] may be one of the solutions to avoid the identification problem for individuals. Currently, retail stores are using encryption techniques to protect the stored data. However, technologies like D-ID would take protection one step further, making the facial data unreadable by algorithms.

D-ID technology makes the facial data impossible to read for algorithms.[163] It protects the individual's face from FRT by modifying the image to interfere with automated face recognition systems. D-ID accomplishes this by using modification methods and modifies the image of a face. Therefore, the difference between the two pictures is not recognisable to the human eye. However, for algorithms, the facial data becomes unidentifiable. After D-ID, the picture is almost identical to the original one, but not recognisable by facial recognition systems.

[161] De-Identification of Personal Information, Simson L. Garfinkel, National Institute of Standards and Technology October 2015, < https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2015/10/nistir_8053_draft.pdf > , p. 9 Accessed 1 January 2019

[162] Official Website of De-Identification <https://www.deidentification.co/#footer > Accessed 1 January 2019

[163] Paul Monckton (Forbes, 29 January 2018) 'New AI Tech Blinds Computer Facial Recognition Systems'<https://www.forbes.com/sites/paulmonckton/2018/01/29/d-id-defeats-facial-recognition/#be5d4b334b0d> Accessed 1 January 2019

CHAPTER 4: CONCLUSION

This thesis has aimed to answer the central question of whether the GDPR's legal grounds are suited for facial recognition technologies (FRT), and what are the GDPR’s various regulatory approaches to tackle facial recognition as a means of categorization in the contexts of employment, digital signage, and retail. It has addressed this research question by analysing the following sub-questions:

1. What is FRT? How does facial recognition work as a means of categorisation and what risks are there in these common use-cases?
2. What are the legal grounds under the GDPR when FRT is used in the employment, digital signage, or retail contexts?
3. What are the GDPR’s various regulatory approaches to tackle facial recognition as a means of categorization in the contexts of employment, digital signage, and retail?

The focus of this thesis was to assess the lawfulness of processing facial data with FRT for the purpose of categorisation under the GDPR. GDPR’s regulatory approach has been analysed in three different contexts and the related privacy concerns have been highlighted.

Chapter 2 outlines the development of FRT and introduces how the technology is used in the employment, digital signage, and retail contexts. It is shown that FRT can disclose sensitive information regarding data subjects and enables the categorisation of individuals. Further, it is established that such profiling increases the impact on the right to privacy of individuals, and for that reason, privacy protection for individuals is required.

The chapter established that due to the high-risk nature of FRT for individuals, it is important to indicate how facial data differs from other personal data. The risks involved with FRT have been highlighted to demonstrate why it requires strict safeguards. Regulatory approach of the GDPR is especially essential for individuals so that they are less vulnerable to be targets for personalised advertising and profiling. Facial data requires stricter rules than any other biometric data.

Facial recognition technology in the employment context for categorisation purposes enables many opportunities for employers. Moreover, the technology is already being used for commercial purposes in digital signage and retail stores. However, these use-cases of FRT involve risks, such as profiling and they raise data protection and privacy concerns that need to be resolved. As is explained in this thesis, the use of FRT creates a number of risks for data subjects due to its technological features. These risks arise from the fact that facial data can be extracted without the knowledge of the data subjects and can lead to categorisation, commercial profiling and identification of data subjects.

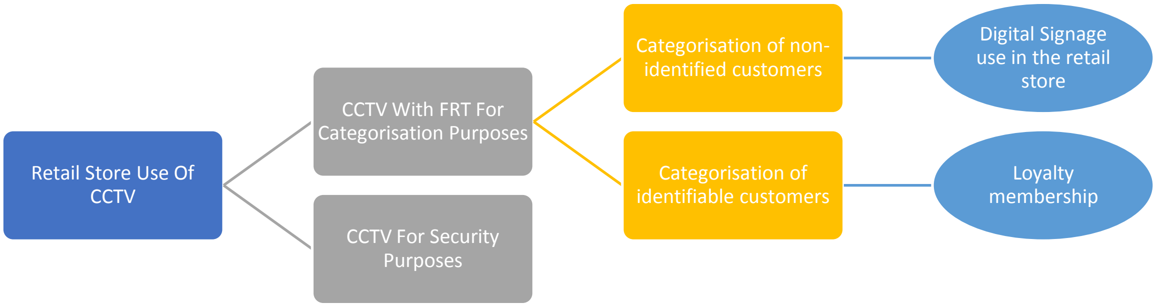
Retail Store Use Of CCTV
CCTV With FRT For Categorisation Purposes
CCTV For Security Purposes
Categorisation of non-identified customers
Categorisation of identifiable customers
Digital Signage use in the retail store
Loyalty membership

Figure 5 Current practices for the use of CCTV cameras in retail stores

Chapter 3 focused on examining the second sub-question and it was established that the GDPR provides an exhaustive list of legal grounds, which have to be applied differently to each context in which FRT is being used.

- In the context of employment, there are not any legal grounds that would provide a lawful basis for the processing of employee data with FRT as a mean if categorisation, because of the disproportionality of the processing and the imbalance of power between the employer and employee.

- In the context of digital signage, the GDPR allows data controllers to use FRT to categorise individuals. Data controllers can use legitimate interest as their legal ground, as long as the processing complies with strict safeguards. In an Italian case, the Italian DPA highlighted adequate safeguards that were used in the processing:
  - The data was processed for the purpose of statistical analysis, and the processing did not use FRT for biometric identification.
  - Facial data was stored only for a few tenths of a second at most, and immediately deleted afterwards.
  - The Italian DPA required *Grandi Stazioni Retail* to be more transparent about the data processing and ordered it to put a notice next to the digital signs and to provide more detailed information about processing on their website
  - As a security measure, the Italian DPA required periodic monitoring of the proper functioning of the devices at least every six months.

- In the context of retail stores, use of FRT can be lawful in two different scenarios:
  - First, if the retail store does not identify the customer, then the data processing activity may fall under the legitimate interest of the data controller in a similar way as in the context of digital signage.
  - Second, explicit consent from customers can justify the data processing activities by retail store owners. However, due to the strict requirements of explicit consent, there are still other conditions that must be met before the processing is lawful.
    - If a retail store is identifying the customer, consent cannot be accepted as explicit with just entrance to a store that has a prominent notice on the front door.

- ➢ If a retail store acquires consent together with a loyalty program, and the consent is explicit, freely given, informed and unambiguous, the consent can be accepted as valid.
- ➢ Companies have to overcome the high standards of acquiring valid consent, especially in guaranteeing that the consent is informed, specific and explicitly given, which is difficult to achieve in practice given the features of FRT and the possible uses of facial data for categorisation purposes.

Legal Grounds for Facial Recognition as a Means of Categorization				
	Categorization Without Identification of Data Subject Article 6 of the GDPR			Categorization with Identification of Data Subject Article 9 of the GDPR
	Consent	**Performance of a contract**	**Legitimate interest**	**Explicit consent**
Employment context	No	No	No	No
Digital signage context	Yes	No	Yes	No
Retail stores context	Yes	No	Yes	Yes

Figure 6 Legal Grounds for Facial Recognition as a Means of Categorisation

When we apply the GDPR's legal ground requirements to FRT, there is no legal ground in the context of employment that justifies using FRT in the workplace. However, the legal grounds for commercial purposes are not so strictly regulated and the lawfulness of processing remains possible but needs to be assessed on a case-by-case basis. According to the Italian DPA, the use of FRT in digital signage can fulfil the requirements of lawful processing if adequate safeguards are in place and the use of biometric data is minimal.

Consequently, in such cases of digital signage, the legitimate interest of the controller can justify the data processing activity. The most troublesome cases arise in the retail context, as companies are interested in identifying their customers and profiling their shopping preferences and behaviour. A significant concern in the retail context is the requirement in Article 9 of the GDPR of explicit consent when dealing with biometric data. The validity of such consent is still questionable because acquiring explicit consent for such a complex and multipurpose processing activity like FRT shifts the burden of understanding the technology, its possibilities, and the data protection risks to the individual. Another problem is that there is an imbalance between an individual customer and a company, similar to the imbalance of employer-employee relationship, which means that customers don't enjoy the same level of protection as employees. Thus, regulators should narrow their approaches for commercial use-cases of FRT. This would reduce the risk of profiling for identified data subjects due to the intrusive characteristics of FRT and enhance the overall protection of individuals as customers to the level they would have as employees.

According to the analysis of the above research questions, it can be concluded that the use of FRT as a means of categorisation can be lawful in certain circumstances under specific legal grounds provided by Articles 6 and 9 of the GDPR. These legal grounds are consent, legitimate interest and explicit consent as shown in the above figure. But there must be strict safeguards in place to lawfully process facial data, and every new use-case and application should be assessed to ensure compliance with the rules and principles of the GDPR.

4.1 Limitations and Recommendations

The scope of this thesis is limited mainly to FRT in three different contexts, namely: employment, digital signage and retail. It should be noted that besides these three contexts that have been examined in this thesis, FRT is used by an increasing number of different entities. They are interested in the use of FRT and the data that is collected, which can subsequently be used for multiple purposes. These entities include both private and public service providers, such as law enforcement for crime investigation, airports for public security, the military, banks, casinos, public events, commercial buildings, correction agencies, government agencies, and agencies that deal with finding missing children and combating human trafficking. It needs to be kept in mind that FRT is used in different ways in these fields and may also involve many other risks, higher and lower, which have to be tackled differently.

The downside of choosing these three scenarios is that the examination is narrow and limited to these contexts. The conclusions of this thesis should not be directly applied to other use cases of FRT. This thesis has focused on the use of FRT in the private sector and different considerations have to be taken into account when applying the rules of the GDPR to the use of FRT in the public sector.

Lastly, it is recommended that further research be carried out on the topic. Also, the Article 29 WP – with its new name, the European Data Protection Board – should provide an opinion on this specific topic to limit the use of this technology in an intrusive way.

BIBLIOGRAPHY

Literature

1. Alex Pentland, Tanzeem Choudhury, ‘Personalizing Smart Environments : Face Recognition for Human Interaction’ (8 October 1991), The Media Laboratory Massachusetts Institute of Technology, http://hd.media.mit.edu/tech-reports/TR-516.pdf

2. Bernard Marr, (2018, 1st Edition). ‘Data-Driven HR: How to Use Analytics and Metrics to Drive Performance’.

3. Bing Liu. Sentiment Analysis and Opinion Mining, Morgan & Claypool Publishers, May 2012.

4. Buckley, Ben & Hunter, Matt. (2011). Say cheese! Privacy and facial recognition. Computer Law & Security Report. 27. 10.1016/j.clsr.2011.09.011. Available online: <https://www.researchgate.net/publication/251544161_Say_cheese_Privacy_and_facial_recognition>

5. Charles Darwin, (1872) ‘The expression of the emotions in man and animals.

6. Cootes, T., & Taylor, C. (2000). Statistical models of appearance for computer vision. Technical report, University of Manchester, Wolfson Image Analysis Unit, Imaging Science and Biomedical Engineering. University of Manchester. Available at, http://www.face-rec.org/algorithms/aam/app_models.pdf.

7. Custers, Bart and Ursic, Helena, Worker Privacy in a Digitalized World under European Law (January 2018). Comparative Labour Law & Policy Journal, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3179425

8. Daniel J. Solove, ‘Privacy Self-Management and the Consent Dilemma’ [2013] Harvard Law Review.

9. De-Identification of Personal Information, Simson L. Garfinkel, National Institute of Standards and Technology October 2015, < https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2015/10/nistir_8053_draft.pdf> .

10. Farinella G.M., Farioli G., Battiato S., Leonardi S., Gallo G. (2014) Face Re-Identification for Digital Signage Applications. In: Distante C., Battiato S., Cavallaro A. (eds) Video Analytics for Audience Measurement. VAAM 2014. Lecture Notes in Computer Science, vol 8811. Springer, Cham.

11. Fernando De la Torre and Jeffrey F. Cohn, (2011) Facial Expression Analysis. In: Moeslund T., Hilton A., Krüger V., Sigal L. (eds) Visual Analysis of Humans. Springer, London.

12. Hildebrand M, 'Profiling from data to knowledge the challenges of a crucial technology [2006] 30(9) Datenschutz und Datensinchercheit. Available at https://pdfs.semanticscholar.org/c0a1/aa843e812925127dfb8f9540089e1a0a72b5.pdf.

13. Huang, T., Xiong, Z., & Zhang, Z. (2011). ‘Face recognition applications. Handbook of Face Recognition’ https://doi.org/10.1007/978-0-85729-932-1

14. Jang, E. H., Park, B. J., Park, M. S., Kim, S. H., & Sohn, J. H. (2015). Analysis of physiological signals for recognition of boredom, pain, and surprise emotions. Journal of physiological anthropology, 34(1), 25. Available online: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4490654/ >

15. Jennifer Lynch, ‘What Facial Recognition Technology Means for Privacy and Civil Liberties’ [2012] SSRN Electronic Journal 9.

16. Kamenskaya, E & Georgy, Kukharev. (2008). ‘Recognition of psychological characteristics from face’Available online: https://pdfs.semanticscholar.org/b85f/c769fe5624fa1402d23f6e1cc45f555d635b.pdf

17. Karl de Leeuw, Jan Bergstra, ‘The History of Information Security: A Comprehensive Handbook’ (Published Date: 28th August 2007).

18. Lewinski Peter and others, ‘Face and Emotion Recognition on Commercial Property under EU Data Protection.’ Psychology & Marketing, Wiley Periodicals 729-746. Available at, https://onlinelibrary.wiley.com/doi/abs/10.1002/mar.20913

19. M Turk, ‘A Random Walk through Eigenspace’ [2001] IEICE Transactions on Information and Systems.Available online: <http://cs.ucsb.edu/~mturk/pubs/TurkIEICE2001.pdf >

20. O'Connor, Sean. (2002). Biometrics and Identification after 9/11. SSRN Electronic Journal. 10.2139/ssrn.299950.

21. Pankaj Sareen, ‘Biometrics- Introduction, characteristics, basic technique, its type and various performance measures’ Int J Emerg Res Manage Technol 2014, p,109

22. S Huang, T., ‘Computer Vision: Evolution and Promise’ (2018). <https://cds.cern.ch/record/400313/files/p21.pdf>

23. Selvapriya.M , Dr.J.KomalaLakshmi, (International Journal Of Engineering And Computer Science, Volume 3 Issue 12 December 2014) Available online : <https://www.ijecs.in/index.php/ijecs/article/download/1662/1538/>

24. Solove Daniel, 'A TAXONOMY OF PRIVACY' [2006] 154(3) University of Pennsylvania Law Review. Available at, https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf

25. Takeo Kanade, (23 May 1974), ‘Picture processing system by computer complex and recognition of human faces’ Available online: <https://repository.kulib.kyoto-u.ac.jp/dspace/bitstream/2433/162079/2/D_Kanade_Takeo.pdf >

26. Terry Hutchinson and Nigel Duncan, ‘Defining and Describing What We Do : Doctrinal Legal Research’ (2012) 17(1) Deakin Law Review.

27. Welinder, Yana, A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks (July 16, 2012). Harvard Journal of Law and Technology, Vol. 26, No. 1, 2012. Available at SSRN: https://ssrn.com/abstract=2109108 or http://dx.doi.org/10.2139/ssrn.2109108

28. Yana Welinder, (Santa Clara High Technology Law Journal, 2013) 'Facing Real-Time Identification in Mobile Apps &amp: Wearable Computers' page. 94 Available online: <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1577&context=chtlj>

29. Yaniv Taigman and others, 'DeepFace: Closing the Gap to Human-Level Performance in Face Verification'.Available online : <https://www.cs.toronto.edu/~ranzato/publications/taigman_cvpr14.pdf >

30. Yasin Yilmaz, Alfred O. Hero (3 August 2015) "Multimodal factors enable a powerful means of clustering based on a diverse set of observations.", https://arxiv.org/abs/1508.00408

31. Sentiment Analysis: Detecting Valence, Emotions, and Other Affectual States from Text" Saif M. Mohammad, Emotion Measurement 2015 Available at: https://pdfs.semanticscholar.org/12f8/11a52e5a786f556598c99c560ee3539ad684.pdf Accessed

Article 29 WP opinions

32. The Article 29 Data Protection Working Party, 5062/01/EN/Final WP 48, Opinion 8/2001 On the Processing of Personal Data in The Employment Context, Adopted on 13 September 2001.

33. The Article 29 Data Protection Working Party, 5401/01/EN/Final WP 55, Working Document on The Surveillance of Electronic Communications in The Workplace, Adopted on 29 May 2002.

34. The Article 29 Data Protection Working Party, 00323/07/EN WP 131, Working Document on the processing of personal data relating to health in electronic health records (EHR), Adopted on 15 February 2007.

35. The Article 29 Data Protection Working Party, 01197/11/EN WP187, Opinion 15/2011 on the definition of consent, Adopted on 13 July 2011.

36. The Article 29 Data Protection Working Party, 00727/12/EN WP 192, Opinion 02/2012 on facial recognition in online and mobile services, Adopted on 22 March 2012.

37. The Article 29 Data Protection Working Party, 00720/12/EN WP193, Opinion 3/2012 on developments in biometric technologies, Adopted on 27th April 2012.

38. The Article 29 Data Protection Working Party, 844/14/EN WP 217, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on 9 April 2014.

39. The Article 29 Data Protection Working Party, 17/EN WP 249, Opinion 2/2017 On Data Processing at Work, Adopted on 8 June 2017.

40. The Article 29 Data Protection Working Party, 17/EN WP251rev.01, Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016\679, Adopted on 3 October 2017, as last Revised and Adopted on 6 February 2018.

41. Article 29 Data Protection Working Party, 17/EN WP259, Guidelines on Consent under Regulation 2016/679, Adopted on 28 November 2017

Legislation

42. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on The Protection of Natural Persons with Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, And Repealing Directive 95/46/EC (General Data Protection Regulation), (27 April 2016)

Case Law

43. Köpke v Germany, App no. 420/07 (ECHR, 5 October 2010)

44. Spanish Constitutional Court, 39/2016 "Bershka", (Victor Bescós, (Pragma International, 24 January 2018) Dismissal with Video Surveillance as Supporting Evidence, Has it Changed Case-law?<‘http://pragma.international/article/dismissal-with-video-surveillance-as-supporting-evidence-has-it-changed-case-law)

45. Register of measures n. 551 of 21 December 2017, Doc. web n. 7496252, Installation of "digital signage" promotional devices (also called Totems) at a railway station - 21 December 2017. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252

Websites/Blogs/Reports

46. Alex Hern and David Pegg , (The Guardian, 11 July 2018) ‘Facebook fined for data breaches in Cambridge Analytica scandal ’ https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal

47. Amber Tenuta, (NY Times, 29 June 2017) ‘5 Benefits of Facial Recognition Time Tracking Solutions’ http://blog.epaysystems.com/5-benefits-of-facial-recognition-time-tracking-solutions

48. Ava Kofman, ‘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/>

49. BBC News, (24 July 2017), ‘Wisconsin company Three Square Market to microchip employees’ <https://www.bbc.com/news/world-us-canada-40710051>

50. Ben Virdee-Chapman, (Kairos, 26 May 2016) ‘5 Companies Using Facial Recognition to Change The World’ <https://www.kairos.com/blog/5-companies-using-facial-recognition-to-change-the-world>

51. Bryan Pearson, (Forbes, 15 March 2018) <https://www.forbes.com/sites/bryanpearson/2018/03/15/3-ways-retailers-can-use-facial-recognition-to-express-better-experiences/#794793541766>

52. Center for democracy & technology, Facial Recognition & Privacy: An Eu-Us Perspective October 8, 2012. Available online: https://www.cdt.org/files/pdfs/CDT_facial_recog.pdf

53. Data Protection Commissioner, 'Press Release on the use of Facial Detection Technology in Advertising'' (15 May 2017) Available online: < https://www.dataprotection.ie/documents/Facialdetection.pdf>

54. David Berreby,(The Guardian, 3 March 2017) 'Click to agree with what? No one reads terms of service, studies confirm' <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print >

55. David Fulton, (Information- Age, 11 May 2018) 'How facial recognition could save insurance companies billions' Available online: < https://www.information-age.com/how-facial-recognition-could-save-insurance-companies-billions-123472478/ >

56. Don Reisinger, 'Amazon's Facial Recognition Linked the Faces of 28 Members of Congress to Mugshots' (Fortune, July 26, 2018) http://fortune.com/2018/07/26/amazon-facial-recognition-mugshots/

57. Ellen O'Brien, (Data Guidance, 1 February 2018) 'Italy: Garante's decision on digital signage "correctly balances parties' interests" < https://www.dataguidance.com/italy-garantes-decision-digital-signage-not-easy-one/ >

58. Face Recognition Technology (FERET) Explanation of the project, Available online: <https://www.nist.gov/programs-projects/face-recognition-technology-feret>

59. Face Recognition Vendor Test (FRVT) Explanation of the project, available online: < https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt>

60. Guidelines for De-identification of Personal Data, June 30, 2016, Office for Government Policy Coordination | Ministry of Interior, Korea Communications Commission | Financial Services Commission Ministry of Science, ICT and Future Planning | Ministry of Health and Welfare

61. IBM Official Website<https://www.ibm.com/nl-en/marketplace/ibm-connections

62. installazione di apparati promozionali del tipo "digital signage" (definiti anche totem) presso una stazione ferroviaria - 21 dicembre 2017 [7496252] Available online:<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252>

63. Internet.org. 'A focus on efficiency: A whitepaper from Facebook, Ericsson and Qualcomm' (13 September 2013.). Retrieved May 20, 2015 Available online:< https://www.parool.nl/rest/content/assets/1368f07e-16b8-415d-bd3a-a4046f2fa9bd >

64. Janene Pieters, (20 February 2018) 'Dutch Cops Used Facial Recognition to Id 93 Suspects' <https://nltimes.nl/2018/02/20/dutch-cops-used-facial-recognition-93-suspects>

65. Jena McGregor, (The Washington Post, 4 April 2017) 'Some Swedish workers are getting microchips implanted in their hands' <https://www.washingtonpost.com/news/on-leadership/wp/2017/04/04/some-swedish-workers-are-getting-microchips-implanted-in-their-hands/?noredirect=on&utm_term=.3ebaa81eaa33>

66. Justin Brookman, (CDT, 16 June 2015) 'CDT Withdraws from the NTIA Facial Recognition Process' <https://cdt.org/blog/cdt-withdraws-from-the-ntia-facial-recognition-process/ >

67. Justin Lee, (Biometric Update, 9 February 2017) 'MasterCard to launch facial recognition payment app in Australia' <http://www.biometricupdate.com/201702/mastercard-to-launch-facial-recognition-payment-app-in-australia>

68. Kanjoya official website. https://www.ultimatesoftware.com/Kanjoya-is-now-Perception

69. Kashmir Hill, (Forbes, 1 September 2011) 'Kraft To Use Facial Recognition Technology to Give You Macaroni Recipes' <https://www.forbes.com/sites/kashmirhill/2011/09/01/kraft-to-use-facial-recognition-technology-to-give-you-macaroni-recipes/#6ccf03bc5390>

70. Katharine Schwab, 'Facial Recognition Systems Are Even More Biased than We Thought' (Fact Company, 13 February 2018) https://www.fastcompany.com/90160327/facial-recognition-systems-are-way-more-biased-that-we-thought

71. Kaveh Waddell (The Atlantic, 29 September 2016) "The Algorithms That Tell Bosses How Employees Are Feeling" < https://www.theatlantic.com/technology/archive/2016/09/the-algorithms-that-tell-bosses-how-employees-feel/502064/>

72. Lauren C.Williams, (Think Progress, and 23 June 2015) 'Facial Recognition Is the New Normal, Even When Your Face is covered' https://thinkprogress.org/facial-recognition-is-the-new-normal-even-when-your-fa

73. Lydia DePillis, (The Washington Post, 25 November 2015) <https://www.washingtonpost.com/news/wonk/wp/2015/11/25/people-are-suing-more-than-ever-over-wages-and-hours/?utm_term=.41b15d00b126>

74. Maggie Astor, July 25, 2017, Microchip Implants for Employees? One Company Says Yes https://www.nytimes.com/2017/07/25/technology/microchips-wisconsin-company-employees.html

75. Mathew Wall, 'Is facial recognition tech really a threat to privacy?' (BBC Technology, 19 June 2015) Available at, https://www.bbc.com/news/technology-33199275

76. National Telecommunications and Information Administration, United States Department of Commerce Publication, (17 June 2016) 'Privacy Multistakeholder Process: FRT' <https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology >

77. Nicholas Jackson, (The Atlantic, 16 December 2010), ‘Facebook Will Start Using Facial Recognition Next Week’ Available online: < https://www.theatlantic.com/technology/archive/2010/12/facebook-will-start-using-facial-recognition-next-week/68121/>

78. Official Website of De-Identification <https://www.deidentification.co/#footer >

79. Official website of Defense Advanced Research Projects Agency, Available online:< https://www.darpa.mil/>

80. Official website of the National Institute of Standards and Technology, Available online:< https://www.nist.gov/>

81. Paul Monckton (Forbes, 29 January 2018) ‘New AI Tech Blinds Computer Facial Recognition Systems’<https://www.forbes.com/sites/paulmonckton/2018/01/29/d-id-defeats-facial-recognition/#be5d4b334b0d>

82. Phil Lee (FieldFisher, 12September 2016) ‘The nuance of "accepting" vs. "reading" a privacy policy’ <https://privacylawblog.fieldfisher.com/2016/the-nuance-of-accepting-vs-reading-a-privacy-policy>

83. Press Releases, Digital Signage Market worth 32.84 Billion USD by 2023, The report "Digital Signage Market by Product < https://www.marketsandmarkets.com/PressReleases/digital-signage.asp>

84. Privacy advocates statement on NTIA facial recognition process, (16 June 2015) Available at <https://www.dropbox.com/s/g7cdhl66p5um7dn/Privacy%20advocates%20statement%20on%20NTIA%20facial%20recognition%20process%20-%20FINAL.pdf?dl=0>

85. Rachael King, (The Wall Street Journal,13 October 2015) ‘How Do Employees Really Feel About Their Companies? < https://www.wsj.com/articles/how-do-employees-really-feel-about-their-companies-1444788408>

86. Rick Ferguson, (RetailWire, 9 January 2018) ‘Facial recognition software comes to loyalty’< https://www.retailwire.com/discussion/facial-recognition-software-comes-to-loyalty/ >

87. Russell Brandom (7 July 2014) ‘Why Facebook is beating the FBI at facial recognition ‘Available online: https://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition

88. Sean Hargrave (The Guardian, 17 August 2016) https://www.theguardian.com/media-network/2016/aug/17/facial-recognition-a-powerful-ad-tool-or-privacy-nightmare>

89. Shan Li and David Sarno (Los Angeles Times, 21 August 2011) ‘Advertisers start using facial recognition to tailor pitches’ <http://articles.latimes.com/2011/aug/21/business/la-fi-facial-recognition-20110821>

90. Swedish Company Biohax International Offcial Website https://www.biohax.tech/

91. Tom Cheshire (SKY News, 18 October 2017) ‘Piccadilly Circus lights facial detection system 'incredibly intrusive'’ <https://news.sky.com/story/piccadilly-circus-lights-facial-detection-system-incredibly-intrusive-11087020 >

92. United States Senate, Committee on Commerce, Science, and Transportation. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller, December 18, 2013. Available at <https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf >

93. Victor Bescós, (Pragma International, 24 January 2018) Dismissal with Video Surveillance as Supporting Evidence, Has it Changed Case-law?<‘http://pragma.international/article/dismissal-with-video-surveillance-as-supporting-evidence-has-it-changed-case-law>

94. Website of the quividi. https://quividi.com/

95. Will Knight, ‘Face-detecting systems in China now authorize payments, provide access to facilities, and track down criminals. Will other countries follow?’ (MIT Technology Review, 22 February 2017) <https://www.technologyreview.com/s/603494/10-breakthrough-technologies-2017-paying-with-your-face/ >

96. Woodrow Wilson Bledsoe, (January 1963) ‘A Facial Recognition Project Report’, Available online: https://archive.org/details/firstfacialrecognitionresearch