University of Twente, Enschede, the Netherlands
Faculty of Behavioural, Management and Social Sciences
Public Governance across Borders
Bachelor Thesis

Beyond Data Protection: Applying the GDPR to Facial Recognition Technology

A comparative case analysis

Ellen Tangerding
30.06.2021
Word Count: 11999

Abstract

The use of facial recognition technology [FRT] poses various societal challenges particularly regarding the current data protection legal system of the EU. This research identifies these challenges and elaborates the following research question: *To what extent is the use of facial recognition technology for non-law enforcement purposes compatible with the EU's current legislative framework?*

Following a mainly comparative but also argumentative approach three different cases of EU member states regarding the use of FRT and their respective regulatory approach to FRT will be analyzed. In doing so, the theoretical focus of this thesis lies on the one hand, on the two fundamental rights to privacy and data protection as constituted in the European Convention on Human Rights and the Charter of Fundamental Rights and, on the other hand, on the EU's data protection principles laid out in Art. 5 GDPR. In principle, FRT use can be compatible with the GDPR if certain requirements are met. In practice, however, the GDPR leaves a lot of room for interpretation and discretion with the EU member states which facilitates an unequivocal regulatory environment and a highly complex, time-consuming, and inscrutable case-to-case assessment of FRT use throughout the EU.

Abbreviations

AEPD -	Agencia Española Protección Datos [Spanish Data Protection Agency]
AI -	Artificial Intelligence
CCTV -	Closed Circuit Television
CFR -	European Charter of Fundamental Rights
CJEU -	European Court of Justice
CoE -	Council of Europe
DPA -	Data Protection Authority
DPC -	Ireland Data Protection Commission
DPIA -	Data Protection Impact Assessment
ECHR -	European Convention of Human Rights
ECtHR -	European Court of Human Rights
EU -	European Union
FOI -	Freedom of Information Request
FRT -	Facial Recognition Technology
GDPR -	General Data Protection Regulation
ICCL -	Irish Council for Civil Liberties
IDPA -	Irish Data Protection Act
LFR -	Live Facial Recognition
LOPD -	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales [Spanish Data Protection Law]
MS -	European Union Member States
NCH -	Ireland’s New Children’s Hospital
NPHDB -	National Paediatric Hospital Development Board

Table of Contents

1. Introduction

In early 2020 information was revealed that the municipality of Como in Italy purchased a facial recognition system from Huawei using public money (Carrer et al., 2020a,b). Public knowledge about the ongoing implementation of this system and overall transparency has been extremely limited. The purpose of the video surveillance system that had been installed in the Tokamakhi Park in Como was to identify natural persons walking through that park (GPDP, 2020). Prior to implementing this system, pursuant to Art. 35 GDPR the municipality conducted a data protection impact assessment [DPIA]. However, it did not consider the highly intrusive functions of facial recognition technology [FRT] and its implications for people's rights in its assessment (Carrer et al., 2020a,b). Following, on February 26th the Italian data protection authority [DPA] issued a decision declaring that the usage of the FRT system in Como happened without a legal basis and therefore, had to be suspended immediately (GPDP,2020). The suspension, however, came months after the system had already been used extensively (Carrer et al., 2020b). This case of FRT use in Como shows how controversial technologies such as FRT with pervasive social implications are loosely implemented across the EU without or only limited judicial supervision.

In Europe law-enforcement, private companies, and governments have introduced FRT to identify, profile, and surveil citizens often without public consultation, debate, or transparency. Still, the application possibilities of FRT are far broader and complex than it is widely known by citizens which makes the current debate about the use of FRT highly controversial and complex (EDRi, 2019). Often the benefits of using FRT are framed in terms of increased efficiency, crime prevention and public security. However, there are various dangers and problems of using FRT. Especially its highly invasive nature has the potential to severely infringe and endanger fundamental rights, civil liberties, and democratic freedoms far beyond data protection.

FRT is primarily regulated by the EU's GDPR which came into effect in 2018 and "although there was no great debate on facial recognition during the passage of negotiations on the GDPR […] the legislation was designed so that it could adapt over time as technologies evolved"(Wiewiórowski, 2019). The GDPR is directly applicable in the member states [MS] and for the first time provides a definition of 'biometric data' in Art. 4 (14). While generally the processing of biometric data is prohibited under Art. 9 (1), there are several exceptions to this prohibition regulated under Art. 9 (2). Still, neither the GDPR specifically addresses FRT nor does any other legislative act of the EU. This creates interpretation problems and differences across EU MS, especially regarding adequate regulation of distinct purposes of FRT use. Also, the unclear definitions of public and private spaces in the law create substantial problems. "Biometrics do […] pose a challenge to the current legal framework currently governing the handling of personal data or personal particulars"(Sprokkereef, 2008, p.279).

Not only the municipality of Como in Italy has been using FRT systems, but most EU MS already use FRT (Gosh, 2020). Schools in Sweden and France used FRT to monitor their staff and students, nonetheless, these projects were later stopped by the national data protection authorities (EDPB, 2019; LQDN, 2020). In Spain a major supermarket company is currently investigated for its FRT use (Navas, 2021), whereas a hospital in Ireland albeit still in construction announced that it will be using FRT (Rollet, 2019). All these examples show that there are several initiatives promoting and using FRT whilst the regulatory framework does not seem to address the matter unequivocally. Particularly it appears that the GDPR facilitates a highly complex, time-consuming, and inscrutable case-to-case assessment of FRT use.

1.1. Research question(s)

Looking at cases from different EU member states, this research tries to answer the following research question:

To what extent is the use of facial recognition technology for non-law enforcement purposes compatible with the EU's current legislative framework?

The choice to leave out considerations regarding the use of FRT in a law-enforcement context was made due to the limited scope this thesis. To answer this research question several sub-questions are developed:

SQ 1: To what extent does the GDPR legitimize FRT use for non-law enforcement purposes in public and private spaces?

SQ 2: To what extent is an absolute ban on FRT the only solution to data protection and privacy rights?

SQ 3: How have national governments in the EU been regulating the application of FRT in public spaces for non-law enforcement purposes?

SQ 4: How have national governments in the EU been regulating the application of FRT in private spaces for non-law enforcement purposes?

1.2. Research design and scientific approach

This thesis is a qualitative legal research. It will mainly follow a comparative approach analyzing three different cases of EU member states regarding their respective regulatory approach to FRT. Along this comparative case analysis an argumentative approach is also followed. In doing so, different principles and considerations laid out in the theoretical legal framework will be applied to examine the conditions under which the application of FRT systems is compatible with the EU's legislative framework. To answer the main research question and the four sub-question this thesis is divided into six chapters. Chapters 3, 4, and 5 explore three identified problem dimensions of FRT usage: banning, public, and private use. In the first chapter the overall topic and issue at hand is introduced followed by an explanation of the five most important concepts used in this analysis and ending with the theoretical legal framework laying out the broader backdrop of FRT in a legal context. Chapter 2 will then introduce the EU's legislative framework surrounding FRT. A tabular overview of this chapter is provided in the appendix. This table will inform the following analyses. Chapter 3 deals with the special case of Belgium analyzing those provisions of its data protection law banning FRT use. Chapter 4 deals with the case of intended FRT use in an Irish hospital. This analysis will focus on the legal provisions regulating the use of FRT in public spaces. Focusing on private spaces, Chapter 5 will analyze the case of a Spanish supermarket. This thesis will end with an overall conclusion in which the main research question will be answered.

1.3. Key concepts

This section will define the five key concepts used in this thesis and necessary to conduct the research.

1.3.1. Biometric data

According to Art. 4 (14) of the GDPR biometric data "means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

1.3.2. Facial recognition technology

The term 'Facial Recognition' refers to a multitude of technologies and applications.

> "Using your face to unlock your mobile phone, using a shop or a bar's security camera footage to match against a watchlist of possible shoplifters, checking someone's age when buying alcohol at self-checkouts, or using an airport e-passport gate"(Brennan, 2019).

FRT is a form of artificial intelligence [AI] (Condie & Dayton, 2020) generally "used to identify people's faces based on datasets and then makes assessments about those people based on algorithmic predictions"(Dushi, 2020, p.3). Nowadays, "biometric facial recognition is one of the most significant and rapidly developing artificial intelligence technologies currently available"(Condie & Dayton, 2020, p.126). FRT can be deployed in almost every dimension of our lives from banking and commerce to transportation and communication (EPIC, n.d.). "Biometric facial recognition systems can be integrated with the closed circuit television systems [CCTV; author's note] that already exist in public and private spaces to identify people in real time"(Smith & Miller, 2021, p.2)

A distinction is made between three key analytics of FRT systems: verification, identification, and classification (Dushi, 2020). Verification refers to the process of one-to-one matching which is a comparison between two face templates to determine whether they are from the same person (FRA, 2020). Identification is the process of one-to-many comparison meaning that one face template is compared with a dataset of many face templates in order to find out whether that person is stored in the dataset (FRA, 2020). There is, however, a distinction between the positive identification of an unknown person (face template is checked against the database - no matching face is found - person is identified as a new person in the dataset) and the calculation of a probability match score with a template already stored in the dataset (Electronic Frontier Foundation [EFF], n.d.). Classification refers to the process of 'face analysis' meaning the categorization of a person's general characteristics (FRA, 2020). This type does not necessarily include the identification or verification of a person. To execute these three analytics FRT systems extract and process biometric data and create a biometric template of people's faces, or 'face template'(FRA, 2020.). To create such a template, the algorithm checks for distinctive details about a person's face like the distance between the eyes or the shape of their chin (EFF, n.d.).

There are some challenges for the algorithm to create a template. These include poor lighting conditions, low quality image solutions, and a suboptimal angel of view (EFF, n.d.). An additional problem of FRT are the 'false positives'(system matches the face to an existing one in the dataset but the match is actually incorrect) and 'false negatives' (systems does not match the face to an existing template in the dataset but the face is actually already in the dataset). Whereas the 'false positives' should be handled more carefully because the consequences of being falsely identified are far more serious (EFF, n.d.). Another problem are biases implemented through training data leading to discrimination against people. "Facial-recognition systems are trained using a vast number of images to create 'faceprints' of people by mapping the geometry of certain facial features"(Condie & Dayton, 2020, p.126). However, often these datasets used to train the AI are overwhelmingly white and male which leads to identification, verification, and classification errors of the system (Condie & Dayton, 2020). So far, several studies found that African-American and Asian faces were "misidentified 10 to 100 times more often than Caucasian men" and the systems also have severe problems identifying women (Condie & Dayton, 2020, p.126).

Of special interest in the following chapters is 'live facial recognition' [LFR]. This deployment form of FRT refers to the (near) real-time scanning of faces through video cameras (Brenna, 2019). LFR is often criticized for having a lower rate of accuracy compared to non-live FRT usage which can result in additional risks for people whose faces are being recognized (EDRi, 2019). These risks are further amplified as LFR enables immediate action (e.g., instant ban on entering a supermarket).

1.3.3. Non-law enforcement purpose

According to Dushi, law-enforcement purposes relate to data processing by competent authorities with the aim of "prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" (2020, p.6). This paper only considers incidents that fall outside this scope, and thus, solely under the scope of the GDPR.

1.3.4. Public space

The distinction between public and private spaces is not well-defined in the law. In this paper the understanding of public and private spaces is based on three key elements: access, property, and interest. Public spaces are open spaces which are free and accessible to the public without major restrictions, owned by a public authority (e.g. municipality) and serve a public interest (Glasze, 2001, p.161).

1.3.5. Private space

In contrast to that, a private space is a generally closed space owned by a private enterprise which can be open to the public due to an economic, commercial, or otherwise private interest (Birch, 2008). The demarcation between public and private spaces can sometimes be rather vague. However, in this paper the emphasized main difference between public and private spaces is the distinction of property (publicly versus privately owned).

1.4. Theoretical legal framework

In the following part the theoretical legal framework regarding biometric data and FRT is examined. This part will start by examining the right to privacy as laid out in the ECHR and the CFR. It will then go on examining the right to data protection and explain the proportionality principle in light of FRT and biometric data. It will end with the EU's key data protection principles.

> "The ability of face recognition technology to track people's location and movements raises many privacy concerns. When this tracking is associated with storing and processing these data, it raises many concerns about personal data protection too"(Dushi, 2020, p.6).

The right to privacy is laid down in Art. 8 ECHR and Art. 7 CFR. Both these articles provide everyone with the right to respect for his or her private and family life, home, and communications. Furthermore, this right to privacy has been and still is protected as a general principle of EU law (Kokott & Sobotta, 2013). The CJEU interprets this jurisprudence as 'private life' including the protection of personal data, which is any information relating to an identifiable or unidentifiable individual (Kokott & Sobotta, 2013, p.223). In Rotura v Romania the ECtHR decided that the collection, storage, or disclosure of information relating to private life interferes with the right to privacy (Kokott & Sobotta, 2013). Any such interference requires a solid justification. Art. 8 ECHR provides that the interference must be in accordance with the law, must pursue one or more legitimate aims, and it must be necessary in a democratic society to achieve those aims. The 'In accordance with the law' requirement means that any interference must be foreseeable and must lay down the limits of the data collection particularly the protection measures against abuse and disproportionate use (Sprokkereef, 2008). With regards to the 'legitimate aim' Art. 8(2) ECHR lays down a limited list of permissible aims: national security; public safety; economic well-being of the country; prevention of disorder or crime; protection of health or morals; or the protection of the rights and freedoms of others. Regarding the 'necessary in a democratic society' condition the ECtHR maintains that "any interference must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim or aims pursued"(Kokott & Sobotta, 2013, p.225).

Possibly, FRT not only infringes the fundamental right to privacy but also the right to data protection. Distinct to the right of privacy Art. 8 CFR provides the fundamental right of data protection which is "unique to the European legal order, being absent from other international human rights instruments"(McDermott, 2017, p.1). The right to data protection is also laid down in Art. 16 TFEU as a general principle of the EU. The scope of the data protection right is broader than the one of the rights of privacy (FRA & CoE, 2018). However, similar interferences with this right also need justification. Art. 8(2) CFR states that personal data must be processed fairly for specified purposes and based on the consent of the person concerned or on some other legitimate basis laid down by law. Just as with the right to privacy there is a purpose-binding principle implied to avoid a 'function creep' of FRT. Additionally, it is possible that one does not interfere with the right to data protection but still interferes with the right to privacy. Therefore, to avoid an interference with any fundamental right the three-level test developed by the ECtHR (legitimate aim, in accordance with the law, and necessary in a democratic society) mentioned above also applies to data protection. Art. 52(1) CFR provides general limitations to and justifications for any interferences. It states that limitations must be provided for by law, must respect the essence of the affected right and, subject to the principle of proportionality, must be necessary and genuinely meet the objectives of general interest recognized by the European Union or the need to protect the rights and freedoms of others. In other words, any interference must be clearly defined, necessary, and proportionate.

This leads to the third aspect of this theoretical legal framework necessary for the following analyses: the proportionality principle. The proportionality principle is a general legal principle in Union law. "It has been developed *inter alia* in the domain of administrative law, human rights law, Union law, international law, penal law and labor law"(Kindt, 2013, p.405). The proportionality principle has become increasingly important in data protection legislation (Kak (eds.), 2020). This principle provides that the "means used are suitable and not going beyond what is necessary to achieve the pursued objectives, without a substantial (adverse) impact on other interests involved"(Kindt, 2013, p.404). In other words, the two conditions under the proportionality principle are appropriateness and necessity. Furthermore, this principle applies in combination with the legality and legitimacy conditions mentioned above. Concerning FRT, Kindt stated that "the crucial and also most difficult question in the debate about biometric data systems and applications is whether the use of the biometric characteristics in an automated system is proportionate and necessary"(2013, p.564). However, at the same time it is clear that applying the proportionality principle to FRT is a difficult task "because few criteria relevant for biometric data processing are clearly set forth in regulation or are agreed upon in guidelines or opinions"(Kindt, 2013, p.567). This in turn substantially reduces the legal certainty for data controllers and data subjects. National data protection authorities are including proportionality consideration in their assessment of biometric data usage, but their opinions and guidelines are often difficult to understand and "contain confusing recommendations for the checks for the necessity and/or proportionality of biometric systems"(Kindt, 2013, p.567). Applying the proportionality principle as well as the legality and legitimacy requirements to biometrics leaves much room for discretionary policy considerations and unpredictable outcomes"(Kindt, 2020, p.63).

The key principles of EU data protection law constitute the fourth aspect of this theoretical legal framework. These are set out in Art. 5 GDPR and govern all kinds of processing of personal data. "Any exemptions from and restrictions to these key principles may be provided for at EU or national level; they must be provided for by law, pursue a legitimate aim and be necessary and proportionate measures in a democratic society. All three conditions must be fulfilled"(FRA & CoE, 2018, p.116). The first principle is the lawfulness principle. Laid out in Art. 5 (1)(a)[1] this principle requires the consent of the data subject or another legitimate ground provided. The second principle, fairness of processing, requires that the data subject "must be informed of the risk to ensure that processing does not have unforeseeable negative effects"(FRA & CoE, 2018, p.117). The transparency principle requires that data must be processed in a transparent manner. This includes among others that the data subject is informed about the processing, its extent and purpose, who the processer is, and the right to access all their processed data (FRA & CoE, 2018). The purpose limitation principles laid out in Art. 5 (1)(b)[2] is the fourth principle. Purpose limitation requires that any processing must be for a specific, well-defined, and legitimate purpose which has to be defined before processing starts. Any further processing incompatible or beyond the original defined purpose is not allowed. The fifth principle, data minimization, requires that the data processing must be limited to what is necessary and appropriate to

[1] "Personal data shall be: processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

[2] collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

fulfill the purpose (Art. 5 (1)(c)[3]). Art. 5 (1)(d)[4] provides the sixth principle, the data accuracy principle. It requires that the data controller is responsible to assure the correctness of all processed data. This has to be implemented in all steps of processing, regularly checked, kept up to date, and any inaccurate or incorrect data has to be deleted immediately. Storage limitation, the seventh principle, means that data which is no longer necessary for the original purpose of the processing must be deleted or anonymized (Art. 5 (1)(e)[5]). The eighth principle is the data security (confidentiality and integrity) principle set up in Art. 5 (1)(f)[6]. It requires that the data controller must take appropriate technical or organizational security measure to prevent any adverse effects for the data subject. Accountability, laid out in Art. 5 (2)[7], is the last principle and states that the data controller and processor are responsible to actively and continuously implement the other eight seven principles to ensure data protection. Furthermore, processors and controller must be able to prove compliance at any time.

2. The legislative framework of FRT

The following part examines the legislative framework of the EU regulating FRT. The most important provisions of existing EU law will be examined. In doing so, the first sub-question of this thesis will be answered. Appendix A provides a tabular overview of this chapter.

First and foremost, it is to say that there is currently no EU law directly addressing and regulating FRT. However, since FRT is based on the processing of biometric data (cf. section 1.3.2.) the GDPR applies to this type of technology. Since May 25th, 2018 the GDPR applies directly in all EU MS. The GDPR is a binding EU regulation. The legal basis of the GDPR can be found in Art. 16 TFEU which lays down the mandate of the EU for what regards the right to privacy and data protection. Thus, the GDPR can be seen as the fulfillment of this mandate. The personal scope of the GDPR includes all private actors established and public institutions operating in the EU as well as controllers and processors not established in the EU that offer goods or services to data subjects in the EU (FRA, 2020). Its material scope comprises all automated processing of personal data in the European Economic Area and processing of personal data by any other means which form part of a filing system, within the scope

[3] adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

[4] accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

[5] kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

[6] processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

[7] "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

of EU law (FRA, 2020). This also means that the GDPR is not applicable to national security-related data processing (FRA, 2020). Appendix A provides a tabular overview of this chapter.

2.1. Biometric data processing

The GDPR is the first legislative instrument of the EU to define the notion of biometric data (cf. Art. 4 (14) GDPR[8]). Noteworthy here is the notion of "specific technical processing". This condition of Art. 4 (14) "effectively excludes 'raw' data stored and retained in databases (e.g., of facial images captured on CCTV, voice recordings, or fingerprints)"(Kindt, 2020, p.64). Furthermore, the GDPR accounts mention that the "processing of photographs should not systematically be considered to be processing of special categories of personal data"(Rec. 51 GDPR). "Video footage of an individual is also not considered biometric data as long as it has not been specifically technically processed in order to contribute to the identification of the individual"(Kindt, 2020, p.64).

The details about the processing of biometric data are laid out in Art. 9 GDPR. Art. 9 (1)[9] provides a general prohibition of the processing of special categories of personal data such as biometric data "for the purpose of uniquely identifying a natural person". Same as the condition in Art. 4 (14) this purpose-binding component of Art. 9 limits the scope of the general prohibition of processing biometric data. For example, the process of verification as explained in section 1.3.2. does not fall directly under the scope of Art. 9 because this function does not uniquely identify a person. Problematic here is that

> "decision makers, if non-experts, may not ascertain the (technical) difference between identification and verification or be able to understand in particular cases which functionality is used. In both cases, information is collected and compared, while the place of storage is far less understood or visible"(Kindt, 2017, p.6).

The process of identification requires a pre-existing biometric database whereas, verification does not need such a database[10]. This difference in the data storage is of key importance adequately regulate different uses of FRT.

The prohibition exists because biometric data is considered to be inherently sensitive because they "may unduly discriminate or stigmatize if processed"(Kindt, 2017, p.4). Art. 9 (1) implies that "all entities falling under the material scope of the GDPR, including public authorities, governments, and private organizations, are in principle not allowed to process biometric data for 'unique identification'. For example, a shopping mall would in principle not be entitled to identify troublemakers by using a

[8] "biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;"

[9] "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

[10] For definitions of these different functionalities see also ISO/IEC 2382-37:2017 – Information Technology – Vocabulary – Part 37: Biometrics.

biometric comparison"(Kindt, 2017, p.4f). For law-enforcement authorities a distinct regime applies, namely the EU Directive 2016/680.

2.2. Exceptions to the general processing prohibition

If the processing of biometric data by any controller still falls under the scope of Art. 9 (1), Art. 9 (2) lays down several exceptions. There are ten exceptions in total, with the most important ones for this thesis elaborated in the following. Art. 9 (2) a)[11] provides an exception to the general prohibition when the data subject has given explicit consent to the processing of their personal data. This exception is however, for several reasons problematic when applied to real-life circumstances. For example, a question that could arise is whether the choice of going into a place which is open to the public is equal to a free, informed, and specific explicit consent given that the required legal information about the biometric identification is provided. In other words, what exactly is 'explicit consent'? This is especially controversial regarding FRT since these systems are often employed in public or open private spaces with little public knowledge and without data subjects being able to opt-out. Art. 7 (2)[12] can be of help in this regard because it provides the conditions for giving consent to data processing. However, this article is not exhaustive and cannot absolutely resolve the before posed question. Art. 9 (2) e)[13] is a particularly interesting exception because it provides a permission to process biometric data with the purpose of uniquely identifying a natural person if the data subject has manifestly made the data public. Potentially, this exception could allow for face recognition even without explicit consent or law stating a substantial public interest. The 'substantial public interest' exception is laid down in Art. 9 (2) g)[14] stating that processing of biometric data is allowed if it is "necessary for reasons of substantial public interest". Additional conditions of this article are that the processing must be "proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interest of the data subject". However, unclear remains what exactly constitutes a 'substantial public interest' and what kind of measures and safeguards need to be implemented to fulfill the conditions of Art. 9 (2) g). It is up to the EU MS and their national law to determine on a case-to-case basis whether the requirements of this article are met. Thus, potentially leading to substantial differences across the EU.

[11] "Paragraph 1 shall not apply if one of the following applies: the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;"

[12] "If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding."

[13] "processing relates to personal data which are manifestly made public by the data subject;"

[14] "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;"

2.3. Data protection impact assessment

It has been shown that the processing of biometric data for the purpose of unique identification of a natural person can be legal if it falls under at least on exception from Art. 9 (2). In case this processing is “likely to result in a high risk to the rights and freedoms of natural persons”, conducting a DPIA prior to any processing is necessary (Art. 35 (1)[15]). The DPIA is an assessment of the “impact of the envisaged processing operations on the protection of personal data”. A DPIA is also necessary where special categories of data are processed on a large scale (Art. 35 (3) b[16]) and if any publicly accessible area is systematically monitored on a large scale (Art. 35 (3) c)[17]). The controller of the data processing operation is responsible to conduct the DPIA. This is in accordance with the rationale of the GDPR and emphasizes once again the controller’s is responsibility to demonstrate compliance with the legislation as required by the principle of accountability (cf. section 1.4.). Art. 35 (7) lists the necessary components to be included in any DPIA. However, it remains problematic with conduction a DPIA when the processing of biometric data for uniquely identifying a natural person is on a ‘large scale’. According to Recital 91 GDPR ‘large scale’ means that a “considerable amount of personal data at regional, national or supranational level which could affect a large amount of data subjects” is processed. This still leaves a lot of room for interpretation. Interesting is the component “new technologies” of Art. 35 (1). This condition subsequently requires a DPIA whenever FRT is deployed.

2.4. Prior consultation

In case the DPIA indicates that the processing of data results in a high risk insofar as the controller cannot mitigate such risks by appropriate measures, a prior consultation with the supervisory authority becomes necessary (Art. 36 (1)[18]). An example of ‘high risk’ is given by the Art. 29 Working Party. Accordingly, a high risk includes “where the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome, and/or when it seems obvious that the risk will occur”(Art. 29 WP, 2017, p.18). “In the biometric context, this could be where the data subject cannot change its biometric credentials in case of theft of its biometric identity details”(Kindt, 2017, p.10).

[15] “Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.”

[16] “processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

[17] a systematic monitoring of a publicly accessible area on a large scale.”

[18] “The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.”

2.5. Four categories of biometric data

Based on all these legal aspects it results that data relating to the physical, physiological, or behavioural characteristics of a natural person can be categorized into four different types (Kindt, 2017). These are important to mention here for a better understanding of the law and its application. The first type is the 'ordinary' personal data relating to the aforementioned characteristics of a natural person. This first type is not considered to be biometric data under Art. 4 (14) and thus, does not fall under the specific provisions regulating the processing of biometric data. The second type is biometric data as defined in Art. 4 (14) "resulting from specific technical processing which allow or confirm the unique identification of a natural person". Since there is no specific legal regime applicable to this type of data other than the general GDPR regulations, biometric data is in principle subject to the same legal regime as ordinary personal data. The third type is the sensitive biometric data processed for the purpose for uniquely identifying a natural person. Hence, the processing of this type must comply with Art. 9 GDPR. Problematic here is that sensitive biometric data for the purpose of verification (1:1 comparison) does fall into the second category of data and thus, is subject to an easier legal regime (Kindt, 2017). The fourth type is sensitive biometric data processed for unique identification on a large scale. This type is yet another category because in addition to falling under Art. 9 processing of this type also must comply with additional legal requirements. These are the DPIA and the prior consultation under Art. 35 and 36.

2.6. Conclusion: Answer to sub-question 1

This section has examined the legislative framework of FRT in the EU, namely the GDPR. Based on these insights an answer to the first sub-question of this thesis can be formulated: *To what extent does the GDPR legitimize FRT use for non-law enforcement purposes in public and private spaces?*

FRT systems that process biometric data with the purpose of uniquely identifying a natural person must comply with the strictest regulations under the GDPR. This type of processing is generally prohibited under Art. 9 (1), but ten exceptions exist under Art. 9 (2). The most import ones regarding the deployment of FRT are 'explicit consent given by the data subject' (Art. 9 (2) a), 'data has been made manifestly public' (Art. 9 (2) e), and 'substantial public interest' (Art. 9 (2) g). However, all these exceptions are problematic. If the use of FRT falls under one of the exceptions of Art. 9 (2) an additional requirement applies: conducting a DPIA. Furthermore, Art. 36 requires that if the DPIA indicates a high risk for the data subject, the controller must consult with the supervisory authority prior to the processing. If any of these requirements are not met the use of FRT is not legitimate from a legal perspective. Important to note here is if FRT is not used for the purpose of unique identification but instead for e.g., verification or classification this strict legal regime does not apply. This is mainly because the technical circumstances behind verification and classification differ from the ones necessary to directly identify a natural person. Nevertheless, this is a controversial issue also because data controllers could potentially misuse this loophole in the law. Regarding public and private spaces, the

GDPR does not make any substantial differentiations. However, when applying the regulations, the interpretation whether FRT is deployed in a (open) private or public space can play a vital role in e.g., determining the risk for potentially affected people.

3. Banning FRT: The Belgium case

Belgium is particularly interesting for this thesis because it provides an example on how a ban on FRT could look like. It is currently the only country in the EU, and one of only two countries worldwide to ban the use of FRT (Gosh, 2020).

> "Belgium has effectively banned the use of facial recognition and other biometrics-based video analytics in surveillance cameras for private, non-police use, taking a strong stand and showcasing the impact of new EU privacy regulations on video surveillance"(Rollet, 2018).

3.1. Belgian data protection law

Belgium adopted four acts to supplement the GDPR. Art. 78 of the act of 21st March 2018 on camera surveillance only applies to non-law enforcement cameras and reads:

> "The use of intelligent surveillance cameras coupled with registers or personal data files is only authorized for the automatic recognition of license plates, provided that the controller processes these registers or these files in compliance with the regulations relating to the protection of privacy."

This provision effectively bans the use of FRT systems. FRT is an AI-based technology hence, considered 'intelligent surveillance'. The use of FRT for purposes like unique identification would not be compliant with this law because it requires a database of people's personal characteristics. Nevertheless, other applications of FRT would still be allowed. For example, for purposes of access control or verification (Rollet, 2018).

Many civil organizations like Statewatch have also called for a ban or moratorium on FRT. The UN expert on freedom of opinion and expression, David Kayne has called for an immediate moratorium on surveillance technology "until human rights-compliant regulatory frameworks are in place"(Kaye, 2019).

3.2. Safeguarding data protection and privacy rights

"The rights to respect for private life and protection of personal data are at the core of fundamental rights concerns when using facial recognition technology"(FRA, 2020, p.33).

Both rights are closely related and strive to protect similar values. Above all "the autonomy and human dignity of individuals, by granting them a personal sphere in which they can freely develop their personalities, think and shape their opinions"(FRA, 2020, p.23).

The use of FRT entails both risks and promises considering fundamental rights. Advantages include among others: (1) Artificial intelligence can be more effective than human intelligence. Human surveillance (e.g., security guards) is a common practice but also humans can fail and might be (unknowingly) very discriminatory and biased against certain people. AI and FRT are becoming increasingly accurate and sophisticated. Thus, replacing human surveillance with AI surveillance systems can be beneficial. (2) FRT can enhance public security. For example, in cases of emergency like the current Covid-19 pandemic FRT can be incredibly helpful in e.g., tracking infections and people with the purpose of preventing further spreading of the disease and thus, protect people.

The risks of FRT are extensive: (1) There is a substantial danger of biometric mass surveillance when deployed in publicly accessible areas. (2) The technology can still be inaccurate in recognizing people which can lead to discrimination. (3) FRT automatically processes data which creates problems for the data subjects because they have limited or no knowledge about the processing and the data storage. (4) This is enhanced through the non-transparent deployment of FRT systems. (5) FRT can have substantial adverse consequences for people outside the scope of the pursued aim of the system.

FRT interferes with the right to privacy and data protection by collecting data relating to an identified or unidentified individual. Interferences must have a solid legal justification. They must be in accordance with the law, pursue a legitimate aim and necessary in a democratic society. The biggest issue of FRT lies with the necessity and proportionality. FRT systems can pursue a legitimate aim like public security or offering certain services to citizens. However, often their necessity and proportionality to pursue this aim is contested. This is also because often less invasive methods are just as effective and adequate. Additionally, a clear legal basis is necessary to justify the infringements to the right to privacy and data protection. The GDPR does not fully provide that leaving a lot of room for interpretation and thus, unintended uses of FRT which dismiss the rationale of the GDPR.

3.3. Conclusion: Answer to sub-question 2

To what extent is an absolute ban on FRT the only solution to data protection and privacy rights?

The fundamental problem around FRT is walking the fine line between facilitating technological innovation for the benefit of society and protecting fundamental rights. The right to data protection and privacy are not absolute rights and can be subject to limitations (FRA, 2020). Thus, the context at hand (i.e. the sensitivity of the data, how it is used and stored) always has to be taken into account. Data protection and privacy rights implications of using FRT vary substantially depending on the purpose, context, and scope of the use. There is no clear answer to the second sub-question.

Belgium's approach looks promising protecting privacy and data protection rights because it allows for FRT use in some instances but prohibits the especially invasive kinds of FRT usage like identification. Thus, the benefits of FRT still can be utilized within the limits of privacy and data protection fundamental rights.

4. EU member state's use of FRT in public spaces – The Ireland case

The following chapter examines the case of an Irish children's hospital planning to deploy FRT-capable surveillance cameras. First, general information about the case will be presented introducing the hospital and its surveillance system. Second, considering the theoretical framework (see section 1.4.) and the legislative framework of FRT (see section 2.) an analysis of the case will be conducted. Third, based on this analysis an answer to the third sub-question of this thesis will be formulated.

4.1. Statement of case facts

On October 25th, 2019 Charles Rollet, a journalist from IPVM, a leading video surveillance information source, made a Freedom of Information [FOI] request about the New Children's Hospital's [NCH] video surveillance system. The FOI contains information that the NCH is planning to deploy cameras which are capable of FRT (O'Rourke, 2019).

Ireland's New Children's Hospital located in Dublin is still under construction and scheduled to open in 2023 (NCH, n.d.). The development of the hospital is coordinated by the National Paediatric Hospital Development Board [NPHDB] which is a public body.

According to the FOI, the NCH will be using an all-Hikvision surveillance system of CCTV cameras (Rollet, 2019). Some of these cameras are capable of mapping facial features caught live on video and compare them to a database of images to confirm the identity of a natural person (Cronin, 2021). These FRT cameras can consequently identify any person entering the hospital. Hikvision is a Chinese company and has been in recent years involved in several scandals regarding human rights abuses in China and general data protection and privacy rights concerns (Farries, 2019).

IPVM's estimated number of cameras potentially deployed at the NCH range in the hundreds, many of them capable of facial recognition (Rollet, 2019). More information has been requested by IPVM about the surveillance system and especially about the potential use of FRT. However, this request was denied by the NCH because this information was deemed "commercially sensitive"(O'Rourke, 2019). To this day no detailed information about the full scope of the surveillance system of the NCH has been made public.

Rollet's s article sparked wide-spread outrage and concerns about the deployment of FRT in a public children's hospital. The Irish Council for Civil Liberties [ICCL] is extremely concerned about the "growing and unnecessary use of FRT in Irish society"(Farries, 2019). Following this public attention, the Irish Minister for Health, Simon Harris, subsequently told the Irish parliament that "it has not yet been decided which aspect of the security systems' capabilities will be used" and that "less than 3% of the cameras procured for the new children's hospital have the potential for high-definition facial recognition capabilities" (Oireachtas, 2019). However, according to IPVM's estimations that would still make for an estimated 10+ FRT-capable cameras deployed in the hospital (Rollet, 2019). If these were to be placed strategically at entrances, virtually every person entering the hospital can be captured by the system (Rollet, 2019). Looking at the FOI and the NCH Annual Report 2019, the contract with Hikvision indicates that a decision to use FRT has already been made. Otherwise, why would one preorder the far more expensive FRT cameras if apparently a decision to be using this technology has not been made yet? From an economical viewpoint this makes little sense. Additionally, the NCH Annual Report 2019, published after information broke about the surveillance system, does not explicitly mention the use of FRT. It does mention its "digital hospital concept" but without a detailed explanation what it entails exactly (NPHBD, 2019).

4.2. Analysis

Privacy rights expert Elizabeth Farries from ICCL says on this issue:

> "The New Children's Hospital contracting face surveillance technology for children accessing medical care would be incredibly invasive. Children are afforded enhanced personal data protections under the law. Deploying this tech in this manner would run afoul of those protections. It's expensive, inaccurate, discriminatory, and in this situation, likely unlawful" (2019).

The adaptation of the GDPR is the Irish Data Protection Act 2018 [IDPA]. Appendix B provides an overview of the relevant GDPR articles and their respective adaptions into the IDPA.

Children are offered enhanced personal data protection under the GDPR and the IDPA. The GDPR states that "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data"(Rec. 38). The key principles of EU data protection law laid out in Art. 5 GDPR (see section 1.4.) are additionally emphasized by the GDPR whenever the processing relates to children. For example, for children the transparency principle requires that "any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand"(Rec. 58). Thus, due to the highly problematic nature of FRT processing data of minors for facial recognition purposes can be deemed unlawful (Boran, 2019). This is also reflected in the cases of Swedish and French schools fined for using such a system (EDPB, 2019; LQDN, 2020). The Minister of Health emphasized before the parliament that the decision to use FRT

> "will be taken nearer the opening of the hospital by Children's Health Ireland and will be fully in line with Irish and European data protection and privacy legislation and guidelines, to ensure that the occupants of the hospital have the appropriate protections and security afforded to them, in line with their privacy rights"(Oireachtas, 2019).

Any FRT deployment needs a clear legal basis. However, for the case at hand there is no clear basis in the law apparent now. Officially, the purpose of the FRT cameras is to prevent babies being "snatched"(Keena, 2020). This is based on the special child protection responsibilities of the hospital (Keena, 2020). Art. 9 (2) i) GDPR[19], could potentially be used as a legal basis. This provision allows for special data processing where it is necessary for public interest reasons around public health. Nevertheless, it is controversial whether confirming people's identities can be regarded as necessary for providing essential healthcare and serve the public interest. The notion of "public interest" is notoriously vague. It always includes a balancing exercise where arguments must be weighed. No cases where a similar exception has been invoked and recognized legitimate could be found so far.

Additionally, there is a fear of a function creep. As the NCH proclaimed to be the "first public digital hospital", FRT could be used as part of the plans for an Electronic Healthcare Record which would go far beyond the original purpose and would entail even severer infringements of data protection and privacy rights (NCH, 2019). Other exceptions under Art. 9 are just as problematic, especially the "explicit consent" exception which requires freely given, informed, and specific consent to the processing. On the one hand, this exception is problematic here because it is questionable to what extent a minor can give consent to such a processing (cf. Art. 8(1) GDPR). On the other hand, it is problematic because the "freely given" condition implies that consent must not be conditional but if people refuse to consent to FRT they subsequently cannot enter the NCH.

> "To protect everyone's rights, including children's, the state should not install these face surveillance systems in hospitals in the first instance, and certainly not in cooperation with private surveillance companies with controversial rights track records. A data protection impact assessment would demonstrate the risks. Has the New Children's Hospital conducted one?" (Farries, 2019).

Ireland's data protection watchdog has also warned the hospital if it is considering using FRT in its surveillance system it will have to conduct a DPIA first (O'Keeffe, 2019). Graham Doyle, from the Irish Data Protection Commission [DPC] said that FRT systems need to be justified as necessary and proportionate (O'Keeffe, 2019). Besides that, any processing of data also must pursue a legitimate aim in a democratic society (see section 1.4.). This condition of the key principles of EU data protection law is in this case controversial since to this date the NCH did not provide any detailed information about their legitimate aim pursued or the necessity and proportionality of the system. Normal CCTV cameras could achieve the same results in preventing babies being stolen without being as invasive. If the aim of avoiding babies being stolen from the hospital is a legitimate one needs to be further evaluated. This must be done, inter alia, through a DPIA.

[19] "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;"

> “We would also advise that conducting a Data Protection Impact Assessment is likely to be mandatory in these cases, given that the processing would possibly involve new technologies, children’s data, and special category data as defined in Article 9 of the GDPR as well as large scale processing in a publicly accessible area”(O’Keeffe, 2019).

Notable is that the DPC only advised a DPIA to the NCH even though it is required by law in this case. The DPC published a list of types of data processing operations that require a DPIA (DPC, 2018). Furthermore, the DPC has the responsibility to “promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention”(Art. 57 (1) b) GDPR). To fulfill this responsibility the DPC would have to take a stronger stance against the NCH and their surveillance system. The DPC has the enforcement powers to do so (cf. Art. 55 (2) & 58 GDPR) but chose to not act so far.

This is also reflected in the DPC’s past dealings with GDPR compliance. Ireland plays a significant role in the GDPR enforcement since many large tech-companies like Facebook, Twitter, Google, and LinkedIn are based in Ireland and thus, under Irish jurisdiction and the supervision of the DPC (Murphy, 2019). However, the DPC has often been criticized for being overly business-friendly, not independent enough, and overall “toothless from an enforcement perspective”(Murphy, 2019, p.73). So far, the DPC has only issued seven fines in total for GDPR violations with the highest only being 450 000 € for Twitter (GDPR Enforcement Tracker, n.d.). It is also problematic hat the IDPA limits, irrespective of the misdemeanor, the amount of a fine imposed on public bodies to 1 000 000 € (cf. Art. 141(4)).

4.3. Conclusion: Answer to sub-question 3

How have national governments in the EU been regulating the application of FRT in public spaces for non-law enforcement purposes?

Using FRT in a public children’s hospital is very difficult to justify legally. Neither the necessity, proportionality nor the pursued legitimate aim have been adequately laid down so far on the basis of the evidence analyzed. There are multiple legal barriers to be overcome before FRT can be lawfully deployed at the NCH. This case reflects the difficulties of regulating FRT. The GDPR and its Irish adaptation do not address FRT unequivocally leaving a lot of room for interpretation. Thus, the main issue of this case might not primarily be about ‘Could FRT be legally implemented at the NCH?’ but rather about ‘Should everything that is technically possible actually be done?’

The IPVM investigations into the NCH’s surveillance system resulted in major public outrage which could have been utilized by those responsible to inform the public about their plans in an open and transparent manner increasing the legitimacy of any FRT use. However, neither the NPHDB nor the health minister decided to do so. Instead, further public scrutiny was avoided at all costs. Throughout the analysis it became apparent that on both sides the effort to comply with the law and to enforce it was low. The NPHDB could have acted far more proactively in complying with the GDPR. The DPC, could have acted more swiftly and determined in demanding law compliance from the NCH. These dynamics between the actors are particularly interesting since they are all part of the public body. The NPHDB and the health minister are ultimately accountable to the Irish government. The DPC is independent in its work. However, the commissioners are appointed by the Irish parliament (IDPA, Art. 15). Presumably, surrounding these actors seems to be an environment of backroom-politics. Nevertheless, it is to say that there is still some time left until FRT might be used at the NCH. Since there is no apparent specific interest of patients at hand justifying the use of FRT, a revision of this case later is advised.

5. EU member state's use of FRT in private spaces – The Spain case

The following chapter examines the case of a Spanish supermarket which installed a FRT system in its stores. Just like the previous chapter, this will be done in three steps. In the law there is no clear differentiation between public and private spaces. However, considering the theoretical framework of this thesis this case is of interest because the notion of a private space which is publicly accessible due to an economic interest could in practice have substantial differences on the application of the GDPR. The aim of this chapter is to formulate an answer to the fourth sub-question of this thesis.

5.1. Statement of case facts

Mercadona is one of the biggest supermarket chains in Spain currently operating 1 639 stores across the country (Mercadona, n.d.). Privately owned Mercadona supermarkets are publicly accessible places. On July 1st, 2020 Mercadona started using a FRT system in about 40 of its stores in Mallorca, Zaragoza, and Valencia (Blonde, 2020a)[20]. This FRT system is from the Israeli company 'AnyVision' (Blonde, 2020b[21]). AnyVision has been controversial for its links with the surveillance of Palestinians in the West Bank (Aguiar, 2020[22]). Officially, the purpose of the system is to detect people with final sentences or precautionary measures who have a restraining order against Mercadona or its employees that prohibits them from entering the stores (Blonde, 2020a). Mercadona says that the FRT system is "nourished by the images generated by the video surveillance cameras that have been provided as evidence in the judicial procedure where the sentence has been issued"(Blonde, 2020b). This means that Mercadona can use any photos used as evidence in judicial procedures Mercadona has been part of and resulted in a restraining order or similar. Once the facial recognition system detects that a person with a current restraining order wants to access the supermarket, after comparing the image with a database, it issues an alert which will be verified by the security staff on-site (Blonde, 2020a). If that person is ultimately

[20] These sources have been translated from Spanish to English
[21] See 20
[22] See 20

identified as someone not permitted to enter the store the state security forces will be alerted (Blonde, 2020a).

Several major Spanish newspapers reported about the use of FRT in Mercadona stores. Following, on July 6th, 2020 the Spanish Data Protection Agency [AEPD] initiated an ex officio investigation of Mercadona for implementing the AnyVision facial recognition system (El Gobierno, 2020[23]). Many people have voiced their concerns about the FRT system on social media since, expressing their refusal to enter Mercadona stores now because they claim that the system violates their fundamental privacy and data protection rights as well as current data protection regulation (Aguiar, 2020; Navas, 2021[24]).

5.2. Analysis

Spain's adoption of the GDPR, the Spanish Data Protection Law [LOPD] came into effect in 2018. The LOPD is adapted to the new GDPR "but it does not reproduce its content requiring a common reading of both legal texts"(Pauner & Viguri, 2019, p.82). Appendix C gives an overview of relevant articles and their adaptions into the LOPD when provided.

> "The fact that biometric data is categorized by the GDPR as of special protection does not imply a restriction on its processing, but the legal requirement of the adoption of a series of more specific measures aimed at greater protection of said data in its use"(Díaz, 2020[25]).

Thus, one cannot say that Mercadona's use of FRT, by default, violates current data protection legislation. Nevertheless, this specific case has aroused controversy. Any Mercadona store that uses FRT has a poster at the entrance informing customers stating:

> "We inform you that Mercadona S.A., in order to improve your safety, has implemented a facial recognition system to detect only those people with a restraining order or similar judicial measure in force that may pose a risk to their safety"[26].

Mercadona has emphasized that despite initially processing the biometric data of everyone entering its stores, only those data that identify individuals with final court rulings in judicial proceedings in which Mercadona has been directly a procedural party will be further processed (Díaz, 2020). Only that data will be stored in the database, all other data is being deleted within 0.3 seconds (Díaz, 2020). There are, however, still several risks for potential customers. First, people with a restraining order cannot have their sensitive biometric data deleted as long as their order is in force (Aguiar, 2020). This means that despite there being no explicit authorization by law highly sensitive data from them is stored with a company that is known for its controversial surveillance activities. Mercadona assures that once the order has been canceled also the data is deleted (Aguiar, 2020). Still, a risk remains that the data is not

[23] See 20
[24] See 20
[25] See 20
[26] See Annex D

deleted. Second, FRT is not a perfect technology. It can fail and it can be biased. Hence, there is a real risk for people to be wrongly identified as someone prohibited to enter the supermarket. This is especially problematic because a (wrong) identification has immediate legal consequences on the data subject and thus, is a very high risk for people. Third, all people entering the store are being scanned and recognize through the system, even children. Does the publicly unknown, potentially very small number of people with a restraining order compensate for the fact that everyone entering the store is recognized? Fourth, there is again the problem of identification and verification. The purpose of the FRT system in this case is to uniquely identify people. The processing therefore falls under the especially restrictive legal conditions (cf. section 2) and would need, inter alia, a DPIA and prior consultation with the AEPD (AEPD, 2019). It is unknown whether this has been done. Mercadona insists that its system is legal and that they have been in contact with the AEPD during the planning process (Blonde, 2020a). Admittedly, why would the AEPD initiate an official investigation only five days after Mercadona stared using FRT even though they were allegedly involved in the planning process? Another question remaining is, whether the FRT system is proportionate and necessary to fulfill the purpose Mercadona aims at. A simpler surveillance system solely based on CCTV cameras without FRT could also fulfill the purpose just as good without the severe rights infringements and risks for the people.

The processing operation of this case requires an exception under Art. 9 (2) GDPR. Since there are comprehensive information posters placed at the entrances of the stores entering could be seen as giving consent to the processing operation. However, under the LOPD the mere consent from the data subject is not enough to allow the processing of special categories of data (cf. Art. 9 (1) LOPD[27]). Mercadona states that its processing is based on substantial public interest and necessary to exercise juridical orders (Blonde, 2020b). Thus, the exceptions Mercadona is invoking are Art. 9 (2) f) [28]& g). The problems of the "substantial public interest" exception have already been explained (cf. section 2.2.). First and foremost, it is unclear what exactly a "substantial public interest" is in the context of FRT use. Additionally, in this case it is very questionable whether Mercadona really acts in the interest of the public. It seems to be rather a corporate interest. Art. 9 (2) f) would in principle entitle Mercadona to process the biometric data only of those individuals previously convicted and with judicial measures. This exception does not allow for any processing of other individual's data. Whether this exception can be applied in this case then comes down to two essential issues: (1) Does the legitimate interest of Mercadona to prevent criminals entering their stores outweigh the right to data protection? (2) How strict are national authorities going to be interpreting the law surrounding FRT?

[27] "For the purposes of article 9.2.a) of Regulation (EU) 2016/679, in order to avoid discriminatory situations, the consent of the affected party alone will not be enough to lift the prohibition of the processing of data whose main purpose is to identify their ideology, union, religion, sexual orientation, racial or ethnic origin or beliefs. Provided in the previous paragraph will not prevent the processing of said data under the other cases contemplated in article 9.2 of Regulation (EU) 2016/679, when appropriate." [Translated]

[28] "processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;"

> “The Spanish Data Protection Agency is usually especially restrictive with the use of facial recognition techniques for the identification of a person, as seems to be the case of Mercadona”(Blonde, 2020b).

The European Data Protection Supervisor, Wojciech Wiewiórowski, has publicly questioned the precision and necessity of the FRT system in the Mercadona supermarkets (Navas, 2021). This case has also already been subject in the Spanish parliament. On November 5th, 2020 Senator Carles Mulet Garcia asked how far along the AEPD investigation is and when results can be expected (Mulet Garcia, 2020[29]). Those responsible answered that the investigation is not concluded yet and currently is in the phase of “preliminary investigation”(El Gobierno, 2020). The AEPD’s investigation is based on Art. 67 LOPD (El Gobierno, 2020). Accordingly, paragraph 2 requires that any such investigation may not take longer than twelve months. Hence, results are expected before July 6th, 2021.

In case the AEPD investigation finds that Mercadona violated data protection law the GDPR imposes a very strict and severe sanctioning regime. Art. 83 (5) regulates infringements pursuant to Art. 9: These infringements “shall […] be subject to administrative fines up to 20 000 000 Euros, or […] up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher”.

In the past, the AEPD has acted swiftly and strict when it comes to GDPR compliance of data controllers. To date, the AEPD ranks on place five of the total sum of fines imposed under the GDPR with a total sum of more than 29 million Euros (GDPR Enforcement Tracker, n.d.). In the total number of fines imposed the AEPD even ranks on place one with a total of 228 fines issued (GDPR Enforcement Tracker, n.d.).

Furthermore, the AEPD seems to be generally aware of the potential legal issues around new technologies such as FRT. On May 28th, 2020 the AEPD published a report on the use of facial recognition systems by private security companies (AEPD, 2020a). It is argued that the application of the “essential public interest” exception as a legal basis for deploying FRT requires an additional, currently non-existent rule with the rank of law that clearly justifies to what extent and in what cases FRT use would respond to it (AEPD, 2020b). Additionally, in February 2020 the AEPD published extensive and detailed guidelines on the GDPR compliance of processing that embed AI (AEPD, 2020c). These were extended in January 2021 with a document on specific audit requirements for personal data processing activities involving AI (AEPD, 2021).

5.3. Conclusion: Answer to sub-question 4

How have national governments in the EU been regulating the application of FRT in private spaces for non-law enforcement purposes?

It took the AEPD five days to initiate an ex officio investigation into Mercadona after they started using FRT. This is a considerably short amount of time for any public authority to act. At the time the

[29] See 20

investigation began the legality of the FRT system has been questioned. In contrast to the Irish case, the mere consent of the data subject is not enough to allow for FRT processing operations in Spain. Mercadona's FRT system falls under the especially restrictive legal conditions of the GDPR and the LOPD because it is used to uniquely identify people. From the information available it is currently doubtful whether Mercadona has met those requirements. Hence, the AEPD is currently investigating whether the pursued aim of the FRT system is legitimate under Art. 9 (2) f) and if the system is proportionate and necessary in light of the pursued aim. One of the main questions to be answered in this regard is if the legitimate interest of Mercadona to prevent criminals entering their stores outweighs the right to data protection and privacy.

Since the regulatory framework of FRT leaves a lot of room for interpretations this question will be answered at the discretion of the AEPD. Based on the insights from the case analysis and the fact that in the past the AEPD has been very strict in demanding GDPR compliance from data controllers, it is likely that the AEPD will not allow for Mercadona to further use FRT in its stores.

A revision of this case after July 6th, 2021 when the results of the investigation are published, is advised.

6. Conclusion

The aim of this bachelor thesis was to formulate an answer to the main research question: *To what extent is the use of facial recognition technology for non-law enforcement purposes compatible with the EU's current legislative framework?'*

The GDPR does not imply a general prohibition on the use of FRT. However, it demands certain safeguards and security mechanism to be implemented to assure compliance with data protection and privacy rights. Hence, using FRT is compatible with the GDPR *as long as* all the requirements under Art. 9, 35, and 36 are met. Furthermore, the GDPR does not consider all processing of biometric data as treatment of special categories of data. Thus, not all FRT deployments, like verification, fall under the especially restrictive regulations. This can be problematic when decision-makers do not sufficiently understand the technological backgrounds of FRT and its different analytical functions creating legal loopholes to be exploited by data controllers.

The GDPR does not directly differentiate between public and private spaces or actors. Nevertheless, the circumstance under which FRT is deployed play a substantial role in assessing whether the use is legitimated and compatible with the regulations. Locations play a vital role in assessing the risks for the data subjects. Private spaces, which can be open to the public, have a bit more discretion in using FRT. Whereas, FRT usage in public spaces entail more risks, for example, because people often do not have options to refuse being recognized by the system.

There is also a lack of case law surrounding FRT. As has been shown in the case analyses, national governments are currently handling FRT ambiguously. Spain has been in its past and current behaviour very strict in demanding GDPR compliance from data controllers, especially regarding new technologies. Ireland, however, not so much. In practice, the GDPR leaves a lot of room for interpretation and discretion with the EU MS which facilitates an unequivocal regulatory environment and a highly complex, time-consuming, and inscrutable case-to-case assessment of FRT use throughout the EU. These problems can be avoided by banning FRT for some functions, like Belgium did. This is a promising approach in safeguarding data protection and privacy rights. However, one must consider that even though a ban might be adequate for the time being, it can be disproportionate in the long run. EU Regulators and DPAs learn and become more aware of the risks and benefits enabling them to better handle FRT usage.

Due to the limited scope, time, and resources of this thesis several aspects could not be included into the research. For example, including considerations about FRT use in law-enforcement. Also including more case analyses would be beneficial to this study allowing for a more detailed picture and comparison between EU MS. Another limitation is that the investigations of the Spain and Ireland cases have not be concluded by the time this study is completed. Hence, the outcomes are currently unknown and should be analyzed in further research. Another interesting future research topic could be the EU's proposal for an 'Artificial Intelligence Act', published on April 21st, 2021. This act aims at balancing the benefits AI technology, like FRT, can bring about whilst protection European values, fundamental rights, and principles.

Keeping these limitations in mind, the findings of this thesis still have a high societal, scientific, and political relevance. This thesis is very contemporary with 2021 being only the fourth year of the GDPR in force, the 20th anniversary of the CFR, and the increasingly rapid rise of AI technologies affecting more and more aspects of our everyday lives. This study fills the gap of scientific research and literature in the context of 'regulating biometrics' as well as data protection and privacy issues of new AI technologies. It contributes to a better understanding of these issues and can facilitate a new debate prioritizing fundamental rights, democratic freedoms and civil liberties whilst supporting technological advancement. Having this debate is crucial and will help policymakers and enforcement authorities find adequate regulatory solutions that are desperately needed.

7. References

7.1. Academic Articles

Birch, E. L. (2008). Public and Private Space in Urban Areas: House, Neighborhood, and Cit. In R. A. Cnaan & C. Carl Milofsky (Eds.), Handbook of Community Movements and Local Organizations. pp. 118–128. Springer.

Condie, B. & Dayton, L. (2020). Reading between the lines. Nature Index. Vol. 588. pp. 126-128.

Cronin, O. (2021). Hikvision cameras in a children's hospital in Ireland. In: International Network of Civil Liberties Organisations [INCLO]. (2021). *In Focus: Facial Recognition Tech Stories and Rights Harms from around the World*. p. 21.

Dushi, D. (2020). The use of facial recognition technology in EU law enforcement: Fundamental rights implications.

Glasze, G. (2001). Privatisierung öffentlicher Räume? Berichte Zur Deutschen Landeskunde, 75(2/3), pp.160–177.

Kaufmann, J. (eds.). (2019). *GDPR National Legislation Survey 5.0*.

Kindt, E. J. (2013). Privacy and Data Protection Issues of Biometric Applications - A comparative legal analysis. Springer.

Kindt, E J. (2017). *Having Yes, Using No? About the new legal regime for biometric data*.

Kindt, E. J. (2020). A first attempt at regulating biometric data in the European Union. In: Kak (Eds.). *REGULATING BIOMETRICS: Global Approaches and Urgent Questions*. AI NOW Institute. pp. 62-69.

Kokott, J., & Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. International Data Privacy Law, 3(4), pp. 222–228.

McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. In Big Data and Society (Vol. 4, Issue 1). SAGE Publications Ltd.

Murphy, M. H. (2019). The Irish adaption of the GDPR: The Irish Data Protection Act 2018. In: McCullagh K., Tambou, O., & Bourton S. (Eds.). (2019). *National Adaptations of the GDPR*. Collection Open Access Book, Blogdroiteuropeen. pp. 72-79.

Pauner, C. & Viguri, J. (2019). The adaption of the GDPR in Spain: The new data protection act (LOPDGDD). In: McCullagh K., Tambou, O., & Bourton S. (Eds.). (2019). *National Adaptations of the GDPR*. Collection Open Access Book, Blogdroiteuropeen. pp. 80-88.

Sprokkereef, A. (2008). Data Protection and the Use of Biometric Data in the EU. In S. Fischer-Hübner, P. Duquenoy, & A. L. Zuccato (Eds.), IFIP International Federation for Information Processing: The future of identity in the information society. Vol. 262, pp. 277–284. Springer.

Tambou, O. (2019). Opening Remarks. In: McCullagh K., Tambou, O., & Bourton S. (Eds.). (2019). *National Adaptations of the GDPR*. Collection Open Access Book, Blogdroiteuropeen. pp. 24-27.

7.2. Reports

AEPD (2019). List of the types of data processing that require a data protection impact assessment under Art. 53 (4). Retrieved from: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-en-35-4.pdf.

AEPD (2020a). The AEPD analyzes in a report the use of facial recognition systems by private security companies. Retrieved from: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/AEPD-informe-sistemas-reconocimiento-facial-empresas-seguridad-privada.

AEPD (2020b). N/REF: 010308/2019. Gabinete Jurídico. Retrieved from: https://www.aepd.es/es/buscador?f%5B0%5D=tipo_de_documento%3A608&search=&page=3.

AEPD (2020c). GDPR compliance of processing that embed artificial intelligence. An introduction. Retrieved from: https://www.aepd.es/sites/default/files/2020-07/adecuacion-rgpd-ia-en.pdf.

AEPD (2021). Audit requirements for personal data processing activities involving AI. Retrieved from: https://www.aepd.es/sites/default/files/2021-01/requisitos-auditorias-tratamientos-incluyan-ia-en.pdf.

Article 29 Data Protection Working Party. (2017). WP 248 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. http://ec.europa.eu/justice/data-protection/index_en.htm

Data Protection Commission (2018). List of Types of Data Processing Operations which require a Data Protection Impact Assessment.

European Union Agency for Fundamental Rights [FRA] & Council of Europe [CoE]. (2019). Handbook on European Data Protection Law. Publications Office of the European Union.

European Union Agency for Fundamental Rights [FRA]. (2020). Facial recognition technology: fundamental rights considerations in the context of law enforcement. https://doi.org/10.2811/231789

Houses of the Oireachtas (11 December 2019). National Children’s Hospital. Irish parliamentary debate, Oireachtas. https://www.oireachtas.ie/en/debates/question/2019-12-11/226/.

Kak (Eds.). (2020). REGULATING BIOMETRICS: Global Approaches and Urgent Questions. AI NOW Institute. https://deweyhagborg.com/projects/how-do-you-see-me.

NPHDB (2019). NCH Annual Report 2019. Retrieved from: https://www.newchildrenshospital.ie/publications/.

7.3. Online Resources and Websites

Aguiar, A. R. (2020). La AEPD investiga a Mercadona por sus cámaras de reconocimiento facial. Business Insider España. https://www.businessinsider.es/aepd-investiga-mercadona-camaras-reconocimiento-facial-672287

Blonde, I. (2020a). Protección de Datos abre una investigación sobre las cámaras de vigilancia facial de Mercadona. El País. Retrieved from: https://elpais.com/tecnologia/2020-07-06/proteccion-de-datos-abre-una-investigacion-sobre-las-camaras-de-vigilancia-facial-de-mercadona.html.

Blonde. I. (2020b). Las claves de la polémica por el uso de reconocimiento facial en los supermercados de Mercadona. El País. Retrieved from: https://elpais.com/tecnologia/2020-07-06/las-claves-de-la-polemica-por-el-uso-de-reconocimiento-facial-en-los-supermercados-de-mercadona.html.

Boran, M. (2019). Facial recognition technology latest woe at national children's hospital. The Irish Times. Retrieved from: https://www.irishtimes.com/business/technology/facial-recognition-technology-latest-woe-at-national-children-s-hospital-1.4112451.

Brennan, J. (2019). *Facial Recognition: Defining terms to clarify challenges*. https://www.adalovelaceinstitute.org/blog/facial-recognition-defining-terms-to-clarify-challenges/

Carrer, L., Coluccini, R., Di Salvo, P. (2020a). How facial recognition is spreading in Italy: the case of Como. Privacy International. https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como

Carrer, L., Coluccini, R., Di Salvo, P. (2020b). Riconoscimento facciale, perché Como è tra le prime città a usarlo. Wired. Retrieved from: https://www.wired.it/internet/regole/2020/06/09/riconoscimento-facciale-como/?refresh_ce=

Díaz, E. (2020). Los sistemas de reconocimiento facial y sus implicaciones legales – Caso Mercadona. El Derecho. Retrieved from: https://elderecho.com/los-sistemas-reconocimiento-facial-implicaciones-legales-caso-mercadona.

EPIC. Ban Face Surveillance. (n.d.). Retrieved March 4, 2021, from https://www2.epic.org/banfacesurveillance/

European Digital Rights [EDRi]. (2019). Facial recognition and fundamental rights 101. Retrieved from: https://edri.org/our-work/facial-recognition-and-fundamental-rights-101/

European Digital Rights [EDRi]. (2019). The many faces of facial recognition in the EU. Retrieved from: https://edri.org/our-work/the-many-faces-of-facial-recognition-in-the-eu/

Electronic Frontier Foundation [EFF]. (n.d.). Face Recognition. Retrieved March 20, 2021, from https://www.eff.org/de/pages/face-recognition

European Data Protection Board [EDPB]. (2019). Facial recognition in school renders Sweden's first GDPR fine. Retrieved from: https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en

Farries, E. (2019). Concern at growing use of unnecessary and possibly illegal facial recognition technology. ICCL. Retrieved from: https://www.iccl.ie/news/concern-at-growing-use-frt/.

GDPR Enforcement Tracker (n.d.). Fines Statistics. Retrieved from: https://www.enforcementtracker.com/?insights.

Gosh, I. (2020) Mapped: The State of Facial Recognition Around the World. Retrieved from: https://www.visualcapitalist.com/facial-recognition-world-map/

Kaye, D. (2019). UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools. United Nations Human Rights. Retrieved from: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736&LangID=E.

Keena, C. (2020). Controversial cameras needed at children's hospital 'to prevent babies being taken'. The Irish Times. Retrieved from: https://www.irishtimes.com/news/health/controversial-cameras-needed-at-children-s-hospital-to-prevent-babies-being-taken-1.4140964

La Quadrature du Net [LQDN]. (2020). First Success Against Facial Recognition in France. Retrieved from: https://www.laquadrature.net/en/2020/02/27/first-success-against-facial-recognition/

Mercadona (n.d.). Retrieved from: https://info.mercadona.es/en/conocenos.

Navas, M. (2021). Continúa la investigación de la AEPD por las cámaras de Mercadona. Retrieved from: https://elcierredigital.com/investigacion/396609595/aepd-investiga-camaras-reconocimiento-facial-mercadona.html

NCH. Delivering Ireland's New Children Hospital (n.d.). Retrieved from: https://www.newchildrenshospital.ie.

O'Keeffe, C. (2019). Watchdog warning over mooted facial recognition cameras at children's hospital. Irish Examiner. Retrieved from: https://www.irishexaminer.com/news/arid-30969373.html.

O'Rourke, E. (2019). Freedom of Information Request. Ref:2019/042/EOR. Retrieved from: https://ipvm-uploads.s3.amazonaws.com/uploads/30f7/7078/FOI.2019.042.Decision.Letter.and.Document.25.11.19%20(1).ppd.

Rollet, C. (2018). Belgium Bans Private Facial Surveillance. IPVM. Retrieved from: https://ipvm.com/reports/belgium-biometrics.

Rollet, C. (2019). Ireland National Children's Hospital Chooses Hikvision End-to-End With Facial Recognition. IPVM. Retrieved from: https://ipvm.com/reports/ireland-hikvision?code=cr

Wiewiórowski, W. (2019). Facial recognition: A solution in search of a problem? European Data Protection Supervisor. Retrieved from: https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en

7.4. Legal Documents

Charter of Fundamental Rights of the European Union, OJ 2012 C 326/391, (2012).

Data Protection Act 2018. Number 7 of 2018. Ireland.

El Gobierno (18th December, 2020). Respuesta del Gobierno. Pregunta escrita a senado. Expediente 684/026869/0002. Retrieved from: https://www.senado.es/web/expedientdocblobservlet?legis=14&id=71518.

EU Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89, (2016).

EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, (2016).

European Convention on Human Rights, 4th November 1950, ETS 5, (1950).

GPDP. Provvedimento del 26 febbraio 2020, N. 9309458, (2020).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitale.

Mulet Garcia, C. (5th November, 2020). Pregunta Escrita. Expediente 684/026869/0001. Retrived from: https://www.senado.es/web/expedientdocblobservlet?legis=14&id=63742.

The Act of 21 March 2018 amending the existing Belgian Act of 21 March 2007 on camera surveillance. “Wet tot wijziging van de wet op het politieambt om het gebruik van camera’s door de politiediensten te regelen, en tot wijziging van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera’s, van de wet van 30 novem- ber 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, bl. 33691.“ Belgische Staatsblad. 188e Jaargang. 16th April 2018.

Treaty on the Functioning of the European Union. 2012/C 326/1. (2007)

Appendix

A. Table 1 – Chapter 2.

Overview of the legislative framework of FRT

GDPR Article	Content	Relevant Provision(s)	Problem(s)	Case
4 (14)	Definition 'Biometric Data'	"specific technical processing"	excludes raw data; Rec. 51	
9 (1)	General prohibition of processing	"for the purpose of uniquely identifying a natural person"	limits the scope; some FRT functions do not fall under this prohibition	Both
9 (2)	Exceptions to the prohibition	a) "explicit consent"	Is entering any place using FRT explicit consent? Conditional Consent - Often no opt-out possibility; Children;	
		e) "data manifestly made public"	Could be misused as a universal excuse for using FRT	
		f) "exercise of legal claims"	processing data only of involved people	➔ Mercadona
		g) "substantial public interest"	Vague term; Unclear definition of safeguards; Corporate vs public interest	
		i) "public interest in the area of public health"	Balancing exercise; no case law	➔ NCH
35	DPIA		➔ When using FRT a DPIA is always necessary	In both cases not conducted
35 (1)		Impact on protection of personal data; "high risk"; "new technology"	Full impact and potential risks can be hard to assess	
35 (3)		a) "produce legal effects or similarly significantly affect a natural person"	No specific explanation about these 'effects'	
		b) "large scale of special categories of data"	Rec. 9; Where is the threshold to 'large scale'?	
		c) "systematic monitoring of publicly accessible areas"		
35 (7)		Necessary contents of DPIA		
36	Prior Consultation	(1) "high risk in the absence of measures taken by the controller to mitigate the risk"	What is a "high risk"? Art. 29 WP/ WP 248	In both cases not done

B. Table 2 – Chapter 3.

Overview of the relevant GDPR articles and their adaptions in the Irish DPA

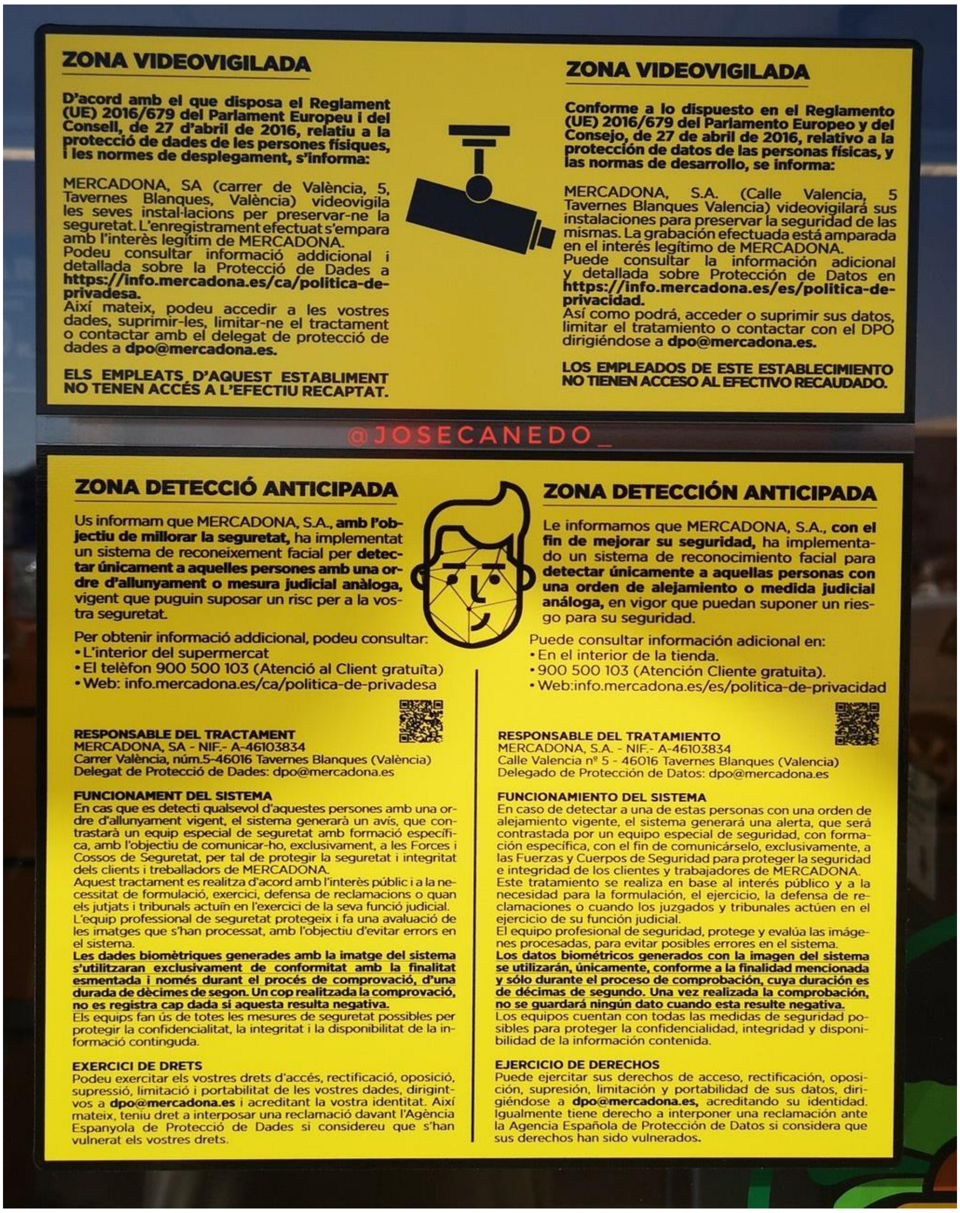
GDPR	IDPA
4 (14)	2 (1)
9	45
9 (2)	46-54
35	84 (1)
36	84 (3)

C. Table 3 – Chapter 4.

Overview of the relevant GDPR articles and their adaptions in the Spanish LOPD

GDPR	LOPD
4 (14)	-
9	-
9 (2)	9
35	28
36	28

D. Mercadona Entrance Poster – Chapter 4.


@JOSECANEDO_

ZONA VIDEOVIGILADA

D'acord amb el que disposa el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de dades de les persones físiques, i les normes de desplegament, s'informa:

MERCADONA, SA (carrer de València, 5, Tavernes Blanques, València) videovigila les seves instal·lacions per preservar-ne la seguretat. L'enregistrament efectuat s'empara amb l'interès legítim de MERCADONA.
Podeu consultar informació addicional i detallada sobre la Protecció de Dades a **https://info.mercadona.es/ca/politica-de-privadesa.**
Així mateix, podeu accedir a les vostres dades, suprimir-les, limitar-ne el tractament o contactar amb el delegat de protecció de dades a **dpo@mercadona.es.**

ELS EMPLEATS D'AQUEST ESTABLIMENT NO TENEN ACCÉS A L'EFECTIU RECAPTAT.

ZONA VIDEOVIGILADA

Conforme a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de datos de las personas físicas, y las normas de desarrollo, se informa:

MERCADONA, S.A. (Calle Valencia, 5 Tavernes Blanques Valencia) videovigilará sus instalaciones para preservar la seguridad de las mismas. La grabación efectuada está amparada en el interés legítimo de MERCADONA.
Puede consultar la información adicional y detallada sobre Protección de Datos en **https://info.mercadona.es/es/politica-de-privacidad.**
Así como podrá, acceder o suprimir sus datos, limitar el tratamiento o contactar con el DPO dirigiéndose a **dpo@mercadona.es.**

LOS EMPLEADOS DE ESTE ESTABLECIMIENTO NO TIENEN ACCESO AL EFECTIVO RECAUDADO.

ZONA DETECCIÓ ANTICIPADA

Us informam que MERCADONA, S.A., **amb l'objectiu de millorar la seguretat,** ha implementat un sistema de reconeixement facial per **detectar únicament a aquelles persones amb una ordre d'allunyament o mesura judicial anàloga,** vigent que puguin suposar un risc per a la vostra seguretat.

Per obtenir informació addicional, podeu consultar:
- L'interior del supermercat
- El telèfon 900 500 103 (Atenció al Client gratuïta)
- Web: info.mercadona.es/ca/politica-de-privadesa

RESPONSABLE DEL TRACTAMENT
MERCADONA, SA - NIF.- A-46103834
Carrer València, núm.5-46016 Tavernes Blanques (València)
Delegat de Protecció de Dades: dpo@mercadona.es

FUNCIONAMENT DEL SISTEMA
En cas que es detecti qualsevol d'aquestes persones amb una ordre d'allunyament vigent, el sistema generarà un avís, que contrastarà un equip especial de seguretat amb formació específica, amb l'objectiu de comunicar-ho, exclusivament, a les Forces i Cossos de Seguretat, per tal de protegir la seguretat i integritat dels clients i treballadors de MERCADONA.
Aquest tractament es realitza d'acord amb l'interès públic i a la necessitat de formulació, exercici, defensa de reclamacions o quan els jutjats i tribunals actuïn en l'exercici de la seva funció judicial.
L'equip professional de seguretat protegeix i fa una avaluació de les imatges que s'han processat, amb l'objectiu d'evitar errors en el sistema.
Les dades biomètriques generades amb la imatge del sistema s'utilitzaran exclusivament de conformitat amb la finalitat esmentada i només durant el procés de comprovació, d'una durada de dècimes de segon. Un cop realitzada la comprovació, no es registra cap dada si aquesta resulta negativa.
Els equips fan ús de totes les mesures de seguretat possibles per protegir la confidencialitat, la integritat i la disponibilitat de la informació continguda.

EXERCICI DE DRETS
Podeu exercitar els vostres drets d'accés, rectificació, oposició, supressió, limitació i portabilitat de les vostres dades, dirigint-vos a **dpo@mercadona.es** i acreditant la vostra identitat. Així mateix, teniu dret a interposar una reclamació davant l'Agència Espanyola de Protecció de Dades si considereu que s'han vulnerat els vostres drets.

ZONA DETECCIÓN ANTICIPADA

Le informamos que MERCADONA, S.A., **con el fin de mejorar su seguridad,** ha implementado un sistema de reconocimiento facial para **detectar únicamente a aquellas personas con una orden de alejamiento o medida judicial análoga,** en vigor que puedan suponer un riesgo para su seguridad.

Puede consultar información adicional en:
- En el interior de la tienda.
- 900 500 103 (Atención Cliente gratuita).
- Web:info.mercadona.es/es/politica-de-privacidad

RESPONSABLE DEL TRATAMIENTO
MERCADONA, S.A. - NIF.- A-46103834
Calle Valencia nº 5 - 46016 Tavernes Blanques (Valencia)
Delegado de Protección de Datos: dpo@mercadona.es

FUNCIONAMIENTO DEL SISTEMA
En caso de detectar a una de estas personas con una orden de alejamiento vigente, el sistema generará una alerta, que será contrastada por un equipo especial de seguridad, con formación específica, con el fin de comunicárselo, exclusivamente, a las Fuerzas y Cuerpos de Seguridad para proteger la seguridad e integridad de los clientes y trabajadores de MERCADONA.
Este tratamiento se realiza en base al interés público y a la necesidad para la formulación, el ejercicio, la defensa de reclamaciones o cuando los juzgados y tribunales actúen en el ejercicio de su función judicial.
El equipo profesional de seguridad, protege y evalúa las imágenes procesadas, para evitar posibles errores en el sistema.
Los datos biométricos generados con la imagen del sistema se utilizarán, únicamente, conforme a la finalidad mencionada y sólo durante el proceso de comprobación, cuya duración es de décimas de segundo. Una vez realizada la comprobación, no se guardará ningún dato cuando esta resulte negativa.
Los equipos cuentan con todas las medidas de seguridad posibles para proteger la confidencialidad, integridad y disponibilidad de la información contenida.

EJERCICIO DE DERECHOS
Puede ejercitar sus derechos de acceso, rectificación, oposición, supresión, limitación y portabilidad de sus datos, dirigiéndose a **dpo@mercadona.es,** acreditando su identidad. Igualmente tiene derecho a interponer una reclamación ante la Agencia Española de Protección de Datos si considera que sus derechos han sido vulnerados.

Source: https://twitter.com/josecanedo_/status/1278743277475414017/photo/1.