The lawfulness of facial recognition technology in public spaces

'A case study that links facial recognition technology in public spaces to the EU GDPR in order to determine the lawfulness of this practice'

Alicia Martins Nunes
S1541862
a.martins.nunes@umail.leidenuniv.nl
Supervisor – Dr. T. van Steen
Second reader – Dr. V. Niculescu-Dincă

Master Thesis – January, 2020
Crisis and Security Management
Leiden University 14.052 words

Abstract

Increasingly, biometric systems such as facial recognition technology are being applied as a tool to forestall risks and enhance the safety and security of society. However, these new technologies may come with undesired effects, such as threats to personal data or privacy. This study is conducted in order to discover if the concerns regarding these technologies can be justified, where such threats to privacy may come from and what can be done to improve the systems and eliminate these concerns. Therefore, it investigates the lawfulness of the use of facial recognition technology in public spaces in the Netherlands through the lens of the EU GDPR. In this study a model has been developed based on the main themes mentioned in the regulation, or six general data principles (Calder, 2018), and links them to specific GDPR articles. Qualitative data was collected predominantly through a single case study method combined with document analysis. Using this model and method showed that not all six principles were adhered to and using facial recognition technology in a public space in the Netherlands cannot be considered completely lawful. The main expectation provided for this finding is that the parties who employ the facial recognition technology do not consider the GDPR to a full extent.

Table of contents

1. Introduction

Biometrics, "the automated method of recognizing an individual based on measurable biological and behavioral characteristics," are gradually becoming a mainstream method to distinguish an individual based on the unique features of each person (Aydogan & Darcan, 2014: 492). One prevalent type of biometrics is facial recognition technology, which can briefly be defined as the identification of an individual by scanning their face in order to check if it matches with a gallery of images stored in an already existing database (Aydogan & Darcan, 2014). This technology is increasingly being used for surveillance purposes, for instance to locate missing children, monitor border movement and identify wanted criminals and/or terrorists that pose a threat to communities (Woodward, 2003). Facial recognition has some advantages, including cost-reduction and more effectiveness for law enforcement agencies in their fight against crime (Aydogan & Darcan, 2014).

Although most basic uses of facial recognition technology receive little criticism and are perceived to significantly improve policing efficiency, it is highly fundamental to consider some of the concerns this development has brought with it. Several scholars discuss not only the advantages of facial recognition technology, but also touch upon some of the disadvantages this new technology generates. One of the main arguments is that facial recognition will increasingly become a part of everyday services and applications that challenge traditional concepts of individual privacy (Fife & Orjuela, 2012). Agre, for example, finds that the use of facial recognition systems in public places should be outlawed due to their potential to be too intrusive, with the consequence of violating basic rights of privacy (2003).

In this thesis, I will focus particularly on facial recognition technology, because currently it is being applied to such an extent that it is nearly becoming a part of our daily lives. One fairly popular feature of the technology is its ability to function as a high-tech key, allowing access to virtual or actual spaces. Instead of presenting a password or similar identifier, the face of the individual seeking access is screened to ensure it matches an authorized identity (Gray, 2003). Facial recognition on iPhone is a recent example of this. It is important to note that in this situation a person usually is fully aware their face is being used and willingly scans its unique facial characteristics onto the device. In addition to this, urban spaces, both private and public, are increasingly fitted with surveillance cameras that apply facial recognition technology with the aim of detecting and sorting out suspected dangerous individuals in the urban environment.

The extended implementation of facial recognition surveillance is predominantly a reaction to perceptions of insecurity (Gray, 2003).

However, the increasing use of facial recognition technology, especially in public spaces, without people's consent may be problematic, specifically when looking at the EU General Data Protection Regulation (GDPR) that was implemented in 2016. In order to discover if this is actually the case, this thesis will answer to the following research question:

'To what extent can the use of facial recognition technology in public spaces in the Netherlands be considered lawful in terms of the GDPR?'

In doing so, I will analyze a specific case in the Netherlands, which I will apply to the GDPR in order to understand if it is lawful and morally acceptable. To keep this feasible, I will attempt to construct a framework that contains the main points of the GDPR and then apply the case to this. In order to conduct this research properly, I have formulated the following sub-questions:

1. *Is the use of facial recognition technology in public spaces without people's consent allowed according to the GDPR?*
2. *If not, what could be the case for this and how could this method become completely lawfully acceptable?*

1.1 Academic and societal relevance

Academic: Although there is extensive literature that has already established that facial recognition technology is becoming more mainstream than ever, that explains how facial recognition technology works and that discusses what its possible threats to privacy are, it has not yet been discovered to what extent it is lawfully acceptable in the Netherlands. There seems to be limited research that focuses on examining facial recognition from the perspective of the GDPR. Increasingly, people are being monitored in several public spaces, including the streets, train stations and airports. It can be highly questioned whether it is lawfully appropriate to monitor people without their consent. However, not much of the literature truly goes into this question. In the Netherlands especially, the debate about the extensive use of facial recognition technology is still in a very early stage, leaving (cybersecurity) companies in a position where they are not receiving many comments. Such a gap in the literature elucidates our lack of knowledge about the consistency of this technology with the GDPR. Therefore, this thesis will attempt to elucidate the fundamental importance of taking the GDPR into account when

deciding upon the usefulness and the lawfulness of facial recognition technology in public spaces.

Societal: the extensive use of facial recognition technology is influencing society in various ways. In his article, Phil Agre examines the ethical questions concerning these systems and he concludes that they may make false identifications and they might even violate basic privacy rights (Agre, 2001). Moreover, privacy is a constitutional right in the Netherlands and the GDPR should ensure the protection of data privacy. In addition to the privacy issues, there is also a realistic chance that the 'chilling effect' may come into existence for people in the Netherlands. This term is known as the discouragement or inhibition of the legitimate exercise of natural and legal rights by the threat of legal sanction. For instance, individuals might not feel comfortable to protest because they have a feeling they are being watched and might be arrested; even though everyone has the right to protest under the Dutch Law (freedom of speech). Since two basic constitutional rights could potentially be threatened by facial recognition technology, it is important to conduct more research on this topic and the dangers/invasiveness of it. As it is increasingly becoming an influential technology, the outcomes of this research may lead to more knowledge and more awareness among individuals and this could ultimately lead to the elimination of several privacy issues.

2. Theoretical framework

2.1 Facial recognition technology: a brief historical overview

At this moment, the world is on the cusp of a shift from a post- to a pre-crime society, "a society in which the possibility of forestalling risks competes with and even takes precedence over responding to wrongs done" (Zedner, 2007: 262). As a consequence, the pre-crime logic of security increasingly overshadows the post-crime orientation of criminal justice. This shift is not temporal, but more sectoral; the responsibility for security against risk falls not only to the State, but also extends to the individual, communal and private agents. With this shift, new trends in policing have emerged and technology is progressively starting to play a fundamental role in policing practices.

The upcoming technological advancements in policing are predominantly concerned with surveillance. This is a topical issue in Western societies, due to the growing awareness and an increase in number as well as type of surveillance technologies. Mostly throughout the

second half of the 20th century, not only the type and number of surveillance technologies, but also the type and scope of spaces and persons being surveilled have gradually increased (Galič et al., 2016). One of the most popular types of technological advancements currently used for surveillance practices, are biometric identification systems. Especially in the fields of personal identification and authentication the application of biometric technologies is increasingly becoming apparent (Miltgen et al., 2013). This is the case because biometric systems are recognition systems that aim at automatic identification or verification of identities through the collection of people's biometric features (Buciu & Gacsadi, 2016). The most notable types of biometrics already in use for the identification of people are fingerprints, iris and voice recognition, hand geometry, and facial recognition (Miltgen et al., 2013).

Facial recognition technology is used for various purposes: as a high-tech key that allows admission to virtual or real spaces, as a substitute for passwords on smart devices such as iPhones, as a mechanism to improve counterterrorism policy, as a tool to strengthen border control, to locate missing children, or as a means to track down terrorists or other wanted individuals. As this thesis will mainly focus on using facial recognition technology to monitor individuals without them knowing it, a controversial example of its use in public spaces in the last 5 years shall be briefly discussed to provide a better understanding of how, where and why this is generally done. The first example is that of Taylor Swift using facial recognition technology at some of her concerts last year. Rolling Stone magazine revealed that specifically at her May 18th Rose Bowl show, rehearsal clips of the artist were being displayed for her fans to watch. However, the spectators were unaware that a facial recognition camera inside the display was taking their photos, after which those were transferred to a command post where they were checked against a database of hundreds of Taylor's known stalkers (Knopper, 2018). It did not become clear what exactly happened to the data after it was used.

A similar case gained attention in the Netherlands in 2017. During this period it was discovered that multiple 'smart billboards' were dispersed across NS (Nederlandse Spoorwegen or Dutch Railways) train stations. These billboards contained hidden cameras and were equipped with the technology VidiReports, which is able to automatically trace every passing individual's face. This was mainly done with the goal of measuring people's reactions to the advertisements or to be able to specify them. Even though the billboard supplier claimed that data was not stored and the data could not be linked to specific people, there were several questions raised about the lawfulness of this procedure. By filming individuals, their personal data is

automatically obtained, which is not allowed according to the law, especially not for commercial ends.

The third chapter will elaborate on this case and the justification of certain choices that were made throughout the writing process of this thesis.

2.2 The existing literature on facial recognition and the GDPR

The exploration of this subject currently draws upon information from several disciplines, including criminology, sociology, surveillance studies and security studies. When combining the relevant literature from these disciplines, the emergence of two recent key trends can be agreed on: first, a shift to more predictive and pre-crime methods and second, surveillance technologies such as databases becoming increasingly ubiquitous in policing (van Brakel & De Hert, 2011). As I have mentioned before, quite some research has been done about facial recognition technology, what it entails, how it is used etc. Furthermore, the majority of the literature extensively discusses the privacy issues that come with the wide-spread use of facial recognition technology for security purposes.

According to Gray, "seeking to protect society from insecurity with the pervasive faze of facial recognition may generate heretofore-unimagined insecurities" (2003: 314). He also states that instead of ensuring security, it may actually add to urban insecurity in a fundamental way which is the transformation of society in unforeseen directions (Gray, 2003). Essentially, there is power inherent to the collection and analysis of information and facial recognition "with its ability to digitally archive a limitless gaze over urban space, represents a leap in this disciplinary influence" (Gray, 2003: 315). He even goes as far as to argue that "one cannot assume that traditional conceptions of privacy would have meaning in a society riddled with facial recognition cameras. And it is not just privacy that could be affected: fundamental ways in which members of society interrelate are also vulnerable to change" (Gray, 2003: 315). Moreover, Fife and Orjuela argue that new technologies, such as facial recognition, gradually become part of everyday services and applications that are acknowledged to challenge traditional concepts of individual privacy (2012). Additionally, they state that the average person may not yet be entirely aware of the extent to which their privacy and security are being affected by such practices (Fife & Orjuela, 2012). Miltgen et al. express that facial recognition systems "have potential to both enhance and threaten privacy and it is the security of the whole system which leads to potential privacy risks or protection (2013: 104). Furthermore, in his

article that examines guests' perceptions of biometric systems in hotels, Morosan discusses the use of biometric systems, including facial recognition technology, in the specific case of hotels (2012). He clearly states that hotels have not offered many biometric systems, with privacy issues arguably being one of the main issues (Morosan, 2012). The majority of the articles agree that the most common privacy issues associated with the use of biometric systems include identity theft, the storage of biometric data and tracking or tracing individuals (Schouten & Jacobs, 2009).

As we have seen in the previous paragraphs, privacy issues regarding facial recognition technology have been broadly discussed. However, not much has been written about the use of this technology in public spaces without people's consent. Most of the literature emphasizes privacy issues from a more moral perspective and examines the individuals' perceptions of privacy, rather than the legal aspect. Therefore, in this paper I want to fill (part of) this gap by exploring to what extent the use of facial recognition technology in public spaces is in line with the EU GDPR and what could be improved to make this technology completely consistent with the regulation.

2.3 Conceptualization

In order to answer the central research question and the sub-questions, the key concepts have to be operationalized into feasible and understandable concepts. For this research, three concepts are key to answering the central research question: biometric systems, facial recognition technology and the GDPR.

Biometric systems are a type of surveillance that uses biometric features, such a handprints, iris scans and facial recognition (Bennett, 2001). The term 'biometric features' typically entails a person's unique physical or behavioral features. The application of biometric technologies is becoming increasingly apparent in the personal identification and authentication fields (Miltgen et al., 2013). Biometric systems are used for multiple purposes, including counterterrorism policy, preservation of airport security, consumer use, and general surveillance practices. According to Shaikh and Rabaiotti, one of the primary applications of biometric-based identity management is for "identity verification and law enforcement" (2010: 342) specifically by national agencies and governments. The technology generally requires two operational dimensions: first, enrollment, in which biometric data are obtained and linked with a person's

identity and second, authentication or recognition, in which new biometric data are compared with the stored data (Langenderfer & Linnhoff, 2005). Even though evidence shows that augmented interest in biometric technologies is fueled by "an anticipated decrease of costs, improved technical quality of the systems and socio-political pressures for better security-related controls" (Miltgen et al, 2013: 103), it has been a topic of discussion for quite some time. This is mostly due to its pervasive technology, which makes users feel fearful, uncomfortable, or hesitant around these systems. Especially because they are perceived by the users as means for potential infringements into their privacy (Miltgen et al., 2013).

Facial recognition technology is part of the growing realm of biometrics. Because face images are an identification source that is unique to individuals, facial recognition can easily be used to recognize a human face and then compare it with a database of known faces to ultimately try and find a match. Facial recognition technology "maps details and ratios of facial geometry using algorithms, the most popular of which results in a computation of what is called the 'eigenface' or Principle Components Analysis (PCA) composed of 'eigenvalues'" (Gray, 2003: 315). Most basic uses of this technology, such as it allowing access to actual or virtual spaces, receive little criticism. The condemnation arises when facial recognition is connected to digital surveillance cameras in order to monitor spaces and the presence of certain people whose digital images are stored in databases, leading to the possibility that these images can ultimately be recorded and paired with identities. When various systems, public and private, are networked together to share information, surveillance power grows (Gray, 2003). Nevertheless, some potential dangers remain, because similar to other surveillance tools, facial recognition technology shares the problems that arise from secrecy of implementation (and the possibility of data errors). "Individuals often remain unaware that they are being observed and even when aware, they generally have no access to the information collected and therefore no ability to correct erroneous data" (Gray, 2003: 318). Especially when information about individuals is shared, it is claimed to be frequently used in numerous ways, most of which have not been consented to by the subjects. This can become even more complex when private and public institutions share information with each other (Gray, 2003).

GDPR or General Data Protection Regulation is a legal framework in EU law on data protection and privacy for all individual citizens of the European Union as well as the European Economic Area (EEA). It was adopted by the EU Council and Parliament in April 2016, and it was

officially implemented on the 25th of May 2018 (Calder, 2016). It contains a new set of rules and regulations that are primarily aimed at giving EU citizens more control over their personal data (Mohan et al. 2018). Therefore, the data subject, which is the individual whose personal data is collected, is allowed to demand companies to reveal what information is held, to object to processing the data, or to request to delete the data. The GDPR distinguishes two types of entities that must obey to their laws: data collectors (the collector and user of personal data) and data processors (the processor of personal data on behalf of the controller). Note that the rules and regulations may vary for these two different entities (Mohan et al. 2018). Under the GDPR, it must be completely clear to individuals that they are providing personal data and that this might have an effect on their privacy, thus allowing them to make an informed decision on whether they consent to their data being stored and used (Laybats & Davies, 2018). As Mohan et al. also state "GDPR-compliant services must ensure that personal data is collected legally for a specific purpose, and are obliged to protect it from mis-use and exploitation" (2018: 1). Hence, companies that wish to stay GDPR-compliant must take careful measures to ensure the protection of user data and because people's consent may be withdrawn at any time, organizations should review regularly whether those they hold data from, are continuing to agree with that (Laybats & Davies, 2018). Moreover, the regulation is designed to protect individuals from having their personal data collected without their consent or without them even knowing about it. This part is fundamental for this research and will be elaborated on in the following section. Finally, the GDPR has six general data protection principles: transparency, data minimization, storage limitation, accuracy, confidentiality, and purpose limitation (Mohan et al. 2018).

2.4 Theory: Calder and the GDPR as a theoretical framework

In order to conduct this research, it is important to establish a theoretical framework to illustrate whether or not a certain case of facial recognition used in public spaces is in line with the GDPR. However, since no proper literature has been produced regarding the use of facial recognition in public spaces and its relationship to the GDPR, it is very difficult to acquire an appropriate, already existing theory. Therefore, a new framework will be attempted to be formulated that measures the correlation between the main concepts. For this model, the GDPR's six general data protection principles as Calder (2016) has formulated them will be considered and will be converted into a model that shall test if facial recognition in public spaces is or can be GDPR-compliant. Additionally, to increase the reliability of the six data principles and to understand how they may be matched, the articles that are the most relevant for each

principle will be briefly mentioned and specified. In order to assess if the model functions properly as a tool to find out if facial recognition in public spaces without people's consent is or can adhere to the GDPR, a case from the Netherlands will be applied to the model and this will eventually lead to a valid conclusion.

First of all, it is important to note that Article 5 of the GDPR outlines six general data protection principles that should be applied to any collection or processing of personal data. Calder (2016) explains these principles as follows:

1. Lawful, fair and transparent processing of personal data.
2. The collection of data can only be for specified, explicit and legitimate purposes.
3. Data must be adequate, relevant and limited to what is necessary for processing.
4. The personal data must be accurate and kept up to date.
5. Personal data through which a subject can be identified cannot be kept longer than is necessary for processing.
6. Personal data must be processed so that it ensures security.

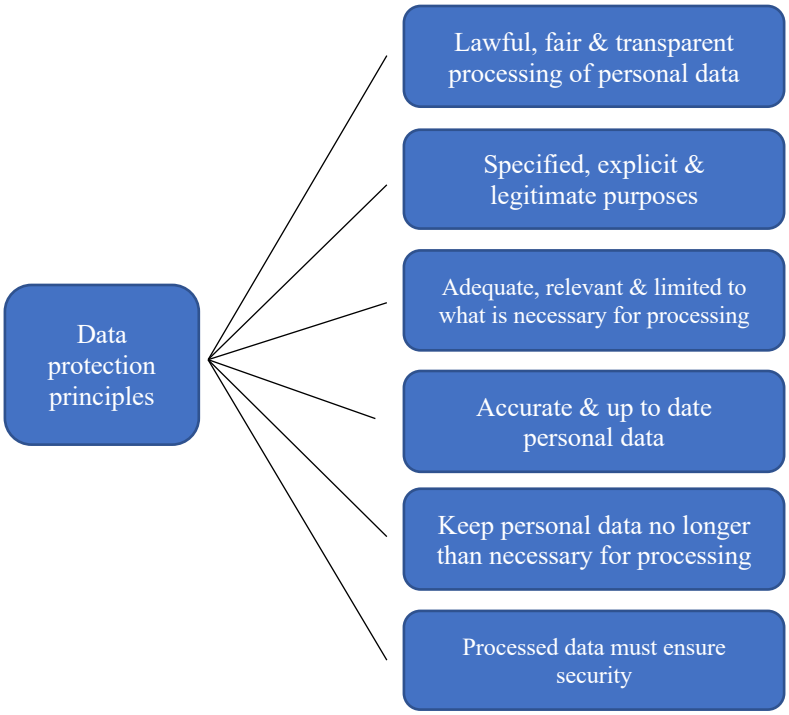

Figure 1: The six general data protection principles that should be applied to any collection or processing of personal data

If organizations match these six principles, it is likely that they are in a good position to meet the GDPR compliance requirements. However, it should be noted that this is not always the case, because there is a realistic chance that organizations eventually encounter aspects of the regulation that they did not account for. For this reason and to strengthen the model, a number of relevant articles that are significant for the six general data principles mentioned before, will be selected from the GDPR and the case will be applied to them in the fourth chapter. Moreover, adding these specific articles will provide a clearer understanding of how the six data principles may be achieved, it will impose more credibility and reliability to the model, it will elucidate the legal aspect of the principles, and by linking the actual regulation to the principles the framework will overall become more complete. For each data principle, one or two articles will carefully be selected on the basis that they shall be followed in order to match that particular principle. Before this is done, some clarifying definitions of terms used in the regulation will be provided, since they may initially be unclear to the reader.

One of the most important terms used in the GDPR and in this research is personal data. Therefore, it is key to have a clear definition of what exactly is meant when the term is mentioned. As stated in Article 4 of the regulation, personal data is defined as "any information relating to an identified or identifiable natural person ('data subject')" (GDPR, 2016: 33). The data subject can be identified, directly or indirectly, particularly by reference to an identifier such as a name, an identification number, an online identifier, or location data. Additionally, a natural person may be identified by reference to their biometric and behavioral features or factors specific to the physical, genetic, mental, physiological, economic, social or cultural identity (GDPR, 2016).

A second term that is fundamental to understand is processing, which is defined as any operation that is performed on personal data or personal data sets, whether or not by automated means, including the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, dissemination or otherwise making available, combination, restriction, erasure or destruction (GDPR, 2016). When the processing of personal data is automated and consists of the use of personal data to evaluate certain personal aspects relating to a data subject, it is called profiling. Profiling is generally performed to predict or analyze aspects concerning that data subject's economic situation, performance at work, personal preferences, interests, behavior, health, reliability, location or movements (GDPR, 2016).

Data processing is usually carried out by two different entities that each play their own role in the process. The first of these two entities is the controller, which alone or jointly with others determines the means of the data processing. The second entity, the processor, processes data on behalf of the controller (GDPR, 2016).

Finally, since this research and the regulation mention consent multiple times, this is also a very important term to clearly define. According to the GDPR consent is "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (GDPR, 2016: 34). This entails that, in the first place, the data subject should be aware that their data is being processed and secondly, the subject has to freely give an indication that they agree to the processing of their personal data.

In the following section a brief description will be given of the article(s) that have been selected in order to provide a better understanding of each data protection principle.

Lawfulness, fairness and transparency

The first of the six general data protection principles that Calder mentions is that the processing of personal data should always be lawful, fair and transparent (2016). One of the main articles included in the GDPR that is aimed at ensuring that this principle is adhered to, is Article 6 'lawfulness of processing' (GDPR, 2016: 36). This article establishes what conditions make processing lawful, for instance if the data subject has given consent and if processing is necessary for compliance with a legal obligation, for the performance of a task carried out in the public interest, in order to protect certain vital interests of the data subject, or for the performance of a contract to which the data subject is party (GDPR, 2016). Furthermore, this article determines that Member States are free to maintain or introduce more specific provisions to adapt the application of the rules of the regulation as long as the basis for processing is laid down by Union law or Member State law to which the controller is subject. Finally, it discusses what the controller should take into account when processing for a purpose other than that for which the data have been collected if it is not based on the subject's consent or on a Union or Member State law (GDPR, 2016).

Specified, explicit and legitimate purposes

The second principle, which is that the collection of data can only be for specified, explicit and legitimate purposes, is enforced through Article 9 'processing of special categories of personal data' (GDPR, 2016: 38). This article is based around defining when processing shall be prohibited. This is the case when, for example, the processing of personal data reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or when biometric or genetic data and data concerning health is processed. Moreover, it establishes that the aforementioned criteria shall not apply when "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes" (GDPR, 2016: 38), when processing is necessary to protect the data subject's vital interests or those of another natural person where the subject is legally or physically incapable of giving consent. Finally, it states that Member States may maintain or introduce further conditions or limitations and it briefly mentions one exception that is not relevant for this study and will therefore not be elaborated on (GDPR, 2016).

Adequacy, relevance and limits

The third general data principle is that data must be adequate, relevant and limited to what is necessary for processing (Calder, 2016). Various articles deal with ensuring that this is the case, such as Article 13, which mentions that controller shall inform the data subject about the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing (GDPR, 2016). Another article that is relevant for this principle is Article 14, which ensures that where the controller intends to further use the processed data for a different purpose than the original, it shall inform the subject on that purpose in advance. In this case, Article 13 focuses on the information to be provided where personal data are collected from the data subject, while Article 14 stresses the information to be provided where personal data have not been obtained from the data subject (GDPR, 2016).

Accuracy and up to date

The fourth principle addresses that personal data must be accurate and kept up to date. The two most fundamental articles that link to this principle are Article 16 and Article 18. Article 16, 'right to rectification', ensures that the personal data remains accurate and up to date by providing the data subject with the right to "obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her" (GDPR, 2016: 43). Also, when taking the purposes of the processing into account, the subject shall have the right to have the

incomplete data completed. Article 18, 'right to restriction of processing', establishes that the data subject shall have the right to obtain a restriction of processing from the controller if the accuracy of the personal data is contested by said subject at least for a period so the controller can verify the accuracy of the personal data (GDPR, 2016). Finally, when such a restriction is in place, personal data may only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims, for the protection of another natural person's rights or in the public interest (after the subject is informed about the restriction being lifted).

Time period that data may be kept

Calder's fifth principle is that personal data through which a subject can be identified cannot be kept longer than is necessary for processing (2016). The two articles that are aimed at ensuring that this principle is adhered to are Article 13 and Article 17. Article 13, 'information to be provided where personal data are collected from the data subject', establishes that the controller shall always provide the data subject with information about the period for which the personal data will be stored, the criteria used to determine that period, and the existence of the right to request rectification or erasure of the data whenever a subject wants. Article 17, 'right to erasure', ensures that "the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay […]" when, for instance, the data is no longer necessary for the purposes it was collected for (Calder, 2016: 43).

Personal data for security purposes

The sixth and final principle indicates that personal data must be processed so that it ensures security of that data. Article 32 'security of processing' states that taking into account certain factors, such as the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of severity for the rights and freedoms of natural persons , the controller and processor must implement the appropriate technical and organizational measures to ensure enough security to eliminate the risks (GDPR, 2016). This is also to ensure confidentiality, resilience and integrity of processing systems or to restore the availability to personal data in the event of a physical or technical incident. Furthermore, Article 85 'processing and freedom of expression and information' establishes that Member States shall by law reconcile the right to the protection of personal data pursuant to the entire GDPR with the right to freedom of expression and information. This includes processing for journalistic, academic, literary or artistic purposes (GDPR, 2016). Both these articles are strongly linked to the sixth principle, since they are aimed at ensuring the security of personal data.

In the analysis chapter, the chosen case will be applied to these principles and articles that form the basis of the theoretical framework, and this will result in an answer to the main- and sub-questions of this research.

2.5 Hypotheses

Based on the aforementioned information some hypotheses can be formulated regarding the research question 'to what extent can the use of facial recognition technology in public spaces in the Netherlands be considered lawful in terms of the GDPR?'

Hypothesis I: The use of facial recognition technology in public spaces is generally done without people's consent, which is not allowed according to the GDPR. The data subjects have not given their permission for the data to be collected and stored, which is required according to the regulation. The method of collecting individuals' data without their proper consent is not GDPR-compliant and can therefore be considered unlawful.

Hypothesis II: If organizations want to become GDPR-compliant and want to use practices such as facial recognition in public spaces, they must consider every article and regulation mentioned in the GDPR. For instance, it should be made clear to the subjects that they are being monitored/recorded, what the purpose of the data collection is, what the data will be used for, and that they have complete power and control over their personal data.

3. Research design

When conducting a study, researchers will most certainly face various questions regarding the gathering and analysis of information. Such questions may include topics like the selection and collection of data, the selection of a conceptual framework, and the limitations of the research. These and additional questions determine how a study is conducted and affect its outcome (Resodihardjo, 2009). The aim of this chapter is to explain how this research was conducted, thus, allowing other researchers to repeat it and verify the findings. This chapter will start by addressing what research methods have been used in this study and why they were selected. The second section will address the selection of the case and the justification for this. The third section introduces the case, while the fourth and fifth section address how the data for this research was collected and how triangulation was achieved.

In the first chapter, two sub-questions were drawn up in order to acquire an answer to the following research question:

To what extent can the use of facial recognition technology in public spaces in the Netherlands be considered lawful in terms of the GDPR?

The sub-questions relate predominantly to the lawfulness of using facial recognition technology in public spaces according to the GDPR, but also to what could be done to improve this. Therefore, the GDPR will function as the framework for this thesis and hopefully it can be generalizable to the extent that other cases—also from other European countries, since the regulation applies to them too—can be tested through this model too. How more insight into these aspects will be obtained will be discussed in this chapter.

3.1 Research design

In order to come to an answer to the research question, qualitative research will be necessary. This is mostly due to the fact that this thesis is focused on questions related to 'how' and 'why' rather than finding certain statistics or specific numeric results. Qualitative research methods are, amongst others, case study analysis and document analysis. It is certainly possible to carry out only one of these methods, however, to increase the reliability of this research, a combination of these methods will be used.

The aim of this research is to combine a document analysis which will provide a more thorough understanding of the GDPR, with an analysis of a specific case of the use of facial recognition technology in a public space. In the previous chapter various GDPR articles have been listed and in the analysis chapter every point will be applied on the case in order to find out of the hypotheses are correct and what the answer is to the research question.

3.2 Justification of the research design and the logic of the case selection

For this specific research, I have opted for a case study that discusses a situation in which facial recognition technology was used in a public space and this brought some discussion with it. A case study can be very helpful when attempting to acquire very detailed information on a specific event. Since there exists a clearly defined regulation that applies to the location chosen

for this study (the Netherlands), it shall be tested if this regulation is truly being conformed to. There are also increasingly cases of the use of facial recognition technology in public spaces in the Netherlands that have led to much discussion and even initiated a debate on the lawfulness of this practice. Furthermore, very little research has been conducted on the actual lawfulness of using this technology in terms of the GDPR. Therefore, it seems like a logical choice to test whether this debate is justified, through the application of a real-life situation.

I have opted for a single rather than a comparative case study mainly because it will allow me to gain a very in-depth knowledge about the case, but also because the scope of this study does not allow space for more than one case study. A single case study can be very helpful when attempting to acquire detailed, specific knowledge and to test an empirical analysis for instance. Because this research is aimed at testing empirics, it is fundamental to pick a significant case. By conducting a case study, the aim is to place certain processes in their own context to understand their meaning (Esterberg, 2002). Such a design is preferable as case studies are regarded as more suitable to critical situations of which little is known. Yin argues that "case studies are the preferred strategy when 'how' or 'when' questions are being posed, when the investigator has little control over events and when the focus is on a contemporary phenomenon within some real-life context" (2003: 1).

There is always a trade-off that arises when discussing the validity of a certain research: by selecting multiple cases the external validity of the study will increase, however, the internal validity will diminish because the cases will have a less in-depth discussion. Thus, by choosing a single case study this research will have a higher internal validity.

The second method that will be used is document analysis. This provides more in-depth information about the specific subjects discussed in this research. Information gathered through this method differs from the literature used for the previous chapter because these findings do not need to be academic. Several newspaper articles can be examined in order to gain more detailed knowledge about the selected case. Also, articles and books by academics and practitioners and a report on the GDPR will be studied. The most fundamental document for the research is the EU GDPR. Examination of this regulation will offer more insight in what it specifically states, to whom it applies, and what happens if it is not obeyed to. While regulations might often be vaguely written, its explanatory form will help to understand what the European Union's government officials mean with the GDPR.

3.3 Case

Having explained why a single case study is a viable option for the aim of this research, this section will address what I looked for in the case, what exactly the case is and why it is appropriate.

For this particular research, I looked for a case in the Netherlands, that occurred fairly recently (after the adoption of the GDPR), was much-debated, and would be applicable on a larger scale. The case that was eventually decided upon is that of secret facial recognition cameras in billboards at certain Dutch train stations. This case is unique, because it is one of the only known cases of the use of facial recognition technology in a public space, fairly briefly after the introduction of the GDPR, that was not carried out with the intention to enhance security, but rather for marketing purposes. Since the GDPR tends to make exceptions in cases that facial recognition acts as a means to protect citizens and improve their security, this case is unique because it is unlikely to fall under one of these exceptions. Moreover, it is unique because it gained a lot of (social) media attention and initiated some awareness among individuals that these practices exist in real-life. The case was heavily criticized in the Netherlands and is universally applicable because it could have happened at any station in the country (or abroad).

What happened, was that in September 2017, it was discovered that multiple 'smart billboards' were spread across several NS (Nederlandse Spoorwegen or Dutch Railways) train stations. Someone tweeted that they had found that there was a tiny, hidden camera inside a digital billboard at Amersfoort station. A few hours after this tweet, the NS made a statement confirming that advertisers monitored if and how long by passers looked at the advertisements depicted on the pillars through these cameras. Soon, it became clear that Amsterdam Central Station also contained various of these billboards or 'advertising pillars'. Apparently there was a system incorporated in the pillars that belong to Dutch billboard operator Exterion. The pillars contained hidden cameras and were equipped with the so-called technology VidiReports, developed by an American company named Quividi. The VidiReports can be considered facial recognition technology because it is able to automatically detect every passing person's face and therefore, identify exactly who looks at the advertisement (Sondermeijer, 2017). In a tweet, the NS confirmed to have an agreement with Exterion on the use of these 'smart billboards'. The billboard company even verified that around this period, 35 of these screens were installed at Amsterdam Central Station. In total, about 50 of the 750 pillars that Exterion owns contain the active facial recognition cameras. The main reason that these cameras were placed was to

measure how many and what type of people looked at the advertisements depicted in the pillars and for how long they looked at them. Although it was established that the used technology is able to detect faces and therefore, identify people, Exterion initially claimed that the cameras were only able to recognize the gender, age, mood and ethnicity of the passing individuals. This would allow the advertisers to depict ads for the specific area and/or audience.

According to the Dutch newspaper AD, Maatschappij Voor Beter OV claims that Exterion shared an article explaining how the technology works (Koenes, 2017). As stated in this article, the cameras can detect not only gender and age, but also mood and ethnicity (Sondermeijer, 2017). After the this system began receiving a lot of negative comments regarding privacy and legitimacy, Exterion and NS changed their statements and announced that the cameras were more like sensors because they measured behavior and did not generate any proper images (Koenes, 2017). Even though the billboard supplier claimed that collected data could not be linked to specific people, that it did not monitor emotion and that the data was not stored, many are not convinced that this is just a harmless procedure. Finally, NS stated that they had investigated if the use of the facial recognition cameras was in line with the privacy rules and they concluded that everything was completely legit. Therefore, most of these smart billboard are still in use.

The majority of the criticisms involved concerns about the lawfulness of using this facial recognition technology, especially, with regards to privacy law. First of all, Maatschappij Voor Beter OV expressed their concerns about the fact that recordings made through the billboards could be used—or potentially misused—by unqualified employees working for advertising agencies (Koenes, 2017). Furthermore, several news reports, including those by the AD and NOS, state that according to the Autoriteit Persoonsgegevens (the Dutch data protection authority) it is prohibited to use cameras in public spaces without people being aware of it, especially for commercial ends (Schellevis, 2017). Moreover, Dutch civil rights organization Bits of Freedom thinks this is problematic because due to the facial recognition being used in a public space and being allowed by the NS, it is impossible for passengers to withdraw from it (Schellevis, 2017). Although Exterion claims that they did not store the data, the Autoriteit Persoonsgegevens stated that by filming individuals, their personal data is automatically processed, which is prohibited according to the law. Finally, it was heavily criticized that the individuals watching the advertisements or passing by had no clue that they were being filmed.

The smart pillars showed no indication or warning that they contained facial recognition cameras and individuals had no idea they were being monitored (Sondermeijer, 2017).

3.4 Data analysis

As mentioned before, the data for this study will be examined through two methods: case study and document analysis. During the document analysis, one specific legislative document—in this case the General Data Protection Regulation—will be analyzed in order to get a thorough insight into the aspects and the model that has been developed. Especially the GDPR will be systematically analyzed, followed by some newspaper articles. As stated in chapter two, not only the six general data protection principles mentioned in the GDPR will be used, but some additional, relevant articles have been selected and linked to the principles as well. This has been done to provide a clearer understanding on when the principles are achieved, to increase the reliability of the research and avoid any coincidences in the case study analysis. The more sections of the GDPR the case can be applied too, the higher the chances of obtaining a trustworthy result. The additional articles have been selected on the basis of the topic they cover and its relevance for the six general data principles. This case was problematic in the first stage of the data processing—how is the data obtained—and its information to the data subjects. Therefore, articles have been chosen that stated data subjects' rights, consent, the collector's responsibilities towards the subject, and how to achieve lawfulness in this case. While analyzing the documents and the case, clear answers to the sub-questions and main research question can be formulated.

3.5 Triangulation, reliability & validity

By performing qualitative research, an attempt is made to provide objective observations as much as possible. When looking at the data gathered about the case, there were different newspaper articles that all provided information on the case. This allowed for a more detailed description of what happened in terms of the event, the actions that followed and some of the thoughts of actors involved. In order to improve the quality of the data used in this study, the method of triangulation will be used. As Yin states "the most robust fact may be considered to have been established if three (or more) sources all coincide" (1993: 69). Therefore, in this study, data was collected from various sources: most importantly newspapers, academic articles and a Parliamentary document. The aim is to only use data from a source if it was confirmed by two other sources (Resodihardjo, 2009). For instance, the information written in one

newspaper article shall be checked and confirmed by at least 2 other newspaper articles. By using multiple sources any bias in sources will hopefully be counteracted. “Triangulation helps to reduce this bias—if present—by forcing the researcher to rely on multiple sources of information when building a case (Resodihardjo, 2009: 48). Furthermore, using these different sources and looking at different perspectives together with a very in-depth examination of the case will increase the internal validity. However, by choosing only one case and one regulation, the findings of this research can only be generalized to other situations to a certain extent, hence, a lower external validity. Finally, the in-depth analysis of the case and the use of several varying sources and research methods, will rule out coincidences and with that, enhance the reliability of this study.

4. Analysis

In this chapter the most significant facts and factors will be drawn from the case and will be compared to the GDPR. This will be done systematically by, again, following the structure of the six general data principles and the articles linked to them, which have also been used in the previous chapters. By defining the different fundamental factors from the case and laying them out next to the six data principles and their articles, it should become clear whether this use of facial recognition technology in a public space may be considered lawful or not based on the information that is available. In doing so, first, the lawfulness, fairness and transparency of the data collection will be examined, followed by looking into the (specified) purposes and the adequacy, relevance and limits. Then, the accuracy will be considered, followed by a close look at the time period that the data can be kept. Lastly, it will be determined whether or not the security of the personal data has been ensured. To increase the reliability and objectivity of this study, the process of triangulation shall be carefully considered during the analysis. Some possible adjustments will briefly be addressed that may increase the lawfulness of this and similar cases and may hopefully serve as a recommendation for future uses of facial recognition technology in a public space. In the final section of this chapter there will be a discussion about the possible limitations encountered during the writing process, including the lack of the available information and how this may be surmounted.

4.1 Brief overview of the case's key facts

In order to properly delineate all the facts, it is key to compare the articles written about the NS case by varying newspapers. Providing a brief overview of the fundamental facts will facilitate the comparison of the case to Calder's six general data principles and the GDPR. The newspapers that wrote articles on this case and are therefore relevant for this research are the AD, Trouw and NRC. As news outlet NOS has covered the NS case as well, this has also been selected as one of the main sources and will be included in the comparison.

All four articles describe that a passenger unexpectedly noticed a small, hidden camera in a billboard at the NS train station in Amersfoort. After the passenger posted a picture of the camera hidden in the billboard on Twitter, the case received a lot of (negative) attention and the NS reacted with a statement saying that these cameras made recordings to monitor if and for how long individuals watched the advertisements displayed on the billboard. However, due to many negative reactions, the NS altered its statement, claiming that the cameras were actually not able to make video recordings but were more like a sensor. Exterion, the billboard company, first stated that the devices merely worked as sensors that registered how many people watched the advertisements and for how long. However, after the devices were found to be equipped with the facial recognition software VidiReports, which is known to be able to automatically detect every passing person's face to determine whether it is looking at the advertisement or not, and is able to immediately determine this person's gender and age, ethnicity and mood, the company altered their statement. Exterion declared that the devices technically were actual cameras with the ability to record, but they prefer to use the term sensors because they were not being used as regular cameras and the quality supposedly was not high enough to identify specific individuals and therefore, threaten their privacy. Moreover, Exterion claimed that their billboards are ethically appropriate since they did not store any of the collected data and individuals could not be traced back through the data. All the newspapers that covered this topic agree that the most problematic part of the case is the fact that there was no warning or information at all that the passengers were being recorded or that their data was being collected, which is especially important because train stations are essentially places that many people have to walk past or through. Several organizations, such as De Maatschappij Voor Beter OV, the Autoriteit Persoonsgegevens and Bits of Freedom have placed some question marks and expressed their concerns, especially regarding the possible abuse of the data by non-screened employees of advertising agencies, the lawfulness of using cameras in public spaces for publicity purposes, possible infringements on the

privacy law, and passengers being unable to withdraw from being recorded because they are not aware of it in the first place.

It is important to note that the case remains fairly difficult, because different organizations have varying perspectives on issues such as ‘is filming individuals without their consent still an invasion of privacy if they cannot be recognized due to the very low quality of the recorded images?’.

In the following section the most appropriate facts will be linked to the six general data protection principles that have been explained in the second chapter, in order to discover if and how the case adheres to the principles, and ultimately define whether to case may be considered lawful or not.

Lawfulness, fairness and transparency

To adhere to the first general data protection principle it is highly fundamental that the processing of personal data is being done in a lawful, fair and transparent manner. In the second chapter, this principle has been explained and it was established that Article 6 of the GDPR, ‘lawfulness of processing’, is aimed at ensuring that this principle is being adhered to. Some fundamental conditions that are necessary to ensure lawful, fair and transparent processing include guaranteeing that the data subject has given consent for the collection of their personal data and establishing a valid reason for this. When looking at the facts about the NS case, it immediately becomes clear that neither Exterion, nor the NS has provided any information to the passengers about these smart billboards. According the NOS article, Guy Grimmelt from Exterion, has stated that the devices “are technically cameras, but we prefer to call them sensors because they are not used as regular cameras” (Schellevis, 2017). However, this was not clear to individuals and they had no idea that they were being recorded, or that their behavior was possibly being monitored together with their personal data potentially being collected. The billboards also did not have a (clear) warning that they contained a technology that made it possible for them to define someone’s age, gender and ethnicity by detecting people’s face through a hidden camera as they passed by. Taking this into consideration, it can certainly be concluded that individuals whose personal data was collected at the Amstelveen train station had not given their consent for this to Exterion or the NS.

In addition to this, the passengers were not made aware of the purposes their data was collected for. Article 6 mentions that data processing becomes lawful when the purpose is clearly known, valid and justified, for instance when one of the following applies: it is necessary for compliance with a legal obligation to which the controller is subject, for a task carried out in the public interest or in order to protect certain vital interests of the data subject. Small exceptions may only be granted to processing carried out by public authorities in the performance of their tasks, which is not the case here. In this case, NS and Exterion stated to AD that "with these cameras advertisers check if the passengers watch the advertisements and for how long they watch it" (Koenes, 2017). Moreover, Grimmelt told NOS that "these devices work better than older sensors, because several people can be monitored at once" (Schellevis, 2017). This is all done for commercial ends and with the specific aim of enhancing the accuracy of the advertisements and therefore, the marketing performance of the company. Since the data subjects were completely unaware of the cameras in the billboards and of the processing of their personal data, it can be established that they also were not aware of the aforementioned purpose that required the collection of their data. From the analysis of these facts it can be concluded that the first general data principle has not been adhered to by Exterion or the NS and that the processing of data has not been carried out in a lawful, fair and transparent manner. For this principle, the question marks posed by various organizations are justified and Exterion's approach can be considered somewhat problematic.

Specified, explicit and legitimate purposes

The second general data principle is that the processing of data is only allowed for specified, explicit and legitimate purposes. Article 9 of the GDPR, which is aimed at the enforcement of this particular principle, indicates exactly when processing of data shall be prohibited. In the article it is stated that processing of personal data revealing racial or ethnic origin, political opinions or philosophical beliefs shall be prohibited. This is also the case for the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning a natural person's health or sexual orientation. Additionally, article 9 recites several cases that serve as exceptions and make the aforementioned types of data processing allowed. The processing of certain types of data that would normally be prohibited, may be permitted if the data subject had given explicit consent to the processing of those personal data for one or more specified purposes, when processing is necessary for carrying out obligations of the controller or subject in the field of social security, to protect a natural person's vital interests,

for the establishment, exercise or defense of legal claims, for the purpose of preventive or occupational medicine, or for reasons of substantial public interest.

In the case of Exterion, it is clear that the billboards contained the VidiReports software, which can be considered facial recognition, because it is able to automatically detect every passing person's face and therefore, identify exactly who looks at the advertisement. The technology then is able to determine this person's age range, gender, mood and even ethnicity. On Twitter, NS posted that "with these cameras promoters monitor if passengers look at their advertisements and if they do, for how long" (Koenes, 2017). Even though later, Exterion claimed that the function to measure an individual's mood had not yet been enabled on these specific billboards, they were indeed able to map at least the individual's face, gender and age. Therefore, it can be concluded that in this case the genetic and biometric data were processed together with data that may reveal racial or ethnic origin, which is prohibited according to Article 9 of the GDPR. Furthermore, the Autorteit Persoonsgegevens has stated that "collecting personal data for commercial ends is not something that can easily be done" (Sondermeijer, 2017) because there are many strict rules for this, such as informing the data subjects, asking them for permission and limiting the amount of data that is collected. Article 9 confirms this by stating that the aforementioned criteria for processing data shall not apply when the data subject has given explicit consent to the processing of those personal data for one or more specified purposes. Again, this was not the case for Exterion's billboards, sine the data subjects were not even aware that they were being filmed and that their data was being collected. Finally, the remaining exceptions mentioned in Article 9 did not include the processing of data for commercial or any situation that applies to the Exterion case. From this passage it can be concluded that the second general data principle has also not been adhered to by Exterion or the NS and that the processing of data has not been carried out with a specified, explicit or legitimate purpose.

Adequacy, relevance and limits

To adhere to the third principle it is important for the processing of data to be relevant, adequate and limited to what is necessary for processing. In chapter two this principle has been explained more extensively and it was mentioned that numerous articles deal with ensuring that this principle is being obeyed to. The two most significant articles that have been chosen for this analysis are Article 13 'information to be provided where personal data are collected from the data subject' and 14 'information to be provided where personal data have not been obtained

from the data subject'. Article 13 of the GDPR is aimed at ensuring that where personal data are collected the controller shall inform the data subject about its own identity and contact details, about the purposes of the processing for which the data are intended, the recipients of the data, the period for which the data will be stored, and the existence of the right to request access to and rectification or erasure of the data to the controller. Article 14 states that the same information shall be provided where personal data have not been obtained from the data subject and where the controller intends to further use the processed data for a different purpose, the subject shall be informed of that purpose in advance. When looking at the facts about the Exterion/NS case, it can be fairly easily established that the majority of the mandatory information that shall be provided to data subjects when their personal data are collected or have not been obtained, has not been provided. As mentioned several times before, neither Exterion, nor NS, offered any information to the passengers about the existence of cameras in the billboards, what these cameras did, and for what purpose this was done. Both companies claimed that "no secret recordings were being made" and "no images were generated" (Koenes, 2017) and therefore believed it was unnecessary to provide the proper information. Moreover, since the data subjects were unaware of the practices, they were also not aware of the collector's identity or contact details, its intentions, the recipients of their data, and their right to request access to and rectification or erasure of their data. Therefore, it can be determined that Exterion and the NS have not conformed to Article 13 of the GDPR. Since Exterion has claimed that they "conform completely to the privacy legislation and would never infringe the privacy rules" (Koenes, 2017) and that the collected data has not been further used for a different purpose, it cannot be concluded if Article 14 has or would have been violated as well. Finally, from the available information it may be established that the case is partly inconsistent with the third general data principle.

Accuracy and up to date

To conform to the fourth principle it is fundamental that the personal data is accurate and kept up to date. As stated before the second chapter of this thesis, Article 16 'right to rectification' and Article 18 'right to restriction of processing', are aimed at ensuring that data remains accurate and up to date. Article 16 mentions that the data subject shall have the right to obtain the rectification of inaccurate data concerning him or her from the controller, without undue delay. In this case, both the NS and Exterion released statements in which they claim that the devices "are technically cameras but were not used as regular cameras, rather as sensors" (Schellevis, 2017). As opposed to what is known about the VidiReports technology that these

billboards contained, Exterion finds that their billboards are 100 percent ethically acceptable because according to them, “no images (or at least clear recordings of individuals) were generated or saved” (Koenes, 2017) and specific people could not be traced back through the collected data. Even though the Autoriteit Persoonsgegevens argues that monitoring someone for commercial purposes is already prohibited they find it difficult to pronounce if any actual rules have been broken. On the other hand, professor Nico van Eijk (University of Amsterdam) argues that, contrary to what Exterion claims, the collected data can never remain completely anonymous because “if you would combine the data with a different database, people could definitely be traced back from it” (Sondermeijer, 2017).

However, since the data subjects were unaware of the collection of their data and the purposes of it, they had no knowledge of whether their data was accurate or not and therefore, could not make an appeal to their right to obtain rectification of potentially inaccurate data concerning them as affirmed in Article 16 of the GDPR. Likewise, data subjects had no knowledge of the accuracy of their data, the lawfulness or purpose of the processing and again, they were unaware they could appeal to Article 18 of the GDPR, which gave them the right to obtain restriction of processing from the collector in certain instances. According to Exterion the collected personal data was not stored, which would essentially mean there were no issues with the accuracy of the data or with keeping it up to date. However, data subjects were unaware that they were being monitored and they had not given their consent, thus signifying they were unable to make an appeal to the right they had according to Articles 16 and 18. In conclusion, this case partly adheres to the fourth general data principle in keeping the data up to date, but not so much in the accuracy and acquaint subjects with their rights.

Time period that data may be kept

The fifth general data principle addresses that personal data through which a subject can be identified cannot be kept longer than is necessary for processing. The GDPR articles concerned with ensuring that this principle is being adhered to are Article 13 and Article 17 ‘right to erasure’. First of all, this principle mentions ‘personal data through which a data subject can be identified’. This is a somewhat challenging point of discussion, since Exterion and the NS asserted that the cameras were not working as cameras but rather as sensors that registered images “of too little quality to be considered facial recognition” (Koenes, 2017). Also, they find their billboards to be 100 percent ethically appropriate, because according to them no recorded images were being stored and that it is not possible to trace specific individuals back from the

collected data. This, again, opposes the facts that are known about the VidiReports technology (that was installed on Exterion's smart billboards), which are that this system is also utilized as a tracking system. Although this technology is supposedly able to "automatically detect the faces of the passengers and determine who watches the advertisements" in addition to "establishing their age, gender, mood and even ethnicity" (Sondermeijer, 2017). Nevertheless, Exterion claims the data collected by their billboards remains fully anonymous and that they do not store any of the data. Although this seems to be positive, there is a downside, which is that both Article 13 and 17 were unknown to passengers because they were being monitored without being aware of it or giving their consent. No information was provided to the data subjects and therefore they were unaware of their right to obtain the erasure of their personal data without undue delay from the controller (Exterion in this case).

Nonetheless, considering the information that is available and assuming Exterion is being truthful in their statements and explanations about this system, it can be established that they adhere mostly to the fifth general data principle. They assure that data was not stored longer than necessary for the purposes it was collected for (or at all).

Personal data for security purposes

To adhere to the sixth and final general data principle it is key that personal data must be processed so that it ensures the security of that data. In the second chapter, this principle has been extensively explained and it was determined that Article 32 'security of processing and Article 85 'processing and freedom of expression and information' are both aimed at ensuring that this principle is being conformed to. Given that Exterion claims they do not store the personal data that they collect via their smart billboards, information about the level of security of the data is very little to none. From the previous section it became clear that Exterion has not properly informed data subjects about their rights and freedoms, which makes it difficult to determine whether the appropriate technical and organizational measures have been taken in order to ensure maximum data security. Risks such as unlawful destruction, loss, unauthorized disclosure or alteration of personal data continue existing and it is nearly impossible to regulate if Exterion has applied the proper security measures to protect this data, with the company providing so little information about this part of the process. Article 85 mentions some cases in which the right to the protection of data has to reconcile with the freedom of expression and information. This is usually necessary when processing is carried out for journalistic purposes

or the purpose of academic, artistic or literary expression. In the case of Exterion/NS Artcile 85 is less applicable because they initiated the processing for commercial ends.

Therefore, it is very difficult to conclude whether or not Exterion and the NS adhered properly to this principle. The lack of information available on this part of the data processing elicits a challenging analysis. In order to remain reliable and truthful and not create false accusations it will be concluded that it cannot be determined if the Exterion cases adheres to the sixth general data principle or not.

4.2 Findings

From the preceding analysis some conclusions can be drawn regarding the research questions and the hypotheses presented in the second chapter of this thesis. The first hypothesis refers to the use of facial recognition technology in public spaces without people giving their consent for it and that this is not GDPR-compliant. By using the six general data principles combined with the relevant GDPR articles and applying the Exterion/NS case to these principles, it has become clear exactly to what parts of the GDPR the case adhered or not. Regarding the first hypothesis, the analysis has proven that in this case the recording and data processing has been carried out without the data subjects being aware of it, making it impossible for them to have given their permission. Consent is an issue in a substantial part of the GDPR and in at least three of the general data principles. Therefore, the assumptions made in hypothesis one can be confirmed due to this analysis.

The second hypothesis states that organizations have to carefully take each article and regulation mentioned in the GDPR into account if they want to apply practices such as facial recognition technology in public spaces in a way that is considered GDPR-compliant. This analysis has shown that it is indeed fundamental to consider each and every principle to become fully GDPR-compliant and lawful. This includes making clear to the subjects that they are being monitored/recorded, what the purpose of the data collection is, what the data will be used for, and that they have complete power and control over their personal data. However, the case has also revealed that companies may get away with unlawful processing. Exterion was able to secretly use these cameras, monitor passengers with them and collect personal data without anyone noticing it for a certain period of time. Also, after the Autoriteit Persoonsgegevens and additional organizations found that these practices were not GDPR-compliant, there still was

no further investigation into the case, no sanctions for the companies involved, and the cameras did not even have to be removed from the billboards.

Finally, the analysis has proved that Exterion's did not adhere to all general data principles with its use of smart billboards. Worse still, three of the principles were not adhered to at all and the remaining three were merely partly adhered to. Therefore, it can be concluded that the answer to the research question 'to what extent can the use of facial recognition technology in public spaces in the Netherlands be considered lawful in terms of the GDPR', is that in this case it cannot be considered lawful in terms of the GDPR, because half of the six general data principles were not adhered to, meaning that some GDPR articles were also violated.

4.3 Limitations

It is highly fundamental to realize that there are some limitations regarding this thesis. In the first part, some of the limitations of chapters two and three will be discussed and in the second part, the most challenging limitations from chapter four will be considered.

For this study, one specific case has been carefully selected because it is a clear representation of the (potentially unlawful) use of facial recognition technology in a public space in the Netherlands. By adding various articles to the six general data protection principles and to the theoretical framework, the case could be applied to more varying sections of the GDPR, which will allowed for a more accurate conclusion and more reliable study in general. Nevertheless, by only selecting some articles, a slightly distorted representation of the case may be given. For instance, since the case did not meet the principles or rules that these particular articles define, it might seem like the case is very negative and breaks all the rules, while it may very well obey to all the rules described in the other articles. Furthermore, the research may be repeated by others under similar circumstances. This study could be repeated in the sense that new, similar cases may be applied to the model established here and generate reliable results. Yet, the results of this particular case are not so generalizable, because every case has its own specific characteristics and these may lead to a different outcome than the one found in this research. As mentioned before, by providing a very in-depth analysis of one case, potential extraneous factors can be controlled and it can be made sure that these factors have no effects on the generated results. This means that the internal validity of the study increases. However, this also means that the external validity is lower. In the future the external validity may be increased by selecting more (three or more) cases and compare them to each other. Another limitation

can be the information that Exterion has kept from the public. The company has only provided the information about advertising pillars that they thought would be appropriate to share. This could mean that they acted in their own interest and withheld information that may have had negative consequences for them. Finally, for the case, there is no academic literature on it yet. This thesis will be the first academic piece to write about this particular case, which means that the majority of the information about it comes from Dutch newspapers. I am aware that this may be somewhat problematic, however, to counteract this notion, information from multiple respectable newspapers is combined with statements by large organizations in order to eliminate potential bias and increase the triangulation and the reliability of the information.

Regarding chapter four, it is especially important to consider that the varying newspapers contain information that was largely provided by Exterion and the NS themselves. It is evident that these companies do not want to create any negative images about themselves, which means there may be a possibility that they have not been 100 percent truthful in their statements. NS first declared that with the cameras found in the billboards advertisers were able to see if passengers watched the advertisements and for how long. However, after several negative reactions, the NS altered its declaration and said the cameras were not actual cameras but rather a type of sensor that measures behavior (Koenes, 2017). This also applies to Exterion, that released an initial statement and later altered it to something slightly different and possibly more favorable. When asked about the functioning of the device, Guy Grimmelt, who works for Exterion, literally stated to NOS “we prefer to call it a sensor, even though, technically it is a camera” (Schellevis, 2017). This quote is extremely interesting, because in fact they are contradicting their initial statement, in which they argue that no images were recorded at all. In this quote, Grimmelt actually admits the devices are cameras, but Exterion prefers to label them as sensors, possibly because the use of cameras would be more problematic than the use of sensors. When looking at the newspapers critically, this quote may be perceived as a typical example of Exterion trying to limit the damage after receiving significant criticism on them secretly recording/monitoring numerous individuals and potentially threatening their privacy in the process.

Furthermore, it is essential to understand that there is a chance that some of the information that can be found in the newspapers may be biased, because Exterion and the NS have given the statements that they decided upon and have shared the information they considered was appropriate to be shared, also about matters that cannot be checked properly. Therefore, it

should be carefully considered whether the communication provided by these companies is reliable or not. For instance, Exterion claims that none of the collected personal data is stored afterwards, but without any further research into it, it is quite unattainable to find out whether this statement is true or not. Additional investigations into the smart billboards, the devices hidden in there, the processing of the data and what happens with the data after it is used may be helpful to come to a more conclusive answer in the future. For this analysis, the information has been used as it was presented in the newspapers and with the assumption that Exterion and the NS have been truthful.

5. Conclusion

This chapter discusses the main conclusions of this thesis, as well as the further research possibilities.

Since the world is currently shifting to a pre-crime society, forestalling security risks through surveillance technologies is increasingly becoming a prevalent strategy. Especially biometric identification systems, such as facial recognition technology, are becoming prevalent recognition systems that are able to verify or identify people's identities based on their biometric features. Generally, this is done with the purpose of reinforcing overall security in different types of ways in private, but also progressively in public spaces. However, such new developments come with potential risks, which in this case may be an invasion of privacy or intruding into individuals' personal data. Given that biometric systems are becoming widely utilized in public spaces and their risks could lead to issues such as identity theft, the storage of biometric data and tracking or tracing individuals, it is fundamental to establish if such practices comply with the existing laws concerning this matter. Therefore, this study's aim was to research the lawfulness of the use of facial recognition in public spaces in the Netherlands. In order to define this, a specific case has been analyzed through the lens of the European General Data Protection Regulation (EU GDPR). Due to the GDPR being a rather large document with many varying aspects and articles that are not all as relevant for this study and the lack of appropriate, already existing theoretical frameworks, a model has been developed from the six general data protection principles that Calder (2016) explains. These six principles were linked to and combined with the GDPR articles that were most relevant for this research in order to form a more reliable framework. For the analysis, a specific case was selected and was then

applied to the six principles and their articles to determine to what extent it can be considered lawful.

From the analysis it became clear that, most importantly, the case does not adhere to all principles and therefore, cannot be declared completely lawful. The most problematic elements of the NS/Exterion case were that the recording and data processing has been carried out without the data subjects being aware of it or the purposes and without the billboards containing any warning, as required according to the first and second principle. Moreover, no further information was provided to the data subjects about what their data was used for, what would happen to their data after it had served its purpose and for how long it would be kept, withholding the subjects from making an appeal to their right to obtain rectification of potentially inaccurate data concerning them, the right to obtain restriction of processing from the collector in certain instances, or their right to obtain the erasure of their personal data without undue delay from the controller. This were also requirements for lawful processing, this time, mentioned in principles three, four and five. Due to a lack of the significant information it was not possible to determine if the case conformed to the sixth principle. From these findings, it can be concluded that the assumptions made in both hypotheses have been confirmed. Three out of the six general data principles were not conformed to at all, which leads the conclusion that the case cannot be considered lawful in terms of the GDPR. Still, it is important to mention that even though in this case Exterion did not fully adhere to any of the six principles and all of them contained elements that Exterion must most certainly improve, they did adhere mostly to the third, fourth and fifth principle, so the case cannot be affirmed completely unlawful.

This study has focused predominantly on one of the biometric systems, namely facial recognition technology in the public spaces in the Netherlands. Since very little academic literature exists linking this to regulations such as the GDPR, a framework had to be developed to make it possible to do so. It has succeeded in applying the specific case of Exterion to the model and determining whether the practices were lawful or not. Although the findings were produced from one particular case, they are somewhat generalizable. However, the framework and the results generated from it could become even more reliable and generalizable if more varying cases were to be applied to it. Finally, it would be interesting to look at the similarities and/or differences on how facial recognition technology is applied in public spaces and the lawfulness of it in other EU states. This goes beyond the scope of this research and thus future

research is encouraged to look further into this. For instance, a comparative case analysis between the Netherlands and a similar case in a different EU member state might be a potential start.

Bibliography

Agre, P.E. (2001). "Your Face in Not a Barcode: Arguments Against Automatic Face Recognition in Public Places. *Whole Earth,* 106: 74-77.

Aydogan, H. and E. Darcan. (2014). Facial Recognition Technology. In Harvey, K. *Encyclopedia of Social Media and Politics* (pp. 492-495). Thousand Oaks, CA: Sage Publications.

Bennett, K.A. (2001). Can Facial Recognition Technology Be Used To Fight the New War Against Terrorism?: Examining the Constitutionality of Facial Recognition Surveillance Systems. *North Carolina Journal of Law & Technology,* 3 (1): 151-174.

Buciu, I. and A. Gacsadi. (2016). Biometrics Systems and Technologies: A survey. *International Journal of Computers Communications & Control,* 11 (3): 315-330.

Calder, A. (2016). *EU GDPR: A Pocket Guide.* IT Governance ltd.

Esterberg, G. (2002). *Quantitative Methods in Social Research.* Salem: McGraw-Hill.

Fife, E. and J. Orjuela. (2012). The Privacy Calculus: Mobile Apps and User Perceptions of Privacy and Security. *International Journal of Engineering Business Management,* 4: 1-10.

Galič, M., et al. (2016). Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology,* 30 (1): 9-37.

General Data Protection Regulation (GDPR). (2016). *Official Journal of the European Union,* European Commission.

Gray, M. (2003). Urban Surveillance and Panopticism: will we recognize the facial recognition society? *Surveillance and Society,* 1 (3): 314-330.

Jones, P., et al. (2007). Biometrics in retailing. *International Journal of Retail and Distribution Management,* 35: 217-222.

Knopper, S. (2018, December 18). Why Taylor Swift Is Using Facial Recognition at Concerts. *Rolling Stone,* Retrieved from https://www.rollingstone.com/music/music-news/taylor-swift-facial-recognition-concerts-768741/

Koenes, R. (2017, September 4). Honderden reclameborden uitgerust met 'verborgen'camera. *AD,* Retrieved from https://www.ad.nl/amersfoort/honderden-reclameborden-uitgerust-met-verborgen-camera~aa5a1190/

Langenderfer, J. and S. Linnhoff. (2005). The Emergence of Biometrics and Its Effect on Consumers. *Journal of Consumer Affairs,* 39 (2): 314-338.

Laybats, C. and J. Davies. (2018). GDPR: Implementing the regulations. *Business Information Review,* 35 (2). 81-83.

Miltgen et al. (2013). Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. *Decision Support Systems,* 56: 103-114.

Mohan et al. (2019). Analyzing GDPR Compliance Through the Lens of Privacy Policy. Retrived from https://arxiv.org/pdf/1906.12038.pdf

Morosan, C. (2012). Theoretical and Empirical Considerations of Guests' Perceptions of Biometric Systems in Hotels: Extending the Technology Acceptance Model. *Journal of Hospitality & Tourism Research,* 36 (1): 52-84.

Resodihardjo, S.L. (2009). *Crisis and Chace in the British and Dutch Prison Services: Understanding Crisis-Reform Processes.* Farnham, UK: Ashgate Publishing.

Schellevis, J. (2017, September 4). Reclameborden op A'dam CS weten wanneer en hoelang jij kijkt. *NOS,* Retrieved from https://nos.nl/artikel/2191341-reclameborden-op-a-dam-cs-weten-wanneer-en-hoelang-jij-kijkt.html

Schouten, B. and B. Jacobs. (2009). Biometrics and their use in e-passports. *Image and Vision Computing,* 27: 305-312.

Shaikh, S.A. and J.R. Rabaiotti. (2010). Characteristic trade-offs in designing large-scale biometric-based identity management systems. *Journal of Network and Computer Applications,* 33 (3): 342-351.

Sondermeijer, V. (2017, September 5). Plotseling heft de reclamezuil ogen gekregen. *NRC,* Retrieved from https://www.nrc.nl/nieuws/2017/09/05/plotseling-heeft-de-reclamezuil-ogen-gekregen-12849487-a1572341

Trouw. (2017, September 5). Reclamebord bespiedt treinreiziger. *Trouw,* Retrieved from https://www.trouw.nl/nieuws/reclamebord-bespiedt-treinreiziger~b33e2918/

Woodward. J.D. (2003). *Biometrics: A Look at Facial Recognition.* Santa Monica, CA: Rand Corporation.

Yin, R.K. (2003). *Case Study Research: Design and Methods*. CA: Sage Publications.

Yin, R.K. (1993), *Applications of Case Study Research*. Thousand Oaks, CA: Sage Publications.

Zedner, L. (2007). Pre-crime and post-criminology? *Theoretical Criminology,* 11 (2): 261-281.