Double Degree Master 'Innovation Management, Entrepreneurship and Sustainability'
MSc. Business Administration & MSc. Innovation Management, Entrepreneurship and Sustainability

"Facial Recognition for Public Safety"

A supportive tool for the municipal decision-making process on using facial recognition for public safety, the FRPS risk governance method.

Author:

Roorda, Stephanie Anna Hermina

Supervisors:

Dr. R. Effing
Prof. Dr. M.E. Iacob
Dr. L.H. von Arnim
Dr. A.I. Aldea

Date:

11 January 2020

Word count:

16.528

Keywords:
Facial Recognition, Risk Governance, Public Safety

UNIVERSITY OF TWENTE.

Technische Universität Berlin

Preface

This Master Thesis is written for the Double Degree Master 'Innovation Management, Entrepreneurship and Sustainability'. It is the end report for the Master of Business Administration from the University of Twente and the Master Innovation Management, Entrepreneurship and Sustainability from the Technische Universität Berlin.

The topic of my thesis has been chosen based on my interest on the intersection of technical developments and organisational application. Based on this interest, I created a list of topics and further scoped it together with my supervisors to the topic it has become.
I would like to thank Robin Effing and Aldina Aldea for their feedback and motivational support during my thesis and thanks to Maria Iacob for taking over the role of second supervisor in the end phase of my thesis.

During my thesis, I was supported by PwC. They gave me the opportunity to write my thesis within their organization. I had access to a network of several experts and a supportive mentor. Therefore, I would like to thank my mentor from PwC for his good support, the Risk Assurance team of PwC Zwolle for their open attitude and nice work atmosphere, Jan Visser and Frank Versleijen for their valuable input for my research, and other people I spoke to and got inspiration from.

I would like to thank my family and friends for their emotional support and willingness to listen.
I discovered, during the writing this thesis, that if I cannot solve the puzzle, I need to talk about it which helps me in finding answers. Another point of learning is that I need to take decisions more quickly, in order to finish up my work.

I wish you a lot of reading pleasure.

Stephanie Roorda

Berlin, 29 November 2020

Abstract

One of the applications within the phenomenon of fast technological changes, is facial recognition. A facial recognition system uses face detection to identify a person. Facial recognition systems are being deployed in several areas including the area of public safety and recent application in relation to the global Covid pandemic. The application of facial recognition raises some concerns which resulted in the need for governance around this technology. Thus, the purpose of this study is to create a risk governance method, the Facial Recognition for Public Safety (FRPS) risk governance method, for decision making by municipalities in order to mitigate the risks around using facial recognition for public safety. The FRPS risk governance method gives an overview of the expected risks for municipalities on using facial recognition for public safety as a starting point towards assessing these risks. The FRPS risk governance method is developed based on a systematic literature research and a research from different expert perspectives in the areas of risk management, privacy, security, and/or facial recognition in order to elaborate on the knowledge which is found in the literature. Based on this research, the FRPS risk governance method is described in the analysis part and a visualization of the method is created and displayed in the sixth chapter. The method should be read as a method containing aspects within the risk governance process which need to be seriously considered.
After all, there should be taken into consideration that there should be further research on the method in order to further validate it and develop it into an applicable method.

Table of contents

1. Introduction

1.1 Situation

The world faces phenomena such as globalisation and fast technological changes. These phenomena affect several cities in their development (Giffinger, 2007). The globalisation, fast technological changes and the subsequent problems (such as traffic, pollution, security, privacy and crime (Voda & Radu, 2019)) affecting cities, resulted in the term smart cities coming up. The term smart cities is defined by Voda and Radu (2019) as cities who are motivated by problems to develop and implement intelligent solutions in order to achieve better sustainable development, growth and competitiveness.

A comprehensive concept within the smart city development is Artificial Intelligence (AI) because of its wide variety of possibilities in terms of technologies (Voda & Radu, 2019). AI seems to be applicable in different areas of smart cities stated by Voda and Radu (2019) as smart home, energy efficiency, security and privacy, government, healthcare, education and intelligent transportation. Additionally, it can be applied in different kind of forms defined as branches of AI by Voda and Radu (2019). On of the branches is Vision and contains the application facial recognition.

A facial recognition system uses face detection, an artificial intelligence-based technology, to identify a human face and subsequently, identifying the person (Rouse, 2020). Facial recognition systems are being deployed in areas such as access control, marketing and customer/retail services, healthcare, and security and public safety (World Economic Forum, 2020; Praveen & Dakala, 2020).

With the global Covid pandemic happening in 2020, countries have adopted several measures in order to tackle this global challenge through restrictions on travelling and transportation, measures for reducing mass mobility, social distancing and wearing masks (Aytekin, 2020; Sharma, 2020). After initial hard lockdowns taking place all over the world in spring 2020, countries were hoping to prevent further lockdown by using technologies like contact tracing and facial recognition (Fischer, 2020). For example, in Russia and China, facial recognition is used in order to tackle the Coronavirus.

In the case of Russia, facial recognition has been used during the lockdown of Moscow where it kept track of their residents (BBC, 2020). The system is able to detect crowds, social distancing, face masks and people who were ordered to self-isolate. This resulted in a lot of rule breakers being caught which is the positive result of this application. The argument about the positive effect is countered by concerns around this application like “where does the line between security, privacy, and freedom lie?”, even more when bearing in mind the history of the Soviet repression (Maynes, 2020).

Another critical example of balancing out the public health concerns with data privacy aims, in relation to the global Covid pandemic, can be found in China. In this case facial recognition is used for detecting temperatures in crowds and highlighting citizens when not wearing facemask. The article from Guardian indicates that excessive public monitoring around the Coronavirus is the first step for the Chinese government to further accelerate mass surveillance (Kuo, 2020). Along with this mass surveillance there is mass collection of personal data which can be dangerous given the perspective that China does not have stringent laws around the governance of this data (Kuo, 2020).

1.2 Public safety

For this research the area of focus is public safety. The definition for public safety in this thesis is composed based on the definition ‘security, access control and law enforcement’ from Praveen & Dakala (2020) and ‘safety and security of public spaces’ from World Economic Forum (2020). Public safety is defined as: the application field of safety, security and access control within public areas and events.

This area is chosen because of the relation to the current situation with the pandemic of the Coronavirus. In this situation, there is a need for: control of the implemented measures for preventing the spread of the virus, the protection of citizens and in the end tackling this pandemic (Fischer, 2020; Aytekin, 2020; Sharma, 2020). There are also examples of facial recognition within the area of public safety except from the ones during the occurrence of the global Covid pandemic.

In the United States, facial recognition is applied for the passenger check-in (Radu, 2019). This application has also been used at British Airlines with benefits such as faster boarding and sift out of security threats (Street, 2019). Practises like these have already led to passengers raising concerns about their privacy of data and identify, especially when the implementation of said practises is not made clear to the affected people (Street, 2019).

There are also some examples from European cities. In Germany, facial recognition is applied by the government at a railway station as an experiment (Delcker, 2019). Video surveillance is mentioned as something very important for supporting the police in tracing criminal and terror suspects (Delcker, 2019). On the other side, Delcker (2019) mentions that the experiment causes discussion around privacy concerns, especially taking into account the history of the country. Adding on that, there are comments from critics about the authorities being insufficiently transparent because there is so little information being shared with others.

In the United Kingdom facial recognition is applied by the police for detecting and preventing crime. It can support and reduce time in the identification process and minimize false arrests (Burgess, 2018). However, there seems to be a lack of transparency, regulatory oversight and accuracy about the way of working (Burgess, 2018).

In the Netherlands facial recognition is being implemented in a project by Schiphol Airport in Amsterdam (Schiphol, 2019). This implementation is used for passport control, opening entrance to the gates and entrance to departure lounge. Schiphol (2019) started this project in order to find a way to pass through the process of boarding more smoothly. An article about facial recognition and border control from Forbes (Martin, 2019) states that the technology causes concerns around people being watched and the data which might be hacked and results in more harm than good. Adding on that, the National Police of the Netherlands uses facial recognition systems for faster identification of suspects (Safran, 2017).
To conclude, there are different examples of applications of facial recognition, these applications are a great opportunity, yet they also lead to major public debate around data and privacy.

1.3 Concerns around facial recognition

Political parties are raising a variety of concerns regarding facial recognition and public safety.
The European Union (EU) points towards several undesirable consequences of the implementation of facial recognition technology in public spaces. An article on BBC (2020) suggests that the EU was considering banning facial recognition in public places for up to five years to give some time for development on actions against the undesirable effects. There seems to be limited information about the way and extent of using facial recognition technology and its consequences since the development of the technology is rapid and used by multiple actors (European Union Agency for Fundamental Rights, 2020). Adding to that, there is little known about the impact of the use of facial recognition on fundamental rights (European Union Agency for Fundamental Rights, 2020).
Subsequently, there have been some concerns by the Dutch government. To be able to take advantage of the opportunities that Artificial Intelligence (AI) can offer, there is a need for addressing the risks (Ministry of Economic Affairs and Climate Policy, 2019). Specifically, about facial recognition, there is stated that protection of privacy and maybe other privacy issues play a role. The Minister for Legal Protection even called for research into the privacy risks associated with facial recognition (Ministry of Economic Affairs and Climate Policy, 2019).

IBM declared that the company will stop the research, development and supply of facial recognition systems because of its use for mass surveillance and ethnic profiling. The IBM-director, Krishna (2020) hopes to trigger a discussion about whether and how authorities should use facial recognition. This indicates that there is a need to further research on this topic. Besides, Microsoft writes about the need for government regulation and corporate responsibility around the usage of facial recognition technology (Smith, 2018). Additionally, Microsoft President Smith announced they will not sell facial recognition technology anymore to police departments until there is a law in place, containing human rights, that governs the facial recognition technology (Magid, 2020). Following, Amazon announced that they will implement a moratorium on their facial recognition technology being used by police for one year (Magid, 2020).
At last, during the presence of the Coronavirus many countries have turned to facial recognition as described before in the examples. As stated by Oliver & Neenan (2020), many of these applications have been implemented without proper regulation. This raises the question 'what will happen when we get out of this Coronavirus situation?'(Oliver & Neenan, 2020).

1.4 The need for governance

As can be seen from the described concerns, there is a need for regulation around facial recognition. This debate also takes place on the level of Artificial Intelligence. This debate is in relation to the one focused on facial recognition since facial recognition is an AI application.
The question on how to govern AI is stated by Wirtz, Weyerer and Sturm (2020) as "as the number of AI applications is growing and the technology increasingly permeates everyday life, the question arises of how government and public administration should deal with the potential risks and challenges involved" (p. 819). Adding on that, Butcher and Beridze (2019) point out that development and implementation of AI comes with some ethical issues. "To ensure these issues are addressed, effective governance is required" (p. 96).

1.5 The research goal

The concerns around facial recognition for public safety, the need for governance and the need for further research on risks around facial recognition, bring us to the goal for this research. The aim of this research is to create a risk governance method, the Facial Recognition for Public Safety (FRPS) risk governance method, for decision making by municipalities in order to mitigate the risks around using facial recognition for public safety. The FRPS risk governance method gives an overview of the expected risks for municipalities on using facial recognition for public safety as a starting point towards assessing these risks.

1.6 The research questions

The research conducted in this paper, aims to answer the following questions:
"How should the FRPS risk governance method be designed to give support towards making a decision on using facial recognition for public safety?"

To structure the research, the central research question is divided into sub questions:

1. What risks can be identified for using facial recognition in the area of public safety?
The main goal of this sub question is to investigate the current state of the risks around facial recognition in the area of public safety. First, risks have been identified out of literature. Additionally, risks have been identified from different expert perspectives: 'the facial recognition expert and supplier', 'the expert municipal image recognition' and 'the experts security and privacy'. The experts identified risks based on their experience and the current state of risks from literature has been evaluated.

As an answer to this sub question, an overview is provided of the risks around facial recognition within the area of public safety based on literature and expert perspective. The results of this sub question serve as input for the FRPS risk governance method.

2. What are risk governance aspects for the municipal decision-making process on using facial recognition for public safety?
The purpose of this sub question is to identify aspects of risk governance addressed by literature. Consequently, essential aspects for a risk governance method for using facial recognition for public safety will be identified.
Additionally, within the conducted expert interviews, questions were raised regarding perspectives on municipalities using facial recognition within the area of public safety. The results have been used as input for developing the FRPS risk governance method.

1.7 Contribution to theory

This research has an added value for literature because it is filling a research gap found in literature as well as found in non-research articles.
The first gap identified in the literature is that there is no comprehensive overview of risks and how to deal with these risks yet. If there is no comprehensive overview of risks of using facial recognition for municipalities, wrong decisions could be made. These wrong decisions might result in undesirable effects which could probably be prevented.
Secondly, as several news outlets (Smith, 2018; Ministry of Economic Affairs and Climate Policy, 2019; BBC ,2020; European Union Agency for Fundamental Rights, 2020; Krishna, 2020; Magid, 2020; Oliver & Neenan, 2020) as well as literature (Butcher & Beridze, 2019; Wirtz, Weyerer & Sturm, 2020) find, there is the need for governance and regulations. The research of this thesis has an added value on a more specific level around the governance of AI, namely risk identification and assessment for facial recognition (Wirtz, Weyerer & Sturm, 2020). The AI governance with the specific level this thesis adds value to, is further addressed in the theoretical part of this thesis.
Additionally, Jalonen (2007) states a proposed solution for the issue of creativity and effectiveness of the decision-making within local government. Conflicting interests should be seen as triggers for activating interactions between actors of the process. The more dynamic the environment, the higher the need is for communication within the decision-making process and between the process and its environment (Jalonen, 2007). As can be seen from the introduction of different facial recognition applications, there are conflicting interests in this application area. Next to that, the application area is highly dynamic because of the fast technological developments. Having this said, the to be developed method might be supportive for the decision-making process within local governments and the highly dynamic environment with conflicting interests.

1.8 Contribution to practice

There are different parties who could benefit from this research.
As described in chapter 1.3, the EU and Dutch government point out that there is need for more information about the consequences of the way and extent of using facial recognition and for addressment of the risks around this technology. The result of this research contributes to charting of the undesirable effects by way of a risk governance method. Also, the results could add value to the development of public safety policies and the development around smart cities.
The resulting FRPS method can help improve decision making by making it possible to identify expected risks, avoid them and the undesirable effects.

Additionally, this topic provides added value for municipalities who can use the FRPS risk governance method for supporting their decision-making process on using facial recognition for public safety.

Experts in the field of facial recognition and public safety could use the FRPS risk governance method for a better understanding, research and advice. For example the supplier/developer/researcher of facial recognition will be able to better understand why potential customers would use or not use facial recognition. This could result in improved product development, research and sales.
Adding to that, the supplier/developer/researcher could recommend this research to the potential user to enable a better understanding in terms of deploying any technology in this field.

Experts/advisers can use the results of this research in order to improve their understanding of the risks, supplement their research about facial recognition and subsequently improve their advice to potential users of facial recognition within the public safety area.
Lastly, since this research is written with support from the consulting company PriceWaterhouseCoopers (Pwc), there will be future value for the respective company's consulting practise. PwC can be seen as an expert/adviser, so they benefit in the same way other experts would, as mentioned above. Specifically, there is an added value for PwC in gaining insight in the client processes. One of the questions PwC currently asks to clients, when they implement new technologies, is "what does the client do to cover risks or identify them?" (PwC, 2020)[1]. The result of this thesis might add value for PwC by supporting them and their clients in answering this question.

1.9 Outline

The second chapter is the methodology section, which describes the six activities from the design science research methodology are explained with the main idea of aligning and testing literature-based results with knowledge of experts. Next, there is some further explanation about the research sample, data collection method and data analysis. The third chapter consists of the literature research, containing a systematic literature review on risks, facial recognition and public safety. Furthermore, it contains a literature overview about risk governance. The fourth chapter displays the results from the expert perspective of this research. Then, the fifth chapter shows an analysis containing the literature and expert view together which results in the Facial Recognition for Public Safety (FRPS) risk governance method. The FRPS risk governance method is shown in chapter 6 together with a conclusion. At last, there is given the limitations and further research section.

[1] Source from internal meeting PwC (not publicly available).

2. Methodology

2.1 Design science research

This study is based on the design science research methodology for information system research by Peffers, Tuunanen, Rothenberger and Chatterjee (2007). The designs science discipline of this method is focused on creating an artifact, which is reflected in this research as the creation of the FRPS risk governance method. Then there is the information systems discipline which is reflected in this thesis by the concept facial recognition, which is an information technology.
Given that the agenda of public safety and facial recognition intersect, the design science research methodology for information system research fits to the research goal of this thesis and is therefore used.

2.2 Research design

The methodology consists of six activities. A visualization of these activities within the research design for this thesis, is made in the DSRM Process model which can be seen in figure 1. The main idea of the research design is aligning and testing literature-based results with knowledge of experts which will be further explained by the descriptions of the six activities below.

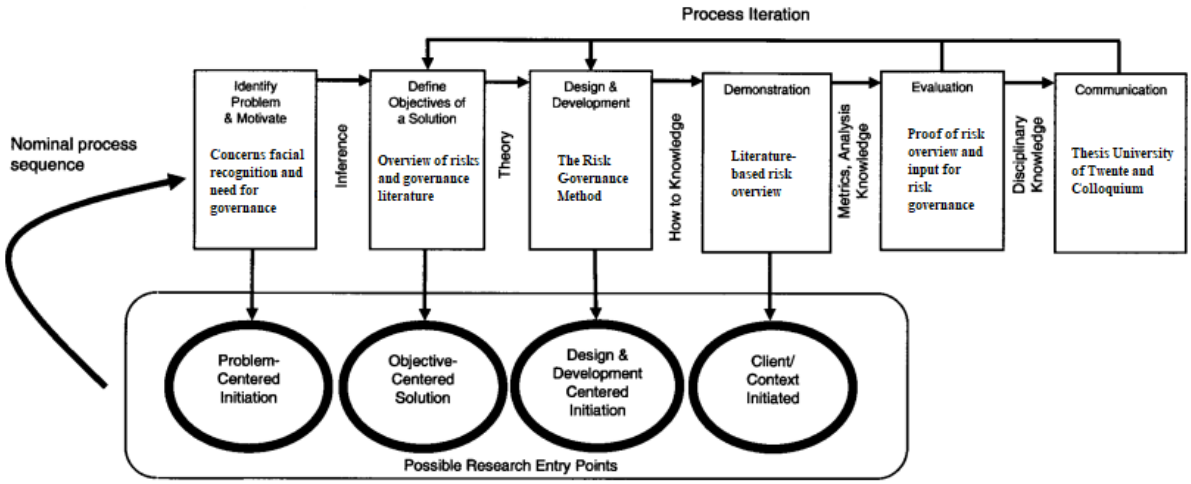


Figure 1. DSRM Process model design completed for this thesis (based on Peffers, et al., 2007)

2.2.1 Problem identification and motivation

The first activity ‘problem identification and motivation’ is represented in the first box of the upper chain in the DSRM Process model. Activity 1 is addressed in chapter 1 of this thesis. This activity contains a definition of the research problem which is reflected in a description of the situation with its concerns and the need for research. Then the value of the desired solution is represented by a description of the need in practice for support on the decision-making process towards using facial recognition.

2.2.2 The objectives for a solution

The second activity ‘define the objectives for a solution’ is represented in the second box of the upper chain. The activity contains a description of the added value the artifact would give and which problem it would solve (Peffers, et al., 2007). Activity 2 is addressed in chapter 1 of the thesis. The activity’s aim is accomplished by a description of the goal of this research, how this would contribute to practice and theory and which research questions are going to be answered.

2.2.3 Design and development

Activity 3 is ‘design and development’ in which the artifact will be created. The artifact in this research is the FRPS risk governance method with the goal to come up with a solution to the problem of decision-making. Research has been conducted into the risks of facial recognition in the area of public safety available in existing theory by doing a systematic literature review, represented in chapter 3.
Additionally, the risk governance literature adds value towards the development of the FRPS risk governance method. The deliverables of this activity support the answer on sub question 1 and 2 by delivering a risk overview and insights about aspects for risk governance from literature perspective. This activity is addressed in chapter 3 of the thesis.

2.2.4 Demonstration and Evaluation

The fourth activity is ‘demonstration and evaluation’. In this activity the artifact has been demonstrated to solve some aspects of the problem (Peffers, et al., 2007). This criteria has been fulfilled in this research by demonstrating the overview of risks to experts by conducting interviews. In the first part of the interviews, the experts have been asked to go through the literature perspective risk overview and highlight those risks they consider to be relevant or irrelevant. Thereafter, there has been given some space for the experts to add risks they are missing.

This demonstration results in an overview of risks adapted according to the information and feedback from the interviews with the experts. This overview is the answer and the deliverable from sub question 1.

In the second part of the experts interviews, the goal was to gather data around the knowledge and experience of the experts about risk governance and their view on risk governance within the scope of this research.

The results of the demonstration and evaluation activity are addressed in chapter 4 of the thesis.

2.2.5 Communication

This research is communicated by a thesis document publicized by the University of Twente. The research will be presented to and examined by a graduation committee.

2.2.6 The research entry point

The research methodology of the thesis has a focus on gathering data around facial recognition and public safety with a focus on municipalities. The data is collected from literature and different expert perspectives. The main goal is aligning and testing the literature-based results with the knowledge of experts. This alignment and testing form an iterative process to arrive at the development of a method as comprehensive and complete as possible. This shows that the research entry point for this thesis is ‘design and development centred initiation’.

2.3 The research sample and data collection

As can be seen in the research design, input is required from experts in the demonstration and evaluation activity. Below, the choice for both the research sample and the data collection method is explained.

2.3.1 The research sample

The unit of analysis for this research are municipalities since the main goal of this research is to design the artifact as a method for municipalities. Municipalities are one of the key stakeholders for ethical and lawful use of Artificial Intelligence for smart city development (Hanania & Thieullent, 2020). Moreover, Wirts, Weyerer and Sturm (2020) indicate that the need for governance and

regulation is increasing because of the public administration hardly keeping up with the quick developments around Artificial Intelligence. This reflects in a lack of governance and legislation around this topic in the specific area of municipalities which makes this an interesting unit of analysis.

Following, the units of observation chosen are experts. There is chosen to gather data from experts instead of municipalities because of the facial recognition technology being quite new. This rises the danger of municipalities not overseeing or not being totally aware about their own risks.
The experts in this research are experienced in the areas of risk management, privacy, security, and/or facial recognition in order to elaborate on the knowledge which is found in the literature.

2.3.2 The data collection method

Interviews has been chosen as the data collection method for this research. This decision is made based on three statements. First, for achieving the goal of this research, it is important to find out what experts know about the risks for municipalities of using facial recognition within public safety. Next, this research focuses on developing the risk governance method, which makes the variable 'risk governance method' underdeveloped considering literature. Thirdly, the gap found in this research is the absence of a comprehensive overview of risks. Due to that, the expectation arises of gathering unexpected information. The three statements mentioned are in line with the reasons for using interviews as the data collection method described by Van der Kolk (2020) [2].

The interviews were conducted in a semi-structured way. For the interviews it is important to gather as much knowledge as possible around the risks of facial recognition within public safety. For this reason, it is important to generate some place for additional sayings and guidance in the moment of the interview. Adding on that, the respondents should be able to emphasize certain aspects they deem to be the most important instead of the interviewer pushing the interview to topics which might be less important. On the other hand, it is important to have some structure within the interviews in order to supplement and correct the literature perspective.
A description of the interview and instruction for the respondent has been added. For this description and instruction, see Appendix I.

Due to the presence of the Coronavirus and the resulting advice of the Dutch government to work from home as much as possible (Ministry of Social Affairs and Employment, 2020), there has been decided to conduct the interviews via video calls. Subsequently, the video calls have been recorded and transcribed. For the interview transcripts, see Appendix II.

2.3.3 Data analysis

After transcribing all recorded interviews, the transcriptions have been coded. According to internal documents, the process of coding is most often unstructured when you are making an inventory of possibilities (Van Der Kolk, 2020)[3]. For this reason, the expert interviews have been coded unstructured and later on categorized. For an extended description of the coding and categorization process, see Appendix III.

[2] Source from University of Twente (not publicly available)
[3] Source from University of Twente (not publicly available)

3. Literature review

3.1 Systematic literature review

In order to find the risks described in literature there has been conducted a systematic literature research. This systematic literature research investigates the current state of knowledge around "public safety", "facial recognition" and "risk". For doing research on these three concepts, the five-stage grounded-theory for reviewing literature in a certain area from Wolfswinkel, Furtmueller & Wilderom (2013) is used. The five-stage grounded-theory consists of five phases which are the following: define, search, select, analyse and present. The structure of this systematic literature research is aligned with these five phases.

The creation of an overview from the current state of literature regarding public safety, facial recognition and the risks, supports answering the first sub question: "What risks can be identified for using facial recognition within the area of public safety?".

3.1.1 Define and Search

The databases approached for this research are Scopus and Web of Science. These databases are chosen because of its high amount of records. Scopus has over 75 million records and Web of Science has over 171 million (Elsevier B.V., 2019; Clarivate, 2020). Next, the different user groups of the platform are an interesting aspect (Elsevier B.V., 2019; Clarivate, 2020), which fit to the diverse perspectives of this thesis.

The starting point of this systematic literature research are the three key concepts, "public safety", "facial recognition" and "risk". To get a good and comprehensive overview of the literature different synonyms for "public safety", "facial recognition" and "risk" were added.

The resulting synonyms can be seen in table 1. The first column shows all synonyms for "public safety", the second all synonyms for "facial recognition" and the third for "risk".

Based on Table 1, made the following search term is made:

("public safety" OR "surveillance" OR "smart surveillance") AND ("facial recognition" OR "facial recognition") AND ("risk" OR "threat" OR "danger").
This search resulted in 60 articles within Scopus and 18 within Web of Science as can be seen in Figure 2. This search result is visualized in Figure 3.

Table 1
Synonyms

1 "public safety"	1 "facial recognition"	1 "risk"
2 "surveillance"	2 "face recognition"	2 "threat"
3 "smart surveillance"		3 "danger"

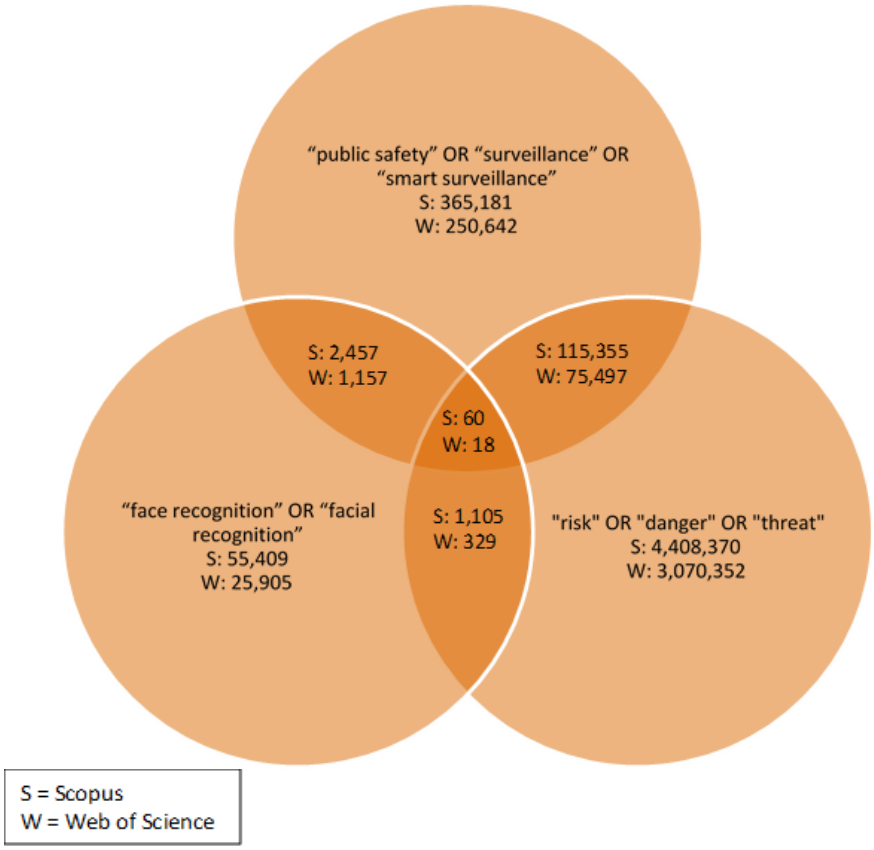


Figure 2. Visualization search result

The criteria for inclusion/exclusion

To further refine the sample, a number of inclusion/exclusion criteria were defined. The first criteria which has been taken into consideration is the language of an article. Articles within the sample written in English will be included in this research. Articles written in other language than English will be excluded.

The second criteria to focus on is the time period in which articles are published. For identifying this criteria the results from Table 1 are analysed. Based on these results, a graph is made which can be seen in Figure 3.

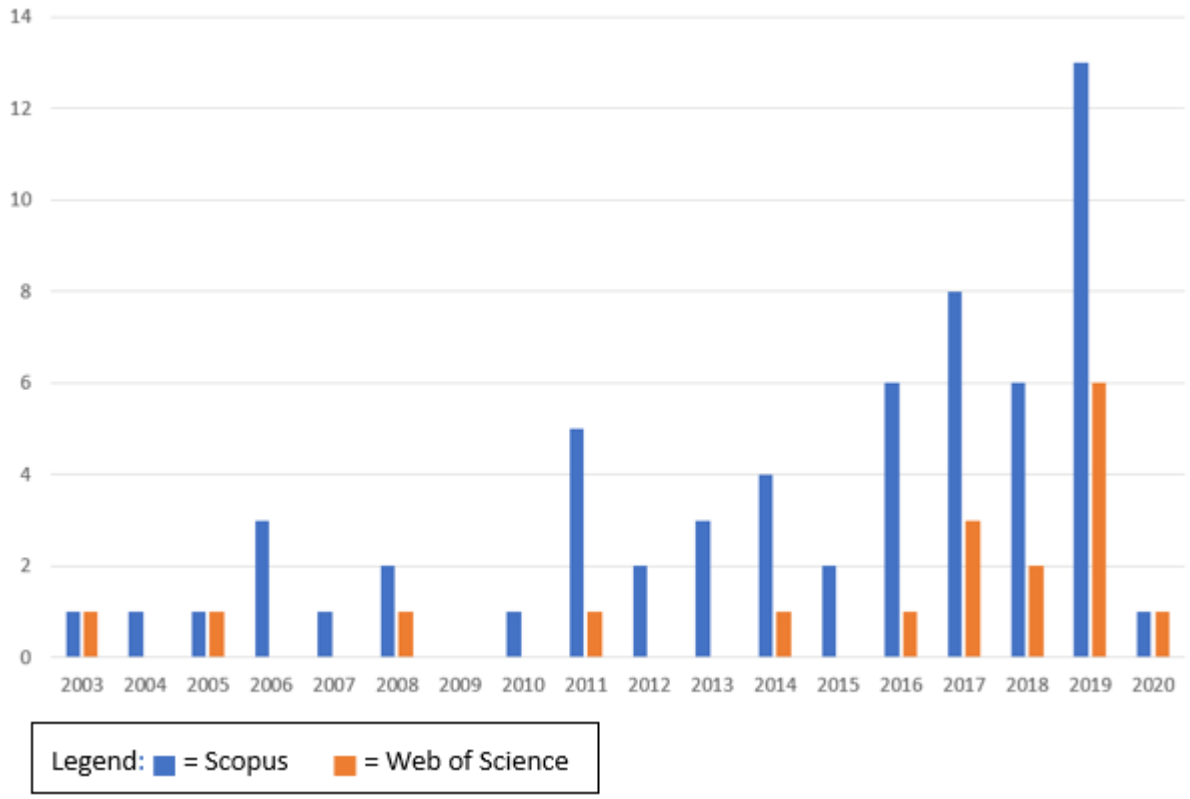


Figure 3. Publications per year Web of Science and Scopus from search term 1

Based on Figure 3, the peak of publications is the highest and roughly constantly rising between 2011 and now. For this reason, there is chosen to include literature written within this period of time. Next to that, the fast development of the technology might result in risks from before 2011 being outdated and irrelevant.
There is chosen to not add more inclusion or exclusion criteria. This choice is made for keeping the most comprehensive overview of risks with the plan for evaluating it later.

After taking the criteria (see Table 2) into consideration, Scopus shows 50 results and Web of Science 14 results. The refined sample which will be used for further research consists of the articles from Scopus and Web of Science together, 64 articles.

Table 2
Inclusion and exclusion criteria

Inclusion criteria	*Exclusion criteria*
Research from 2011 till now	Research older than 2011
Articles written in English	Other languages than English

3.1.2 Select and Analyse

Select
In this phase, the sample of 64 is further refined based on title and abstract, duplicates will be removed and no access articles will be deleted from the sample. The articles will be scanned on containing facial recognition and the risks of using it. After this first scan, the articles without facial

recognition, without a focus on facial recognition, a focus too technical on the software for using facial recognition and without describing any risks, will be deleted. After this refinement there are 21 articles left.

Analyse

In the following step, the sample of 21 articles has been analysed. All the articles are scanned in order to find out the risks of using facial recognition. The overview of these risks is shown in Table 3.

Table 3

Analysis of the sample

Risk / ***Author***	*Privacy*	*Security*	*Technical (+accuracy, speed)*	*Legal (+GDPR)*	*Data protection*	*Ethical (+discrimination, social, trust)*	*Resources (+Cost, storage)*
Hu (2017)						X	
Savastano (2017)	X		X	X	X	X	
Barnoviciu, Ghenescu, Carata, Ghenescu, Mihaescu & Chindea (2019)				X			
Han, Jeong & Won (2011)	X	X					
Kapatamoyo, Ramos-Gil & Dominiquez (2019)	X	X		X	X	X	
Sharif, Bhagavatula, Bauer & Reiter (2016)			X				
Spektor (2020)					X		
Awais, Iqbal, Ahmad, Alassafi, Alghamdi, Basheri & Waqas (2019)			X				
Medapati, Tejo Murthy & Sridhar (2019)			X				
Van der Haar (2019)			X				
Schaffer, Kincses & Pletl (2017)			X				X
Betta, Capriglione, Crenna, Rossi,			X				

Gasparetto, Zappa, Liguori & Paolillo (2011)							
Maeng, Chois, Park, Lee & Jain (2011)			X				
Gorodnichy & Granger (2015)			X				
Li, Liu, Lin & Wang (2017)			X				X
Karishma, Krishnan, Kiran, Dalin & Shivaji (2018)			X				
Jurevicius, Goranin, Janulevicius, Nugaras, Suzdalev & Lapusinskij (2019)			X				
Shareef (2016)			X				
Chun & Papanikolopoulos (2016)			X			X	
Kim & Park (2019)	X		X				
Praveen & Dakala (2020)	X		X			X	

3.2 Theoretical background

This thesis focuses on the risks of facial recognition and an approach to govern these risks. Additionally, there is added the scope of the research which is focused on public safety.

To give the reader an understanding of the topic facial recognition and public safety, these topics are defined in this sub chapter.

3.2.1 Artificial intelligence

Artificial Intelligence is a broad concepts which contains different technological applications. AI is a branch of computer science which focuses on theories, methods, and applications with the goal for simulation, extension, and expansion of the human intelligence for problem-solving (Niu, Tang, Zu, Zhou and Song, 2016). This broad concept contains the following branches: machine learning, robotics, natural language processing, planning and scheduling, expert systems, speech recognition and vision (Voda & Radu, 2019).

Facial recognition, the scope chosen for this thesis, is one of the applications within the broad concept AI. This application is an AI-based technique which is part of the ‘vision’ branch based on the categorisation of Voda and Radu (2019). For a visualization of the position from facial recognition within the concept of AI, see figure 4.

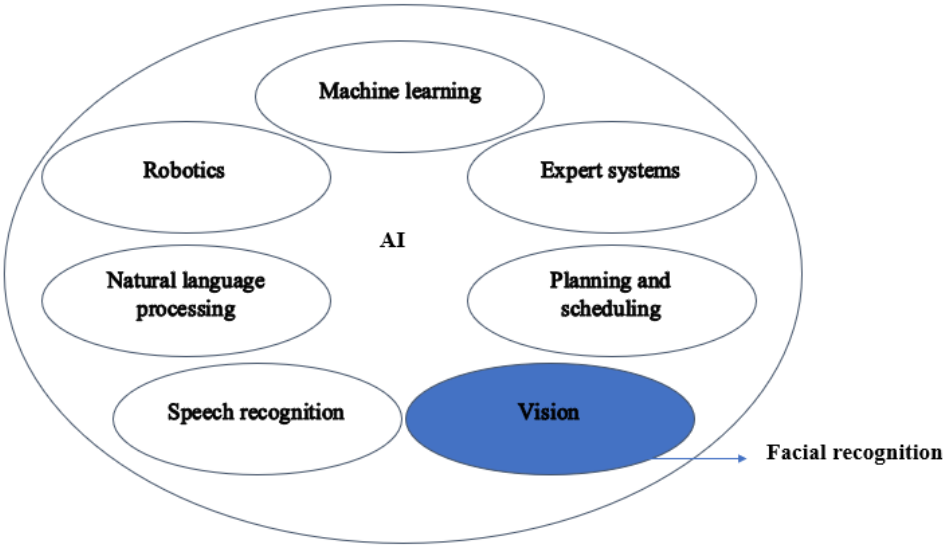


Figure 4. Position of facial recognition within Artificial Intelligence

3.2.2 Facial recognition

Facial recognition is a biometric technique that is able to identify, match, verify or categorize a person's face based on automatically processing digital images (Article 29 Data Protection Working Party, 2012). Facial recognition makes it possible to recognize people in a non-invasive and low cost manner. This makes the demand for facial recognition growing rapidly (Praveen & Dakala, 2020). Joshi (2019) describes facial recognition as a process with the following steps: 'captures images or videos', 'reads the geometric measurements of the face', 'calculates a mathematical formula for the captured face' and 'compares it with the image in the database'.

3.2.3 Public safety

As described in the introduction, the scope of this research is facial recognition in the area of public safety. The definition of public safety for this thesis is composed by comparing the applications mentioned in the introduction with the applications mentioned in the categories from Parveen & Dakala (2020) and World Economic Forum (2020).

The application of 'easy boarding and security checks at airports' is described as well in the introduction as 'passenger check-in, unlocking doors/opening entrances and passport control'. Also 'customs and border protection: identity control' could be part of this application since airports also have to deal with customs and border protection.

Next, there is the use of facial recognition by jaywalking in China. These jaywalkers can be identified by using CCTV cameras with facial recognition (Van Boom, 2018). The application 'safety in public space' from World Economic Forum (2020), which contains automated CCTV, is therefore a similarity to the 'jaywalking' application from Praveen & Dakala (2020). Additionally, the public safety of railway stations and movement tracking, mentioned in the application 'safety in public space', is reflected in the introduction.

The third application 'to book traffic violations by rental transport users' (Praveen & Dakala, 2020) serves the same function as 'private security: tracking shoplifters and burglary prevention' (World Economic Forum, 2020) and the tracking of rule breakers around the situation of the Coronavirus. A follow-up to this would be the 'to build a unified penalty system' described by Praveen & Dakala (2020).

Another application is the 'identifying victims of human trafficking' (Praveen & Dakala, 2020) and corresponds to the application 'person of interest tracking' and 'searching for missing persons' from

World Economic Forum (2020). Additionally, the same way of using facial recognition is seen in the application of ‘criminal identification in the context of environment’ (Praveen & Dakala, 2020).

Following, there are some differences and applications not mentioned before. At first, the ‘identification of men in female-reserved coaches (or) women-only areas like hostels’, mentioned by Praveen and Dakala (2020), is described. Then there is ‘neighbourhood watch: private front-door cameras or external cameras on vehicles used for facial recognition’ described by World Economic Forum (2020). Subsequently, there are the application fields: ‘safety at public events, such as demonstrations and carnivals’, ‘police patrol: body cameras’ and ‘people attendance’. These applications are not mentioned before but might be a possible application field for municipalities because of the public aspect.

After all, the scope of this research is facial recognition within public safety. As described the categories from Prava & Dakala (2020) and World Economic Forum (2020) have a lot in common in the area of public safety. Thus, as mentioned in the introduction, for this research public safety is defined as a mixture of the definition ‘security, access control and law enforcement’ from Praveen & Dakala (2020) and ‘safety and security of public spaces’ from World Economic Forum (2020). Public safety is defined as: the application field of safety, security and access control within public areas and events.

3.3 Risk governance in public administration

This sub chapter focuses on the concept risk and risk governance. This subchapter follows a funnel structure by starting with the concept risk in general, followed by risk governance and risk governance for Artificial Intelligence with and ending of current literature on risk governance in the area of facial recognition. There is chosen for this funnel structure to describe the development of the topic risk governance around facial recognition. Additionally, this structure is chosen because literature about risk governance around facial recognition is underdeveloped.

3.3.1 Definition of a risk

To be able to design a risk governance method, it is important to define the concept ‘risk’. Risk is almost always the main barrier to solve real-life problems such as, among others, the ones related to security and technology (Aven, 2018). The topic of this thesis is in relation to risks, security and technology because facial recognition is a technology with, among others, risks in the area of security. This relation marks the importance of defining a risk even more.

A risk can be defined in a lot of different ways and contexts. A very general term for risk refers to the probability of harm in areas like health, environmental, economic, or others (Van Asselt & Renn, 2011). Following on that, the IRGC framework paper from Renn and Graham (2006) refers to risk as possible intended and unintended consequences which might occur, that violate aspects of what humans value.

Aven (2016, p. 4) sums up some qualitative definitions of risk: (a) the possibility of an unfortunate occurrence, (b) the potential for realisation of unwanted, negative consequences of an event, (c) exposure to a proposition (e.g. the occurrence of a loss) of which one is uncertain, (d) the consequences of the activity and associated uncertainties, (e) uncertainty about and severity of the consequences of an activity with respect to something that humans value, (f) the occurrences of some specified consequences of the activity and associated uncertainties, (g) the deviation from a reference value and associated uncertainties.

The risks in relation to the goal of this research can be very broad due to the amount of different stakeholders, the fast developing technologies and the complex processes within the decision-making process of governments. For this reason, the definition for this research will be defined in a general way with a focus on the municipality, which is the unit of analysis.
For this thesis a risk will be defined as ‘an aspect with a negative consequence for the municipality

(directly) or society (indirectly for municipalities) as a consequence of the decision for using facial recognition'.

3.3.2 Definition risk governance

The goal of this research is to create a risk governance method to support the municipal decision making process. The decision-making process around the usage of facial recognition within the public safety area and its additional risks is of importance for a variety of stakeholders, as can be seen from the different discussions described in the introduction. This is in line with the following description from Jalonen (2007) about the local government decision-making: "a complex process, which includes numerous interactions and interdependencies between the officeholders and the politicians, and between the decision-making system and its stakeholders" (p. 20). To describe this complex process of local government decision-making, the term 'governance' is used in political science (Van Asselt & Renn, 2011). It describes the multitude of actors and processes that lead to collective binding decisions (Van Asselt & Renn, 2011). The IRGC (2019) describes 'governance' as "the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented.

The term 'risk governance' is introduced to literature via European networks and is rooted in the interface between "risk assessment, risk management, regulatory sciences, and policy analysis" (Van Asselt & Renn, 2011, p. 433). In 2003 the International Risk Governance Council (IRGC) was founded with the goal to deal with global risks in different areas and support governments, industry, NGOs and other organisations to deal with these risks (Renn & Graham, 2006). The IRGC mentioned the term 'risk governance' which "applies the principles of good governance to the identification, assessment, management and communication of risks (IRGC, 2019). The term 'risk governance' contains the translation of the content and fundamentals of governance in the context of risk-related decision-making (Van Asselt & Renn, 2011). The situation of the potential usage of facial recognition with the additional concerns, discussions and different stakeholders around this situation results in a risk-related situation for decision-making. Risk governance has the ambition for providing conceptual and normative basis for dealing with uncertainties and risks (Van Asselt & Renn, 2011). This is in line with the research goal of this thesis, which is to develop a concept, the risk governance method, in order to support the decision making around facial recognition.
Risk governance is defined by Van Asselt and Renn (2011) in two ways: "1) as the critical study of complex, interacting networks in which choices and decisions are made around risks and 2) as a set of normative principles which can inform all relevant actors of society how to deal responsibly with risks" (p. 443).

The IRCG (2019) developed a comprehensive framework for risk governance to provide guidance in the process of early identifying and handling risks which could potentially damage "human health and safety, the economy, the environment, and/or the fabric of society at large" (Renn & Graham, 2006, p. 11). The framework, displayed in Figure 5, consists of four interlinked elements and three cross-cutting aspects (IRCG, 2019).

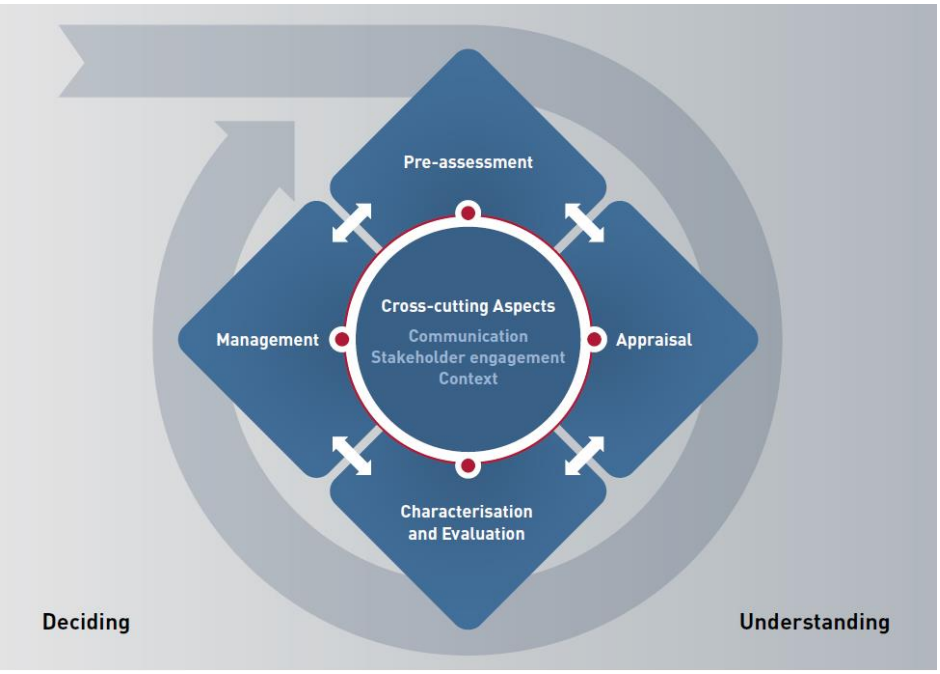


Figure 5. The IRGC Risk Governance Framework (IRGC, 2019)

The first element, pre-assessment, has the aim of capturing the variety of issues that the stakeholders involved associate with as a risk (Renn & Graham, 2006) and potential strategies for addressing these risks (IRGC, 2019).
Then the appraisal consists of developing and synthesizing the knowledge as a basis for deciding on which risk should be taken into account. Following, there will be identified and selected options to prevent, mitigate, adapt to or share the risk (IRGC, 2019). This element contains risk assessment and concern assessment (Renn & Graham, 2006; IRGC, 2017).
The bottom element is the characterisation and evaluation. The aim of this phase is to make a judgement about the risk and the need to manage the risk (IRGC, 2019). The element contains comparing the outcomes of the risk appraisal element with specific criteria, determining the significance and acceptability of the risks and preparation for decisions (IRGC, 2019).
The last element is management in which contains the decision and the implementation of the risk management options (IRGC, 2019). Actions and remedies required to reduce, transfer, avoid or retain the risks are designed and implemented (Renn & Graham, 2006; IRGC, 2019). In this management phase criteria, such as effectiveness, efficiency, minimisation of external side effects, sustainability, etc. are assessed and judged by the assessment criteria (Renn & Graham, 2006).

A crucial point, indicated by Renn and Graham (2006), for the successful outcome of the risk process, and overall risk governance, is the transparency of the implications and challenges throughout all elements. In addition, the three cross-cutting aspects are important throughout the whole process (IRGC, 2019). The IRGC (2019) describes the aspects as ‘communication’ with the crucial role of being open, transparent and inclusive, ‘stakeholder engagement’ with the importance for assessing and managing risks, and ‘context’ with the “need to deal with the risk in a way that fully accounts for the societal context of both the risk and the decision that will be taken”. Also Renn and Graham (2006) point out this ‘communication’ as a major importance throughout the whole process since it creates understanding, help to make informed choices about risk, fosters tolerance, creates trusts, and can have an “impact on how well society is prepared to cope with risk and react to crises and disasters” (p. 15).

Van Asselt and Renn (2011) mention some principles for the governance of systemic risks: “the communication and inclusion principle, the integration principle, and the reflection principle” (p.

431). The first principle, the communication and inclusion principle, refers to exchanges between different stakeholders, such as experts, policy-makers, the organization itself, stakeholders and the general public (Van Asselt & Renn, 2011). The achievement of facilitation of purposeful interaction between actors with a variety of backgrounds in case of uncertainty, complexity, and/or ambiguity is a key challenge mentioned by Van Asselt and Renn (2011). The inclusion part of this principle refers to the multi-actor process, facilitating it and inclusion of actors as a key role in framing the risk, "supposed to support the co-production of risk knowledge, the coordination of risk evaluation, and the design of risk management" (Van Asselt & Renn, 2011, p. 441). Within this principle, consensus-building is an important aspect together with the critical evaluation of it for learning how communication and inclusion can be adequately organized in different cases (Van Asselt & Renn, 2011). Next, the integration principle, assigned by Van Asselt and Renn (2011) contains "the need to collect and synthesize all relevant knowledge and experience from various disciplines and various sources including uncertainty information and articulations of risk perceptions and values" (p. 441-442). Lastly, all actors involved should reflect on what they are doing, according to the reflection principle (Van Asselt & Renn, 2011). This principle emphasizes the importance of repeated consideration during the process from all stakeholders in case of significant and difficult cases. There is pointed out that this set of principles should be read as a synthesis which needs to be seriously taken into account when organizing structures and processes to govern risks (Van Asselt & Renn, 2011).

These views on risk governance are general perspectives. For this research it is interesting to dive deeper into the risk governance literature with a focus on Artificial Intelligence and specifically facial recognition.

3.3.3 Risk governance for Artificial Intelligence

The current literature about risk governance within Artificial Intelligence consists of important insights for this research because of the fact that facial recognition is an Artificial Intelligence based software (Rouse, 2020). An Artificial Intelligence Governance framework has been proposed in the context of public administration, by Wirtz, Weyerer and Sturm (2020). There is specifically pointed out an example of facial recognition within public safety in which "careful consideration of such interventions is needed to apply regulatory methods that protect society from respective violations" (Wirtz, et al., 2020, p. 9). Which points out the need for the research of this thesis but also results in the Artificial Intelligence Governance framework being interesting for this research.
The integrated AI governance framework is displayed in Appendix IV. It is developed based on a combination of insights from governance literature and Artificial Intelligence challenges (Witz, et al., 2020). The framework is developed based on a structure of five layers. "(1) As AI technology, services and applications are able to cause market failures, they represent the objective of regulation (AI technology, services and applications layer). (2) Market failure manifests itself through an external effect of the AI technology and the associated challenges posed to society (AI challenges layer). (3) To counter possible negative effects, a regulatory process is needed to assess costs and benefits as well as to evaluate the outcomes with and without regulation (AI regulation process layer). (4) At the end of the process, policies, laws and other means of regulation are implemented to prevent or adjust the aspects leading to market failure (AI policy layer). (5) Given the great impact of regulation on society and its potentially negative effects, the affected stakeholders and representatives of public and private interest groups should support the entire regulatory process (Collaborative AI governance layer)" (Wirtz, et al., 2020, p. 6). The parts of this framework, closest related to the subject of this thesis, are the AI challenges layer and the AI regulation process layer since these layers touch upon the risks of certain applications.

This risk governance framework covers a large number of facets. On the one hand, this is all-encompassing, even though Butcher and Beridze (2019) argue that instead of implementing a large comprehensive framework, there might be a need for creating a narrowly focused regulatory framework. There needs to be a focus on AI governance for specific application areas before a

broader global and comprehensive framework would appear (Butcher & Beridze, 2019). This might be the case for a specific application like facial recognition.

A consensus-driven approach and collaboration, within the risk governance process, are subjects that recur frequently in literature (Butcher & Beridze, 2019; Wirtz, et al., 2020; European Union Agency for Fundamental Rights, 2020). There seems to be a high amount of agreement within literature about these subjects. Butcher and Beridze (2019) conclude that the required effective governance contains different stakeholders having critical roles on different levels of governance. Therefore, a combination of consensus-driven standards and technical tools is needed. This conclusion is supported by the statement of the European Union Agency for Fundamental Rights (2020) "working with new AI-driven technologies, which are not yet fully understood and where not much experience has yet been gathered, requires the involvement of all relevant stakeholders and experts from different disciplines" (p. 33), which also seems to indicate a consensus-driven approach.
Following, this consensus-driven approach has also been addressed in the AI Governance framework from Wirtz, et al. (2020) in which collaboration between stakeholders is an important aspect through the whole AI Governance framework. The consensus-driven approach is important for creating belief, trust and commitment about the idea in order to boost acceptance and positive effects in society (Wirtz, et al., 2020).

3.3.4 Risk governance for facial recognition

This last paragraph, the end of the funnel structure, is about risk governance in the perspective of facial recognition. This research area is quite underdeveloped considering the need for governance on facial recognition, described in the introduction, and the amount of literature available on this topic.

According to Varley-Winter (2020), there are three overlooked governance issues.
First, the sensitivity of the data which is used by biometric systems or the interpretation of biological data. The level of sensitivity is based on whether the data is identifying. "The scope for the unwanted retention of facial biometrics gives the rise to concern about the identification of individuals and their data being monitored in perpetuity" (Varley-Winter, 2020, p. 6). There are concerns about disproportional usage in commercial settings, as well as in political settings due to the potential connection of data to home or business surveillance. However, non-identifying data seems also be a concern in being a valid systems because it affects the behaviour of the people being monitored and therefore, affects the validity of the facial recognition methods.
Secondly, there is the level of trust in biometric technologies of which the importance is often misunderstood. Varley-Winter (2020) state that ethical regulators and practitioners from industry should reflect on inspiring trust and ensuring trustworthy governance processes.
The third issue mentioned is the contest over regulation until there is a shared system. "When regulators act on a broad suite of both biometrics and artificial intelligence capabilities, it is going to be a complex task to ensure that all types and sizes of firm can participate in socially responsible practices, successfully and competitively" (Varley-Winter, 2020, p. 7).

The research from Madzou and Louradour (2020) is focused on a governance framework for facial recognition, which is comparable to the aim of this thesis. The main thought behind this framework is that facial recognition is intrinsically risky by sense that biometric data is sensitive and particularly in case of safety and security purposes. This results in the need for a governance framework for facial recognition even more. This process, described by Madzou and Louradour (2020), of developing the framework involves a multi-stakeholder approach for ensuring trustworthy and safe usage of facial recognition. The stakeholders involved in this process are industry actors, policy makers, civil society representatives and academics.

The governance framework from Madzou and Louradour (2020) consists of four key steps as displayed in figure 6. The first one is 'define' in which a set of principles for responsible usage of facial recognition are defined containing risks like "privacy, bias mitigation, the proportional use of the technology, accountability, consent, right to accessibility, children's rights and alternative

options" (Madzou & Louradour, 2020, p. 6). Then the 'design' step contains a set best-practices to support a responsible design. Following, 'assess' is the assessment of the responsible design complied with the principles for action from the define step. The last step is 'validate' in which the goal is to get a certification, for proving the ability to deploy a system following the principles for responsible usage, provided after an audit from a trusted third party.

Figure 6. Four-step solution (Madzou & Louradour, 2020)

The risk governance literature is coded and analysed in order to create an overview of relevant output for the FRPS risk governance method. The output of this process is shown in Appendix V.

4. Results

This chapter is structured based on the reoccurring topics among the different interviews. Every reoccurring topic has an own sub chapter in which all results about this topic are described based on four interviews with different experts. Within the results there is referred with codes corresponding to the different respondents from the interviews. Table 4 displays an overview of the respondents and the corresponding codes.

The respondents are expert on different fields in relation to facial recognition. Different fields have been chosen to create a diverse overview of information about the risks and the decision-making towards facial recognition within the area of public safety. The first two respondents are experienced on the area of privacy and security. Privacy and security are related to facial recognition because of the risk around these areas mentioned in literature (Han, Jeong & Won, 2011; Savastano, 2017; Kapatamoyo, Ramos-Gil & Dominquez, 2019; Kim & Park, 2019; Praveen & Dakala, 2020). Besides, the respondents have experience with risk assurance through working with municipalities as an employee from PwC. Risk assurance and municipalities are both part of the research of this thesis and therefore these respondents are a good addition. The third respondent has experience in working as a AI researcher within a municipality. As stated by Rouse (2020), facial recognition is an AI based application, which makes the knowledge in AI a added value for this research. Also, the experience within a municipality is an added value because of municipalities being the unit of analysis for this research. Then the last respondent has experience in development of facial recognition and the supply of this application. This experience has an added value by adding the perspective from delivering and developing facial recognition for the municipality since that is one of their customers.

Table 4

Respondents and codes

Code	Expert category
R1	Privacy and Security
R2	Privacy and Security
R3	Municipality and AI research
R4	Facial recognition research and supplier

4.1 Current application of facial recognition

Based on the interviews, there are identified some applications of facial recognition which are taken in usage. R4 describes the one-to-one comparison for identity check, in which the software compares "the database photo and the visitor (…) so they can double check if the person who is getting the passport or getting the driver's license is actually the authorized person".

Within Dutch municipality X, there is decided to not use facial recognition. The only way it would be used, is for doing research. There has been executed an experiment with "partners, at the arena, with the stewards who work there" in which they could enter more quickly by using facial recognition (R3). The goal of this experimenting is "to be able to understand the technology and be able to continue to pass judgement on it" (R3). R3 describes that these abilities are needed in order to be in possession of the technical expertise and experience in order to make a correct decision.
Apart from facial recognition, the municipality uses "face detection" with the goal to "remove faces". R3 mentions that this is done to "prevent the data we store being used for other purposes in the future". This usage of face detection results in a positive response of citizens.

4.2 Privacy

When talking about facial recognition, privacy seems to be a very important topic and reoccurring in all three expert categories. R4, the facial recognition expert and supplier, points out that "the main

reason governments and big companies, are really not into this technology at the moment is due to privacy". When privacy is not properly considered, then "there is a big risk that many companies" using facial recognition improperly, "would be banned" (R4). R2 mentions privacy as "the main driver or risk perceived by society". This might have to do something with the society of the Netherlands being proud of their "freedom of belief" and "freedom of expression" and for this reason privacy issues are at times complicated in the Netherlands (R2). R3 mentions his concerns around facial recognition and privacy by its experience with a Chinese Professor. In China they do not see privacy as their "top priority" and "this is the setting where the research is being done" (R3). The privacy not being a top priority is probably also the reason why it is applied in China, "the R&D teams there make other considerations" and do not have the juridical costs due to privacy in comparison to the Netherlands (R3).
To conclude on the topic privacy, it is seen as a risk from different perspectives, not properly considered, the consideration by society, and the research point of consideration.

From the supplier perspective there is given a way for mitigating the risk of privacy. As a supplier, they try to solve this privacy risk by working "privacy proof by metrics" so they "make sure that every project or every application" they execute, "is privacy proof" and "say no" to projects with "a lot of privacy concerns" (R4). A way of working privacy proof, is by permission of the consumers. This aspect will be further discussed in a separate paragraph because of its reoccurrence among the different expert categories.

4.3 Data protection

From the perspective of R1, R2 and R4, data protection is a very relevant aspects. Along with the usage of facial recognition comes the registration of data. If this data "is not safely stored, then" there could be potential risks like stolen data or mis usage (R2). R1 adds that "municipalities are vulnerable because they do not always have mature security". As a result, "the data collection" could be "stolen" or the "data collection is used for purposes for which it was not originally collected" (R1). There could be a "malicious person" interested in the data "in order to recognize (…) patterns" and following "break into my house or want to know something" of a certain person (R2). "This can have significant consequences for the person in questions which cannot be undone" (R1). The data protection is a topic which is "underexposed in the public debate on facial recognition" (R2).

R4 describes the way of protecting the data. The supplier of facial recognition has "a cloud based facial recognition solution" (R4). They mitigate the risk of access by any unauthorized party by building "different kind of encryption methods in" their platform like homomorphic encryption for example (R4). By doing this, they do not need to store the photos, only the facial rector. "So that provides kind of security because even if someone breaches a platform, still they cannot access original identities" (R4). The supplier states that by using this encryption method, the data "is only visible by us or by the clients". In this way they try to manage the risk when storing data at a third party cloud environment. Also, the facial recognition application "should be protected from hackers".

The Dutch municipality X follows the shared values for a responsible city, described in the "Tada Manifest", when working with data (R3). This manifest consists of the following shared values for a responsible city: 1) including, 2) participation, 3) human size, 4) legitimate and controlled, 5) open and transparent, 6) from everyone – for everyone (Tada, 2020). The manifest with explanation of the shared values is displayed in Appendix VI.

4.4 Accuracy

An important aspect for facial recognition software seems to be the accuracy, since it is a reoccurring topic in all interviews. From the municipal perspective the accuracy constitutes a risk. It is an issue when the software matches the image to "the wrong persons" "explicitly because municipalities see

potential in implementation around the topic safety" (R2). Also R1 points out the accuracy as an important aspect. When using data from bad quality "security cameras" there is "a much greater margin of error". This results in "the muncipality not reaching its objective" and an higher chance of "mistakes that will have adverse effects on the citizen". The supplier of the facial recognition software adds to this point that the software has "a chance that one of" the million comparisons "will be inaccurate" (R4). The accuracy "is becoming very high" and " there can be multiple checks as well, so instead of one photo, the camera can capture three", or more, which will make the situation "a bit more reliable" (R4).
R2 mentions another functional aspect from the software, "speed". There could be made some "functional requirements" on this aspect for the "supplier" of the facial recognition software, in order to be "able to act fast enough" as the party working with the application (R2).

The facial recognition expert and supplier gets more in depth about the different risks around accuracy. Challenges around accuracy are "lighting conditions, exposure" such as the "distance from the camera, different angle of the face" or "partly excluded faces", "quality of the camera", "light is projected from behind" and "people wearing sunglasses" (R4). Next, there can sometimes be "motion blur when we want to detect and track people when they are walking and they walk very fast", "but that can alse be removed" (R4).

R4 reflects on the risk of discrimination from the literature perspective as this risk being the consequence of the accuracy of some facial recognition algorithm. The "design of the algorithm should be more careful", with balanced "training data into the algorithm", in order to achieve a good accuracy and mitigate the risk of discrimination (R4).
Another risk reflected upon is the spoofing attacks mentioned in literature. Examples of this kind of attack are "playing a video of an authorized person in front of the camera" and "showing a picture to the camera" (R4). "Those attacks can be detected easily". Therefore, this spoofing attack might not create a "risk factor for the municipality" (R4).
Other examples of these spoofing attacks, mentioned by R4, are "building a personalized customized mask of an authorized person, that is a different kind of attack and there you need 3D camera to really find out". In case of the usage at muncipalities for one-to-one comparison it is "not really a risk factor". Also, "it is possible that the system is deceived because of the plastic surgery" (R4). As long as the software is not 100% accurate, it is not possible to "attribute an offence to somebody" (R2). This could lead to a risk from jurisprudential perspective, further discussed in chapter 4.5 Legal.

A risk for the accuracy of the facial recognition application could be "the chilling effect" (R1). This is the effect on someone's behaviour when the person knows that he or she is "being monitored" (R1). R1 points out that this fact might be seen as "a restriction on your freedom to behave as you wish".

4.5 Legal

"When using facial recognition, you are working with personal data" (R3). The expert municipal image recognition points out that the use of personal data "is within the privacy regulations" and creates a risk of doing something illegal as a governmental organization.

In order to identify the risks around the implementation of the facial recognition software, the supplier has a "project manager who is specialized in GDPR" (R4). "Everything should be according to the GDPR and plus some more privacy concerns from end user" (R4). From the supplier perspective, R4 mentions that "considering GDPR guidelines it is very important" that every company has at least one person "really expert in GDPR and data regulations", like a "data protection officer or privacy officer". Software developers or researchers "are only building software" and do mostly not have a high knowledge of these regulations (R4).

For a municipality it is "mandatory to execute an analysis on privacy risks" (R1) whenever processing is likely to result in a high risk to the rights and freedoms of individuals (European Commission,

2020). An instrument which is already being used, is the risk assessment for privacy impact called "DPIA". "The DPIA is an important instrument to start "measure whether the new development complies with the "legal framework of the GDPR (AVG)" (R2). R2 points out that "the law is decisive for the municipality and they must comply with the GDPR" also R1 mentions that the DPIA is an obligation. This DPIA ensures "that you take a very broad view of the consequences for citizen" (R1). A risk is the level of qualification of "the person who executes the analysis" (R1). Additionally, "a municipality has to comply with the baseline information security government (BIO)". Municipalities base their information security policy and their justification towards the municipal council and the regulators from the kingdom on this BIO which is focused on risk management (VNG, 2020). The baseline describes "the rules of the game, which we have agreed on with each other around information security" (R2).

The expert privacy and security, R2, points out that "you may expect that" the ethical, privacy and law aspects will be considered correctly. "On the other hand, you see that legislation is not always clear about what is permitted and what is not" (R2). Additionally, R1 mentions that "the fact that something is juridically allowed, by privacy legislation, does not necessarily mean it is a wise idea". This unclarity is also mentioned by T. Ali as "GDPR is a good step" in making clearer how data should be handled, "but now there should be more guidelines".

There is a risk around video footage on a jurisprudence perspective. "Can someone object against" the fact that it is him or her at the footage and what if someone can demonstrate that he or she was not there at that moment (R2). This case raises the question for R2 "what rights may the municipality or I, as a citizen, derive from this footage on which someone is recognized". As long as the software is not 100% accurate, it is not possible to "attribute an offence to somebody" (R2).

4.6 Reluctance

"There is quite a lot of reluctance around" (R2) the topic facial recognition among municipalities and many people "are still afraid of using facial recognition (R4). R2 points out he is scared that "the more conscious people would become of the technical possibilities, the more reticent the response will be". The usage of facial recognition rises question like "how is it for me as citizen in my municipality, how do I know what the municipality does with the information that is collected and how is my privacy guaranteed, but also how do we avoid me being falsely accused" (R2). "Surely, here in the Netherlands, we are quite fond of our freedom and also of our privacy" (R2). The understanding why such applications would be needed is complicated and "the fact that there is a great deal of uncertainty about facial recognition" which creates reluctance (R2).
All the current news reporting (e.g. BBC, 2020; BBC, 2020; Ovide, 2020) about "ethical aspects" make the situation more complex (R2). It becomes a "balancing act for municipalities" between possibilities and reluctance. "Politically no one dares to say something" about the topic and most of the time the application of facial recognition is called "a pilot" (R2) or "facial comparison" (R1). Furthermore, R2 points out that it is an unclear point about "who is going to be decisive when there are no clear guidelines from the national government". In this case, the Netherlands, "municipalities have a lot of autonomy as long as they follow the guidelines of the law" (R2). On the other hand, according to R3, it seems hard to find a politician who "wants to give a clear opinion or wants to speak out".

As an addition to this reluctance, R1 mentions that "there is a lot of resistance to facial recognition in the Netherlands on the basis of principle". "If there is a meaningful application, then as a municipality, you have to communicate this very well in terms of stakeholders' expectations, otherwise it" evolves in a discussion in "terms of public opinion and politics" (R1).

4.7 Transparency & trust

R1 mentions that besides the areas of law, regulations and privacy, “management of society’s expectations” is really important. As municipality “you can come up with something juridically valid”, but if “society feels surprised” by the implementation and “did not realise sufficiently what the consequences would be or the municipality did not communicate sufficiently” about their intentions, then this results in a lot of reactions (R1).
Also, R2 points out the communication towards the “citizens”. There is “a question of trust attached to” the usage of facial recognition from the organizational perspective, for example “as a local authority” (R2). The organization should figure out how to “demonstrate to” its “citizens”, “society or to the supervisor that” they do not store the data “or only store them for a specific purpose” and that they remove the data after a certain time (R2).

As a solution for this trust question, R2 mentions a “certificate”. The doubtfull side of a certificate is the saving of data and its level of “transparency” and whether it can be “measurable”. R3 would deal with trust and transparency by “being transparent about image recognition, where does it happen, organize meetings about it, and see the reactions of” the citizen before implementing it. Also the supplier of facial recognition takes part in the creation of transparency. Their project manager “looks at all the data flows in the system of the client and he also looks at our data flow and our cloud based environment. And he tries to manage that everything is very transparent to the end user and only the person who is authorized can get access to the data” (R4).

Another aspect about trust and transparency, which is addressed by R4, is in case when “the solution is not provided by one party”. Then it is important to work together for addressing “where the data is stored”, “who is the owner of the data and what kind of opeations can be performed by” the different parties, “all these things should be properly addressed” (R4).

4.8 Permission

In the current situation “it is almost impossible to avoid sharing more and more information”. This raises the question for R2 “how can I now partly determine myself what happens to my data, but also what remains registered and what not, and for what purpose?”. One way of doing this is mentioned by R3, the supplier offers a platform in which people give permission for using their data. “Only if a person enrols himself or herself by a phone, then we recognize them” (R4). In this way the supplier of the facial recognition software can ensure privacy of the consumers in which “the end user is given complete consent on” the “data and on the photo” and “nobody else can enrol someone else” (R4). T. Ali points out the permission aspect several times during the interview and specifically mentions that “nobody should be recognized without their consent”. This permission aspect is also in line with the case of the application of facial recognition at location X, where there was permission of the employees to be scanned, as mentioned by R3.

4.9 Applicability

Monitoring by using facial recognition seems to be something hardly applicable when considered by R2. The reason for this is that in that situation it is unclear “what is being done with the data and there is no clear goal for using it” and “if there is a certain generic goal in which the citizen does not directly see the benefits”, it might not be possible to apply the facial recognition (R2). This is in line with what R3 points out based on his experience with other projects, when placing camera’s in a city “you need to have purpose limitation”. Facial recognition might be more applicable when “there is a very good reason for using” it, “what would make it possible to better justify” the decision (R2).
The only application of facial recognition used at the moment, is one-to-one comparison, as described in chapter 4.1 Usage of facial recognition. R1 thinks this is application is better applicable because the “goal is more clear”. Additionally, there is way less specific and concrete information in the application for one-to-one comparison instead of other application forms, like applying “in public

environments" (R1). An important aspect for applicability of the facial recognition software is the scope. The case of implementing the software in "a very limited physical environment", which will be secured with "very specific emphasis on every person who walks in", creates "a better story for that limited environment" than applying the software into a broader environment (R1).

From the municipal perspective, R3 points out that they only want to apply technologies when they are "scalable and not too expensive". It needs to be an application with which they can really "make a difference in the city" (R3). "One of the strict criteria's" that R3 mentions is that they do not use personal data because the added value does not outweigh the costs. "These juridical costs would probably be more expensive than our own development costs" (R3).

4.10 Decision making

In case of the Dutch municipality X, the decisions around the topic of facial recognition "are being made by the municipal council", the "CTO" and "CIO" (R3). The facial recognition supplier, R4, mentions that the decision making process is a group of people containing "the CTO and the project manager, they are the key people who working closely with the municipality".

The decision making process on using facial recognition can lead to "in-depth juridical and moral discussions" (R1). Therefore, it is important to "reflect objectively" on the application and verify if there is "applied goal reasoning" (R1). R2 agrees on this by pointing out an important step to "get a very clear what purpose they would like to use this software for". This purpose determines "what risks are involved".

4.11 Risk identification

For identifying the risks, it is important to "start reasoning from the objectives" of using facial recognition from the perspective of "the various stakeholders that are involved, including the data subjects" (R1). The different stakeholders might have different objectives for using facial recognition or in the situation of facial recognition being used. Make clear what the objectives are "which they wish to achieve through the application of facial recognition, and what are the risks which stand in the way of that objective" (R1).
R2 agrees it is important that it becomes clear "which risks are there" and the municipality "should be transparent about that". R1 agrees on this by mentioning that the case should also be reviewed by the municipal council "before the municipality decides to implement it".
R2 suggests a way of mapping out the risks for applying facial recognition could be done by a "discussion in a kind of focus group or an survey to figure out how people think about" the application. Also, the "internal risks" like costs, "does it deliver the right" results and what is "the perspective of the citizen/ society are important" (R2). This perspective of the citizen is something which R2 would want to see "reflected very specifically, because it is also community money that is spent". In this reflection it is most important to focus on the data protection part since the "technical requirements are not so important to society" (R2).

The Dutch municipality X conducted a research in order to find out the opinion from the citizen about facial recognition in public areas. They gave presentations in order to see the reactions of citizens and from the internal organization. "Being transparent about image recognition, where does it happen, organize meetings about it, and see the reactions of people", also "internally within the organisation" (R3). This way of identifying risks is in line with the perspective of the experts privacy and security, as described in the previous paragraph.
For risk identification in case of facial recognition for municipalities, R3 would "look for someone" with a Master's program in Business Administration and "make it an assignment to sort" out the risks and applicability. Additionally, there will always be the "point of view from the parties" and "the elections" which has an influence on the risk identification and decision making (R3).

4.12 Pre-implementation

Before implementation of an application like facial recognition, it is important to “ensure the that entire security of that entire environment is in order” which has to do with the security of the data (R1). Following, there should be “maximum attention to communication and managing expectations” (R1). To be able to objectify this case it is important to analyse “the independent view out of the direct field of those involved and the importance” (R1). A way of doing this is to let some independent person look at it.

After all, there is probably “not one good method” for identifying the risks of using facial recognition because of the “sensitivity of this topic” (R2). There should be a “really thorough analysis” to be able to “cover the risks as broadly as possible in order to ensure that data is not misused” (R2). R1 has another view on this because once the risks have been analysed, the results can in principal be used by every municipality as a starting point. “there are a lot of things that one municipality has to deal with that you can easily duplicate to another municipality”, “the basis of such an analysis or a lot of important building blocks” (R1).

4.11 Vision on Facial Recognition

The facial recognition expert, R4, expects a rising number of facial recognition applications over time with a higher quality because ”just recently the GDPR came in and people are a bit more comfortable now with the data protection regulation”. He thinks that “with time there will be standard applications appearing”. Next to these standard applications, there should be “developed guidelines for each of those applications” “from government organizations”, for any country or any supermarket who wants to deploy it.

Facial recognition is something not being used at the moment within the Dutch municipality X, especially not on public areas. “That actually stems from the coalition agreement of 2018” “that every citizen of the city should be able to move around the city without being spied on” and “there need to be really compelling reasons to do it” (R3). This is also the “personal opinion on this subject” from R3. "There is a variety of computer vision techniques, where we think there are a lot of opportunities, but we will avoid the use of facial recognition because of the mayor concerns about privacy" (R3).

The future of facial recognition is uncertain according to the perspective of R2. He finds it interesting to see if “our societal vision on the topic” of facial recognition would change in a way that “the state is able to impose it on us” (R2). As an example R2 states the following: “imagine this pandemic spreads (…) and it gets so bad that we just want to be able to detect people infected with the virus very quickly”.
Also, R1 points out this societal perspective. R1 names it as an interaction, “because what we, as a society, find acceptable is in any case a shifting goal”. What we find acceptable at the moment “would probably not have been acceptable at all 20 years ago” (R1). At the same time, “there are also counter-movements that say that we should actually take a step back, this is all going too far and we need to think carefully about what we are doing to ourselves” (R1).

5. The method

In chapter 3 the results from literature perspective are displayed and in chapter 4 the results from the experts perspective. In this chapter both perspectives will be merged in order to introduce the Facial Recognition for Public Safety (FRPS) risk governance method. For a visualization of the method, see figure 7.

The method is structured based on the layers, 'define', 'design', 'assess' and 'validate', from the governance framework from Madzou and Louradour, 2020. For the FRPS risk governance method there is added the 'pre-implementation' phase, since based on the expert perspectives there are found some aspects which should be taken into consideration before implementing the application of facial recognition.

Within the method, the information described is labelled with codes. These codes refer to the table in Appendix VII, in which the citations, connected to the codes, are displayed.

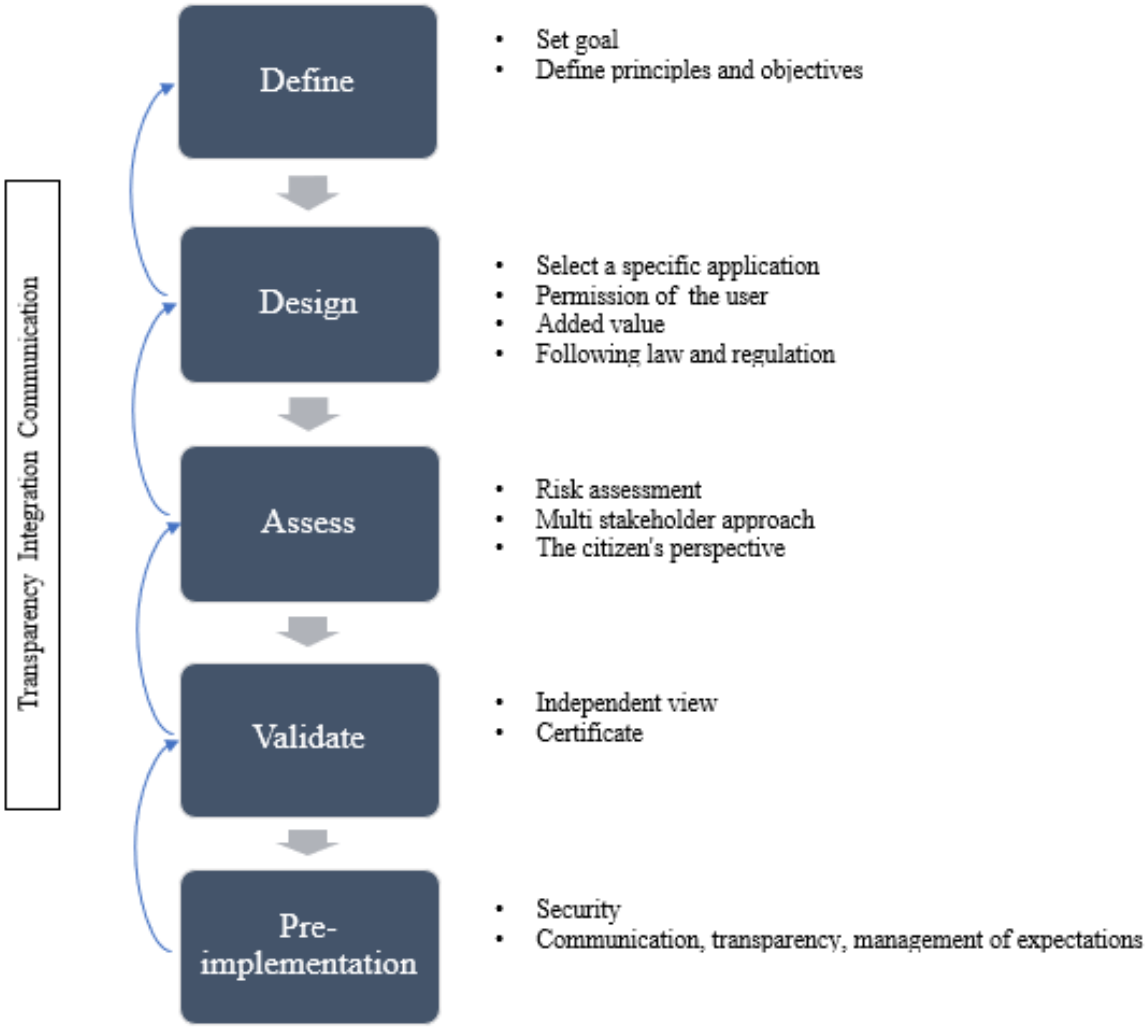


Figure 7. The FRPS risk governance method

5.1 Define

Due to the concern of disproportional usage (FR.1) and the issue of trust around the usage of the data (FR.2 1.1, 1.2), it is important to start with the formulation of the purpose (1.1; 1.2; 1.3; 1.4; 1.5) and scope (1.6) for using facial recognition.

The aim of the define phase from the FRPS risk governance method is the formulation of a goal for using facial recognition for public safety. This consists of formulating a common understanding of the problem (AI.1) and defining objectives for regulatory action (AI.1; FR.3).

It is important to define the goal since it determines what risks are involved (1.2; FR.3). Start with reasoning from the purpose from the perspective of the various stakeholders that are involved (1.7) and also involve these stakeholders in communication and collaboration (AI.2).
Make clear what objectives and/or achievements are there from the perspective of the different stakeholders and what risks might stand in the way (RG.1; 1.7). Stakeholders can be experts, policy-makers, the organization it-self, the general public (RG.2), industry actors, policy makers, civil society representatives and academics (FR.4), the municipal council, CTO, CIO and project manager (1.8).

5.2 Design

The design phase is aiming at the decision on the kind of application which fits the goal and support a responsible design (FR.5). There is a need for a narrowly focused AI governance framework with a focus on specific application areas before a broader and more comprehensive framework would appear (AI.3). Additionally, there might first appear some standard applications together with guidelines for those applications (2.1).

One of these specific application areas might be facial recognition for public safety, in the case of this research. Based on the interview results, there are found the following requirements for the design phase: permission of the user, added value, and following law and regulation.

5.2.1 Permission of the user

The first requirement for the application of facial recognition is permission of the user. There is agreement among the different experts about this requirement as described in chapter 4.8 Permission (2.2; 2.3; 2.5).
The permission requirement can be fulfilled by the supplier party by letting people enrol themselves at the software to ensure that there is complete consent from the user (2.3). Another option is to ask the user for permission (2.5).

5.2.2 Added value

To be willing to implement the application of facial recognition, there should be an added value for the municipality. This means that the application should create an added value for the city, should be scalable and not too expensive (2.6). In case of facial recognition it is hard for a municipality to outweigh the costs because when using personal data, the juridical costs will be really high (2.7). Next to these juridical costs, the costs of the system should be taken into account (AI.1; FR.6; 2.8).

5.2.3 Following law and regulation

The usage of facial recognition goes along with the usage of personal data. This creates a risk of doing something illegal as a governmental organization because the use of personal data is within the privacy regulations (2.9). Therefore, a strict criteria for deciding is the law. The application should follow the law and regulations from the General Data Protection Regulation (GDPR) (FR.7; 2.10; 2.11). A mandatory criteria for a municipality is to execute an analysis on privacy risks (2.12). The Data Privacy Impact Analyse (DPIA) is an analysis which should be used Dutch municipalities (2.13). Additionally, there is the baseline information security government (BIO) (VNG, 2020) on which the municipalities should base their information security policy and their justification (2.14).

After following the law and regulations, there might be expected the ethical, privacy and law aspects are considered correctly (2.15). However, as written in the results, there are some concerns to take

into consideration. Probably individual rights are not strictly shielded by laws (FR.8) or it is not always clear what is permitted and what not (2.16). Having this said, it is not always a wise idea when it is following the law and regulations (2.17) so probably there should be developed more guidelines (2.18).
Another concern is the level of quality of the analysis which goes along with the knowledge and qualification of the person executing the analysis (2.19). To mitigate this concern in the best way possible, there should be integrated different players in the risk identification phase to get a comprehensive view of risks. This is called the multi-stakeholder approach which is addressed in paragraph 5.3.2.

5.3 Assess

The aim of the assessing phase is to assess the responsible design with the principles from the define phase (FR.9). There are some important aspects based on the results from the interviews and the literature.

5.3.1 Risk assessment

It is important to execute a really thorough analysis to be able to coder the risks as broadly as possible for ensuring that the data is not misused (3.1). Identifying the risks could be done by conducting a research towards the risks and applicability (3.2) or the risks could be mapped out during a discussion in a kind of focus group or an survey to figure out how people think about the application (3.3).

Another part of the assessment will be dependent on the political position of the city and its elections which will have an influence on the identification of risks and the decision making (3.4; 3.5).

To support the assess phase it could be useful to have an overview of to be expected risks, there are mentioned several risk throughout this research. An overview is given in the table in Appendix VIII.

5.3.2 Multi stakeholder approach

For identifying and assessing all the risks it is important to involve different stakeholders, or also referred to as consensus-driven approach or multi stakeholder approach (AI.2). This approach creates belief, trust and commitment about the idea designed and boosts acceptance and positive effects in society (AI.2). Furthermore, it ensures a trustworthy and safe usage of facial recognition (FR.10). The stakeholders mentioned in the define phase should be taken into account in the assess phase again.

After all, this multi stakeholder approach seems not only important in the define and assess phase, but through the whole process of risk governance because of the great impact on society it can have (RG.3; AI.4). Besides, the integration, stakeholder engagement and reflection of and together with these stakeholders is important for creating a good background for the risk assessment coming up (RG.4; RG.5).

Within the assess phase, it is important to integrate the citizens perspective as a part of the stakeholder approach (3.6). A way to integrate this perspective is by organizing presentation and observing the reaction form citizens and the internal organization (3.7).

5.4 Validate

The goal of the validation phase is to get a certification, for proving the ability to deploy a system following the principles for responsible usage and provide an audit from a trusted third party (FR.11; 4.1; 4.2)

To validate the application, it is important to get a view from an independent party for objectifying the case (4.1). A way to do this could potentially be the trusted third party giving out a certificate (FR.11; 4.2). There is still some research needed towards the level of transparency and measurability of the application, before this would be possible (4.2).

The certificate could serve, next to the validating purpose, as a solution for the trust issue by showing, and at the same time communicating, that the application is following the guidelines for receiving this certificate (4.2).

5.5 Pre-implementation

The pre-implementation phase is added in this FRPS risk governance method to point out some aspect which should be taken into consideration before implementing the facial recognition application.

At first, it is important to ensure that the entire security around data from the entire environment in which the facial recognition is going to be applied is in order (5.1).

Then there is quite some reluctance around the topic which should be taken into consideration (5.2). There are some questions around this topic from the citizen's perspective like how is the information handled, is the privacy guaranteed, can someone prevent him or herself from being falsely accused, the freedom of people, etcetera (5.3). All the uncertainty around the topic of facial recognition creates reluctance (5.3). Next, there are some question from the internal perspective like who dares to say something from the political side, who is going to be decisive, are there clear guidelines from the national government and who is going to give a clear opinion about this topic (5.4).

If there would be a meaningful application, then it is really important to put effort in good communication, transparency and managing expectations (5.5). The municipality can come up with an application juridically valid but then there is still the risk of society feeling surprised which could result in a lot of reactions (5.6). This makes the effort in good communication, transparency and managing expectations even more important.

5.6 Transparency, integration and communication

In the previous paragraphs of the results chapter and analysis chapter, there is already mentioned a lot about transparency, integration and communication (RG.6; RG.7). In line with the literature, these aspects are important during the whole process of risk governance (RG.6; RG.7). Therefore, these aspects should be integrated in the define, design, assess and validate phase.

A way of being transparent about facial recognition is to organize meetings about it, explain where and how it will be implemented and observe the reactions coming from these meetings, or focus group discussions or surveys (3.3; 6.1). Also the supplier can support in these aspects by charting the different data flows and cloud based environment which are there and try to manage this in transparency and assure only the user can access the data (6.2).

6. Conclusion

The main research question was stated as *"How should the FRPS risk governance method be designed to give support towards making a decision on using facial recognition for public safety?".*
This study shows that by investigating different views about the risks and risk governance aspects for the decision-making process on using facial recognition for public safety by municipalities, there can be concluded on a risk governance method for facial recognition in the area of public safety.

6.1 The risk overview

The first sub question of this research was stated as: *"What risks can be identified for using facial recognition in the area of public safety?"*.

For answering this questions, there is executed a systematic literature review. This resulted in a literature-based risk overview. Additionally, the literature-based risk overview is demonstrated to the respondents in this research who were asked for feedback and additions. In the end, this resulted in a risk overview based on literature and the expert perspective. The overview is displayed in Appendix VIII.

6.2 The risk governance aspects

"What are risk governance aspects for the municipal decision-making process on using facial recognition for public safety?" was the second sub question stated in this research.
To answer this sub question, there are conducted interviews with experts from different backgrounds. The goal of these interviews was to figure out which aspects are important for risk governance towards the decision on using facial recognition for public safety. The interviews resulted in the following aspects:

1) Define: Set a specific goal for the usage of facial recognition (within public safety)
   - Set goal
   - Principles and objectives based on stakeholders' perspective and resulting risks
2) Design: Decide on the kind of application which fits the goal
   - Standard application or broad design
   - Requirements:
   Permission of the user (let them enrol themselves/ ask for permission),
   Added value (added value for citizen/ value outweighs the costs),
   Following law and regulation (GDPR, DPIA, BIO);
3) Assess: Assessment of the design and risks
   - Multi stakeholder approach
   - Include the citizens' perspective
   - Risk assessment with to be expected risks
4) Validate: Validation of the application
   - Independent view out of the direct field (audit)
   - Certificate
5) Pre-implementation:
   - Check security of the environment
   - Take into account transparency, communication, managing expectations for mitigating reluctance

These aspects are further explained and visualized in chapter 5, which together form the Facial Recognition for Public Safety (FRPS) risk governance method.

6.3 Recommendations for practice

The FRPS risk governance method is not a command-type of method, but should be read as a method containing aspects within the risk governance process which need to be seriously considered. This is

in line with the definition of risk governance as a set of aspects for informing all stakeholders involved on how to deal responsibly with risks (Van Asselt & Renn, 2011).
The method has a step-by-step approach which should, in the perfect situation, be followed on order. However, there might occur situations where it is needed to take a step back. For this reason there are arrows presented in the figure to show the situation of being able to go to a previous step.
These recommendations and the FRPS risk governance method need to be validated by doing further research in practice.

6.4 Limitations and further research

After all, this research contains some limitations which could be used as a venue for further research. A first limitation of this research is that there is probably not one good method in the case of using facial recognition because of the sensibility of the topic (R2). Therefore, it might be interesting to further investigate to methodologies and options for governing the risks around facial recognition in the area of public safety.

Secondly, the research of this thesis has a focus on risks. Based on the research from Renn and Graham (2006) it is equally important to focus on a concern assessment, which should complement the risk assessment with insights from risk perception studies and analysis of social and economic implications (Renn & Graham, 2006). The FRPS risk governance method mainly focuses on risks, since that is the goal of this research, for further research it would be interesting to investigate the role of concerns being important in the governance process and decision making process around the usage of facial recognition.

This research has a focus on the Netherlands in case of the described situation and the respondents chosen for this research. For further research it would be interesting to compare the findings among other areas like, Europe, America or Asia. Based on this research, R2 mentions to “take a closer look” into Amerika considering the research which is done there and the incidents “concerning ethnic profiling”. Also R3 mentions there is a different perspective on facial recognition and privacy in China.
This research is focussed on the decision making of municipalities. For further research, it would be interesting to figure out if the method could work for all sizes and kinds of organizations.

There should be done further research to specific applications of facial recognition. When there are more applications, there will be the possibility for research to a broader and/or more comprehensive framework (R4; Butcher & Beridze, 2019).

As described in paragraph 4.5 Legal, there is the concern of the law not always being clear about what is permitted and what not (R2). Additionally, following the law will not always be decisive for the application being a good decision (R1) and there should be developed further guidelines (R4) for making a responsible decision on using the facial recognition applications for public safety.

At last, in the FRPS risk governance method, there is mentioned the aspect ‘certificate’. As described in the analysis, there are some concerns about the level of transparency and that being measurable (R2). To be able to develop such a certificate, there should be conducted further research.

References

Article 29 Data Protection Working Party. (2012). *Opinion 3/2012 on developments in biometric technologies; Opinion 3/2012 on developments in biometric technologies*. http://ec.europa.eu/justice/data-protection/index_en.htm

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. In *European Journal of Operational Research* (Vol. 253, Issue 1, pp. 1–13). Elsevier B.V. https://doi.org/10.1016/j.ejor.2015.12.023

Aven, T. (2018). An Emerging New Risk Analysis Science: Foundations and Implications. *Risk Analysis*, *38*(5), 876–888. https://doi.org/10.1111/risa.12899

Awais, M., Iqbal, M. J., Ahmad, I., Alassafi, M. O., Alghamdi, R., Basheri, M., & Waqas, M. (2019). Real-time surveillance through face recognition using HOG and feedforward neural networks. *IEEE Access*, *7*, 121236–121244. https://doi.org/10.1109/ACCESS.2019.2937810

Aytekin, E. (2020, April 20). *Steps taken by countries in fighting COVID-19 pandemic*. Anadolu Agency. https://www.aa.com.tr/en/health/steps-taken-by-countries-in-fighting-covid-19-pandemic/1812009

Barnoviciu, E., Ghenescu, V., Carata, S.-V., Ghenescu, M., Mihaescu, R., & Chindea, M. (2019). GDPR compliance in video surveillance and video processing application. *2019 10th International Conference on Speech Technology and Human-Computer Dialogue, SpeD 2019*. https://doi.org/10.1109/SPED.2019.8906553

BBC. (2020). *IBM abandons "biased" facial recognition tech*. BBC. https://www.bbc.com/news/technology-52978191

BBC. (2020). *Russia uses facial recognition to tackle virus*. BBC. https://www.bbc.com/news/av/world-europe-52157131/coronavirus-russia-uses-facial-recognition-to-tackle-covid-19

BBC. (2020). *Facial recognition: EU considers ban of up to five years*. BBC. https://www.bbc.com/news/technology-51148501

Betta, G., Capriglione, D., Crenna, F., Rossi, G. B., Gasparetto, M., Zappa, E., Liguori, C., & Paolillo, A. (2011). Face-based recognition techniques: Proposals for the metrological characterization of global and feature-based approaches. *Measurement Science and Technology*, *22*(12). https://doi.org/10.1088/0957-0233/22/12/124005

Burgess, M. (2018). *Facial recognition tech used by UK police is making a ton of mistakes*. Wired. https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival

Chun, W. H., & Papanikolopoulos, N. (2016). Robot surveillance and security. In *Springer Handbook of Robotics*. https://doi.org/10.1007/978-3-319-32552-1_61

Clarivate. (2020). *Web of Science: Confident research begins here.* https://clarivate-com.ezproxy2.utwente.nl/webofsciencegroup/solutions/web-of-science/

Delcker, J. (2019). *Big brother in Berlin*. POLITICO. https://www.politico.eu/article/berlin-big-brother-state-surveillance-facial-recognition-technology/

Elsevier B.V. (2019). *Scopus Factsheet*. *February*, 2. https://www.elsevier.com/__data/assets/pdf_file/0017/114533/Scopus_GlobalResearch_Factsheet2019_FINAL_WEB.pdf

European Commission. (2020). *When is a Data Protection Impact Assessment (DPIA) required?* https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en#:~:text=A DPIA is required whenever,rights and freedoms of individuals.

European Union Agency for Fundamental Rights. (2020). *Facial recognition technology: fundamental rights considerations in the context of law enforcement*. https://doi.org/10.2811/524628

Fischer, S. (2020, September 1). *Algorithmic systems in the coronavirus pandemic – The European approach between surveillance and the protection of basic rights*. Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/en/our-projects/ethics-of-algorithms/project-news/default-1794cf7d46

Gorodnichy, D., & Granger, E. (2015). Target-based evaluation of face recognition technology for video surveillance applications. *IEEE Workshop on Computational Intelligence in Biometrics and Identity Management, CIBIM, 2015-Janua*(January), 110–117. https://doi.org/10.1109/CIBIM.2014.7015451

Han, B.-J., Jeong, H., & Won, Y.-J. (2011). The privacy protection framework for biometric information in network based CCTV environment. *2011 IEEE Conference on Open Systems, ICOS 2011*, 92–96. https://doi.org/10.1109/ICOS.2011.6079313

Hanania, P.-A., & Thieullent, A.-L. (2020). *Perform AI for Public Sector: Public goes AI!* Business Process Incubator. https://www.businessprocessincubator.com/content/perform-ai-for-public-sector-public-goes-ai/

IRGC. (2019). *IRGC Risk Governance Framework*. International Risk Governance Council. https://irgc.org/risk-governance/irgc-risk-governance-framework/

IRGC. (2019). *What is Risk Governance?* International Risk Governance Council. https://irgc.org/risk-governance/what-is-risk-governance/

Joshi, N. (2019). *The implementation of facial recognition can be risky. Here's why...* Forbes. https://www.forbes.com/sites/cognitiveworld/2019/08/29/the-implementation-of-facial-recognition-can-be-risky-heres-why/#19db59487863

Jurevičius, R., Goranin, N., Janulevičius, J., Nugaras, J., Suzdalev, I., & Lapusinskij, A. (2019). Method for real time face recognition application in unmanned aerial vehicles. *Aviation*, *23*(2), 65–70. https://doi.org/10.3846/aviation.2019.10681

Kapatamoyo, M., Ramos-Gil, Y. T., & Márquez Dominiguez, C. (2019). Algorithmic discrimination and responsibility: Selected examples from the United States of America and South America. In *Communications in Computer and Information Science: Vol. 1051 CCIS*. https://doi.org/10.1007/978-3-030-32475-9_11

Karishma, A., Anand Krishnan, K. V., Kiran, A., Dalin, E. M., & Shivaji, S. (2018). Smart office surveillance robot using face recognition. *International Journal of Mechanical and Production Engineering Research and Development*, *8*(3), 725–734. https://doi.org/10.24247/ijmperdjun201877

Kim, J., & Park, N. (2019). Lightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing. *Personal and Ubiquitous Computing*. https://doi.org/10.1007/s00779-019-01299-w

Krishna, A. (2020). *IBM CEO's Letter to Congress on Racial Justice Reform* (p. 3). IBM. https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/

Kuo, L. (2020). *"The new normal": China's excessive coronavirus public monitoring could be here to stay*. The Guardian. https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay

Li, Y., Liu, L., Lin, L., & Wang, Q. (2017). Face recognition by coarse-to-fine landmark regression with application to ATM surveillance. In *Communications in Computer and Information Science* (Vol. 772). https://doi.org/10.1007/978-981-10-7302-1_6

Maeng, H., Choi, H.-C., Park, U., Lee, S.-W., & Jain, A. K. (2011). NFRAD: Near-infrared face recognition at a distance. *2011 International Joint Conference on Biometrics, IJCB 2011*. https://doi.org/10.1109/IJCB.2011.6117486

Magid, L. (2020). *IBM, Microsoft and Amazon not letting police use their facial recognition technology*. Forbes. https://www.forbes.com/sites/larrymagid/2020/06/12/ibm-microsoft-and-amazon-not-letting-police-use-their-facial-recognition-technology/#46242f101887

Martin, N. (2019). *The major concerns around facial recognition technology*. Forbes. https://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/#373a435f4fe3

Medapati, P. K., Tejo Murthy, P. H. S., & Sridhar, K. P. (2019). LAMSTAR: For IoT-based face recognition system to manage the safety factor in smart cities. *Transactions on Emerging Telecommunications Technologies*. https://doi.org/10.1002/ett.3843

Ministry of Economic Affairs and Climate Policy. (2019). *Strategic Action Plan for Artificial Intelligence*.

Ministry of Social Affairs and Employment. (2020). *Werken in Nederland*. Rijksoverheid. https://www.rijksoverheid.nl/onderwerpen/coronavirus-covid-19/werknemers/werken-in-nederland

Niu, J., Tang, W., Xu, F., Zhou, X., & Song, Y. (2016). Global research on artificial intelligence from 1990-2014: Spatially-explicit bibliometric analysis. *ISPRS International Journal of Geo-Information*, *5*(5), 1–19. https://doi.org/10.3390/ijgi5050066

Oliver, K., & Neenan, A. (2020). *In the blink of AI: How facial recognition technology is capitalising on the COVID-19 crisis*. Euronews. https://www.euronews.com/2020/05/14/in-the-blink-of-ai-how-facial-recognition-technology-capitalising-on-covid-19-crisis-view

Ovide, S. (2020). *A Case for Banning Facial Recognition*. New York Times. https://www.nytimes.com/2020/06/09/technology/facial-recognition-software.html

Radu, S. (2019). *The technology that's turning heads*. U.S.News. https://www.usnews.com/news/best-countries/articles/2019-07-26/growing-number-of-countries-employing-facial-recognition-technology

Renn, O., & Graham, P. (2006). *Risk Governance, Towards an integrative approach*.

Rouse, M. (2020). *Face detection*. SearchEnterpriseAI. https://searchenterpriseai.techtarget.com/definition/face-detection

Safran. (2017). *Safran Identity & Security provides a facial recognition system to the National Police of the Netherlands*. Safran. https://www.safran-group.com/media/safran-identity-security-provides-facial-recognition-system-national-police-netherlands-20170316

Savastano, M. (2017). Noncooperative biometrics: Cross-jurisdictional concerns. In *Human Recognition in Unconstrained Environments: Using Computer Vision, Pattern Recognition and Machine Learning Methods for Biometrics*. https://doi.org/10.1016/B978-0-08-100705-1.00010-5

Schaffer, L., Kincses, Z., & Pletl, S. (2017). FPGA-based low-cost real-time face recognition. *SISY 2017 - IEEE 15th International Symposium on Intelligent Systems and Informatics, Proceedings*, 35–38. https://doi.org/10.1109/SISY.2017.8080568

Schiphol. (2019). *Travel with facial recognition – pilot*. Schiphol. https://www.schiphol.nl/en/page/trial-border-passage-based-on-facial-recognition-cathay-pacific/

Shareef, I. R. (2016). Design and implementation smart security system based on Artificial Neural Network. *ARPN Journal of Engineering and Applied Sciences*, *11*(9), 5592–5602.

Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. *Proceedings of the ACM Conference on Computer and Communications Security*, *24-28-Octo*, 1528–1540. https://doi.org/10.1145/2976749.2978392

Sharma, S. (2020, June 24). *Maintain social distancing, use of face masks to avoid second Covid-19 wave - health - Hindustan Times*. Hindustan Times. https://www.hindustantimes.com/health/maintain-social-distancing-use-of-face-masks-to-avoid-second-covid-19-wave/story-SFPWbxW0qTSpeZQvU7MLVJ.html

Smith, B. (2018). *Facial recognition technology: The need for public regulation and corporate responsibility*. Microsoft . https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/#:~:text=Facial recognition technology%3A The need for public regulation and corporate respo

Spektor, M. (2020). Imagining the Biometric Future: Debates Over National Biometric Identification in Israel. *Science as Culture*, *29*(1), 100–126. https://doi.org/10.1080/09505431.2019.1667969

Street, F. (2019). *How facial recognition is taking over airports*. CNN . https://edition.cnn.com/travel/article/airports-facial-recognition/index.html

Tada. (2020). *Het Tada manifest*. https://tada.city/

Van Boom, D. (2018). *Jaywalking in China? Surveillance system could SMS you a fine*. Cnet. https://www.cnet.com/news/jaywalking-in-china-surveillance-system-will-sms-you-a-fine/

van der Haar, D. T. (2019). Real-Time Face Antispoofing Using Shearlets. In *Communications in Computer and Information Science* (Vol. 973). https://doi.org/10.1007/978-3-030-11407-7_2

VNG. (2020). *Baseline Informatiebeveiliging Overheid (BIO)*. VNG. https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/

Voda, A. I., & Radu, L.-D. (2019). How can artificial intelligence respond to smart cities challenges? In *Smart Cities: Issues and Challenges*. Elsevier Inc. https://doi.org/10.1016/b978-0-12-816639-0.00012-0

Wirtz, B. W., Weyerer, J. C., & Sturm, B. J. (2020). The Dark Sides of Artificial Intelligence: An Integrated AI Governance Framework for Public Administration. *International Journal of Public Administration*, *43*(9), 818–829. https://doi.org/10.1080/01900692.2020.1749851

Madzou, L., & Louradour, S. (2020). Building a governance framework for facial recognition. *Biometric Technology Today*, *2020*(6), 5–8. https://doi.org/https://doi.org/10.1016/S0969-4765(20)30083-7

Varley-Winter, O. (2020). The overlooked governance issues raised by facial recognition. *Biometric Technology Today*, *5*, 5–8. https://doi.org/https://doi.org/10.1016/S0969-4765(20)30061-8

Butcher, J., & Beridze, I. (2019). What is the State of Artificial Intelligence Governance Globally? *RUSI Journal*, *164*(5–6), 88–96. https://doi.org/10.1080/03071847.2019.1694260

IRGC. (2017). Introduction to the IRGC Risk Governance Framework, revised version. *Lausanne: EPFL International Risk Governance Center*, 1–52.

Van Asselt, M. B. A., & Renn, O. (2011). Risk governance. *Journal of Risk Research*, *14*(4), 431–449. https://doi.org/10.1080/13669877.2011.553730

Jalonen, H. (2007). *Managing Complexity in the Decision-Making of Local Governments The Value from Sport View project Arvoa urheilusta View project Managing complexity in local governments' decision making*. https://www.researchgate.net/publication/268744262

Praveen, G. B., & Dakala, J. (2020). Face Recognition: Challenges and Issues in Smart City/Environments. *2020 12th International Conference on Communication Systems & Networks (COMSNETS)*, 791–793.

World Economic Forum. (2020). *A Framework for Responsible Limits on Facial Recognition Use Case: Flow Management*. www.weforum.org

Giffinger, R. (2007). *Smart cities Ranking of European medium-sized cities*. www.srf.tuwien.ac.at

Appendix I Interview description and instruction

Instructie voor respondenten (Dutch version)

Deze instructie is geschreven voor respondenten van het onderzoek voor de scriptie van Stephanie Roorda. Het doel van deze instructie is het instrueren van respondenten op een goede voorbereiding waardoor het verloop van het interview wordt bevorderd.
Ter voorbereiding van het interview zou ik u willen vragen, de interviewvragen door te nemen. Verder is het van belang dat bij het beantwoorden van de vragen tijdens het interview, de definities van de concepten in beschouwing genomen worden.

Het interview

0. Wat is uw ervaring met gezichtsherkenning? (werkervaring/kennis/visie)
0.1 En gericht op het gebied van openbare veiligheid?
0.2 En bij het gebruik ervan door gemeenten?

Het interview bestaat uit twee delen. Het eerste gedeelte van het interview heeft als doel het identificeren van risico's welke gemeenten in beschouwing zouden moeten nemen voor het besluit tot gebruik van gezichtsherkenning voor openbare veiligheid vanuit uw perspectief.

1. Kunt u aangeven welke risico's u zou beschouwen bij de beslissing in de beschreven definities van dit onderzoek?

2. Op basis van dit overzicht, kunt u aangeven/ markeren welke risico's u beschouwt als zeer relevant in de beschreven context van dit onderzoek?
2.1 Waarom?
2.2 Zijn er risico's weergegeven die u niet zou beschouwen?
2.3 Heeft u aanvullingen van risico's na het zien van dit overzicht?

3. Wat zou uw aanbeveling zijn voor de wijze waarop gemeenten de risico's kunnen identificeren binnen de beschreven definities van dit onderzoek?

Het tweede gedeelte van dit interview heeft als doel tot een idee te komen voor het maken van een risk assessment framework.
Het einddoel van het framework is: het geven van een overzicht van de verwachte risico's en de mogelijkheid om deze risico's te beoordelen. Het kader moet gemeenten ondersteuning bieden bij het nemen van de beslissing tot gebruik van gezichtsherkenning.

4. Op welke wijze kunnen risico's worden beoordeeld voorafgaand aan een beslissing?

5. Zou u vanuit eigen ervaring een risico assessment kunnen aanbevelen voor de beschreven context van dit onderzoek?
5.1 Hoe is dit framework ontworpen?
5.2 Welke argumenten verklaren uw keuze voor aanbeveling van dit framework?

Definities van concepten in het onderzoek

Definitie gezichtsherkenning:
Gezichtsherkenning is een biometrische techniek die in staat is het gezicht van een persoon te identificeren, te matchen, te verifiëren of te categoriseren op basis van de automatische verwerking van digitale beelden (Groep gegevensbescherming artikel 29, 2012).

Processtappen (Joshi, 2019): legt beelden of video's vast', 'leest de geometrische metingen van het gezicht', 'berekent een wiskundige formule voor het vastgelegde gezicht' en 'vergelijkt deze met het beeld in de database'.

Definitie openbare veiligheid:
Het toepassingsgebied van veiligheid, beveiliging en toegangscontrole binnen openbare ruimten en evenementen.

Definitie van een risico:
Een aspect dat een negatief gevolg heeft voor de gemeente (direct) of de maatschappij (indirect voor de gemeente) als gevolg van de beslissing tot het gebruik van gezichtsherkenning.

Instruction for respondents (English version)

This instruction was written for respondents of the research for Stephanie Roorda's thesis. The purpose of this instruction is to instruct respondents on how to prepare for the interview in order to facilitate the course of the interview.
In preparation for the interview, I would like to ask you to go through the interview questions. It is also important that the definitions of the concepts are taken into account when answering the questions during the interview.

The interview

0. What is your experience with facial recognition? (work experience/knowledge/vision)
0.1 And focused on public security?
0.2 And when used by municipalities?

The interview consists of two parts. The first part of the interview aims to identify risks which municipalities should consider for the decision to use facial recognition for public safety from your perspective.

1. Could you indicate which risks you would consider when making the decision in the definitions described in this study?

2. Based on this overview, can you indicate/ highlight which risks you would consider highly relevant in the described context of this study?
2.1 Why?
2.2 Are there risks that you would not consider?
2.3 Do you have additions of risks after seeing this overview?

3. What would be your recommendation for the way in which municipalities can identify risks within the described definitions of this study?

The aim of the second part of this interview is to come up with an idea for creating a risk assessment framework.
The final objective of the framework is: to give an overview of the expected risks and the possibility to assess these risks. The framework should support municipalities in making the decision to use facial recognition.

4. How can risks be assessed prior to a decision?

5. Based on your own experience, could you recommend a risk assessment for the described context of this study?
5.1 How is this framework designed?
5.2 What arguments explain your choice to recommend this framework?

Definitions of concepts in the study

Definition facial recognition:
Facial recognition is a biometric technique capable of identifying, matching, verifying or categorising a person's face on the basis of automatic processing of digital images (Article 29 Data Protection Working Party, 2012).
Process steps (Joshi, 2019): captures images or videos', 'reads the geometric measurements of the face', 'calculates a mathematical formula for the captured face' and 'compares it with the image in the database'.

Definition of public safety:
The field of application of safety, security and access control within public spaces and events.

Definition of a risk:
An aspect that has a negative impact for the municipality (directly) or society (indirectly for the municipality) as a result of the decision to use facial recognition.

Appendix II Transcribed interviews

Expert Privacy and Security (1)
Name: Jan Visser
Organization: PwC
Date: 09-07-2020

J: Okay, I will also introduce myself briefly. Well, I am Jan Visser. I have been working for PwC for over 14 years now. Studied in Groningen. Eh, Business and ICT. PwC is also my first employer, so I've done a number of different things. I once started in IT audits, which is actually very similar to what risk assurance does. I'm from Overijssel myself, I spent quite a few weeks at the Zwolle office when I was still living nearby. That is why I also know these other persons. Well, you will probably meet them there as well. I now work and live in Amsterdam and over the past few years I have been focusing more on security and privacy assignments. From the perspective of the central government and implementing organisations. Myself, I've done few projects for municipalities, or not recently. From a security and privacy perspective, I keep an eye on all technical developments. Because it is often not an issue that is pressing at local level, but also at government level, because when it comes to municipalities, everyone often looks to the minister to give some kind of directive or direction to what we find acceptable or unacceptable in the Netherlands. Yes, well, I would like to leave like this for now, unless you have any questions about it, but.

S: Yes, well, I am still curious about that. I saw on Talent Link that you also had experience with a Smart city project?

J: Um, yes, that's been a while. I have participated in a Smart city project in the past. For a Dutch municipality that was a bit of a commitment, but that was a short involvement. The information on my LinkedIn profile is more or less what my areas of interest are and in that respect, what I'm doing at the moment is more focused on smart mobility. So autonomous vehicles, vehicles that are also connected to their surroundings and for example roadside systems. All kinds of issues of what the surroundings of a city look like when you talk about smart mobility. So you often come across use cases such as: I drive my car through the city centre of Amsterdam. The objective then is to keep transport movements to an absolute minimum, because I don't want the city to be overfull. So actually I want to lead a vehicle to a suitable parking place as quickly as possible. Close to its destination. And eh how am I going to arrange that.

S: Okay.

J: Well that kind of issues and also from a security and privacy perspective. Because then you always have a situation where a large number of parties have to talk to each other and all of them can measure where you come from, where you are at a certain moment and what is reasonably your final destination. Eh you can perhaps imagine that if I park my car near ‘de wallen’ that is not something I would like the whole world to know. So just to sketch an image.

S: That's an assignment from the Advisory branch of PwC, I think? Or am I wrong?

J: Um, it is not a concrete task at the moment. It is more or less the area of work in which we do various assignments.

S: Okay, but do you do your own research, or does that question come from the work field?

J: That question then comes from the work field. *deleted*. It is not the case that we then take the issue as a whole and simply carry out a full analysis. It is more, a certain context, a certain field of work, about which we each time receive questions from and answer them. From there, we get a total picture of what is going on.

S: Yes, okay. Well, that was nice.
At first I was curious about eh what is your own experience with facial recognition? Have you ever get into contact with it or is it a certain knowledge you have about it? Eh yes.

J: Um, yes, I mainly follow the news in that respect. Facial recognition is a very specific part of it, but I also think it is very much related to something broader about how we deal with camera surveillance in general within the public environment.

S: Yes.

J: Yes, these are very relevant discussions and they are also becoming more and more relevant because we have already investigated and answered these kinds of questions for a Dutch municipality. I don't know personally, but I do have colleagues who investigated it more from a privacy point of view. And, yes, there are always new applications where you can also see that a municipality is struggling with what is and what is not within the legal framework. Eh and that's, for example, about eh. Because you can do a lot with cameras. Only the question is, especially the question, how far can and may I go?

S: Yes.

J: Um and you know the moment you hang up a camera at the big market in Groningen or eh at the hole in the market in Enschede, I'll name just a few. These are locations where fights and that sort of things easily arise. So there you have a very important use case to keep an eye on in general terms so that you can quickly send the police there. Well, as a society, we accept that quite easily. Because yes, that is all in our interests, eh. But, you know, at the moment, and as far as that is concerned, general supervision does not necessarily mean that we are immediately recognisable or anything like that. So that still feels safe. Eh.

S: Yes.

J: But a good thing when I drive into the city of Amsterdam and there are cameras hanging above the road. And those cameras do number plate recognition to check whether my vehicle is not too polluting to enter the city. Because I emit too much soot because I have a diesel from the 90s. Eh then that is still a very good use case. That's still a very good use case. A bit more specific for me as a person, because the number plate is of course recognizable on me or can be traced back to me. Then there is what we are now doing within the Dutch government. Eh, that we do not always handle it with the same care and that the police, for example, finds out that it is quite handy for them to be able to signal that if they know that the vehicle comes from or belongs to a certain criminal eh. That it is useful to know when he is driving into town. But then you are environmental cameras, and that actually happens, eh, but then you are in fact, abusing environmental cameras for a purpose other than what it is intended for.

S: Yes.

J: Even though we may, eh. You know, because you can always have a legal discussion about this, but then of course you always have a discussion about society being surprised by this kind of use.

S: Yes.

J: And I think that is also a very important point for the municipalities. That is sometimes confused. “The fact that something is legally allowed, by privacy legislation, does not mean that it is a wise idea” (2.17).

S: Yes, and do you think, from your point of view, that a clear point can ever be found in it? At that intersection?

J: Well, look, I think it is mainly an interaction, “because what we, as a society, find acceptable is a shifting goal”, so to speak. What we find acceptable now ”would probably not have been acceptable at all 20 years ago”. At the same time, however, “there are also counter-movements which say that we should actually take a step back, this is all going far too far and we need to think very carefully about what we are doing to ourselves”. After all, you know, 20 very small steps passed relatively unnoticed. All in all, that is still a very big step. Perhaps we do not realise that we are taking very big steps in the course of time. And facial recognition could be a very important eh, could be a very important one.

S: Yes

J: And these discussions are also taking place at national level. About what is and what is not acceptable. Things like environmental cameras and surveillance in the public environment well, in principle that is what municipalities themselves decide about, but at the same time you can see that there are enough news reports about the extent to which we apply Clearview technology in the Netherlands. Which is facial recognition software from America, where the makers are not really very ethical in filling their database with facial profiles. Because they are simply emptying every possible form of social media with all sorts of photos. And that today or tomorrow they put in the picture of you and me.

S: Yes.

J: And then maybe they can find my high school photos. Well, maybe I don't want that at all.

S: Yes, but is that probably allowed in America? Not in the Netherlands anyway, in Europe?

J: No, we have much stricter privacy legislation in Europe than they have in North America, much stricter.

S: Yes.

J: Eh, so that is why, and much more privacy awareness, that is also why this discussion is simply being conducted at ministerial and parliamentary level, because questions are also being asked about this in Parliament.

S: Yes, because I did indeed find a report in December 2019 stating that they had indeed applied for facial recognition and were carrying out an investigation. I thought, Eindhoven University did research there into all the privacy risks of facial recognition specifically.

J: Yes. And, you know, it is good that these discussions are being held, but from a technological point of view it is probably not a big step at all to say that I link the cameras of the municipality of Amsterdam to the facial recognition software of Clearview and, in that respect we are taking a big step towards security. That could be the argument.

S: Yes.

J: So they are technically small steps, but socially and morally very big ones.

S: Yes. Okay. Eh, and have you worked on a project in which, for example, you really had that discussion about facial recognition? Or is it just that you follow the news and follow developments in the field? And the knowledge of that?

J: No, no. I did not do that myself and, as far as I know, we have not done any further projects on facial recognition. *deleted*

S: Oh yeah.

J: Also with the idea of, because there are, eh, applications in which you can very easily morph photos of two people into a new photo. And then you could end up in the situation that you could commit fraud by obtaining someone else's personal documents.

S: Okay. Yes, because I think city X also does it with passports that they compare eh the photos. Or at least compare the applicant with the photo in the system.

J: Exactly.

S: Yes.

deleted

S: Yes.

J: So that's why they call it photo comparison. But the technology is just the same.

S: Yes, exactly because what makes the “facial comparison”, that it is manageable in terms of risk compared to, for example, a surveillance application. Is it then that the goal is simply much clearer, or how?

J: I think that eh the “goal is more clear” (1.5). That is to begin with. Eh and, it's in fact also eh much less specific and much less concrete because I think that a lot of facial recognition applications, if you apply that to municipalities in public environments, are very much an element of that person was at that location at that time and behaved in that way. Well.

S: That's a lot more information.

deleted

S: Yes. Yes exactly.

J: While the consequences of facial recognition are eh and then from the perspective of errors. Eh while you are going to apply facial recognition to those very bad “security cameras” with those grainy images on eh which you normally always see on eh police programmes, yes. That has a much greater “margin of error”. Yes, then you will also get the examples I sent earlier this week from the man who was wrongly recognised.

S: Yes. Yes, and what consequences does that have for society, eh, trust and eh, yes.

J: Yes, well, it is interesting because there are all effects and there are all very concrete consequences, so, you know, people who are wrongly recognised, are in the news and that has very annoying concrete consequences for them. And something that is often forgotten is that this is called “the chilling effect”.

S: Chilling?

J: The chilling effect. So eh chilling as in cold. That is also what you should Google that is really a scientifically researched phenomenon and in fact that means that the fact that you are “being monitored” and know that you are being monitored, that in itself has an effect on your behaviour.

S: Yes.

J: Even though that behaviour you are planning to do is perfectly legal and nobody should judge it, it's just a certain intervention, it just has a certain effect. So in that sense you can also look at it as yes it is “a restriction of your freedom to behave as you wish”.

S: Yes exactly. Okay. Then I would like to go back to my research.

J: Sorry.

S: What I actually did first is that I did a piece of literature research and actually looked at what risks are described in relation with facial recognition? And then I specifically focused on public safety. And from that point of view, I would actually like to look at the risks that experts have identified so that I can get a kind of first overview of potential risks. And, yes, that is actually the purpose of the first question as to whether you could indeed sketch out what you see from your own perspective as potential risks for a municipality to make a decision to use facial recognition within the public safety sector.

J: Yes. I think that before I asked that question, I had already sorted out a few things, didn't I? I think I did last week.

S: Yes. You've indeed got that data collection, eh, stolen here. That was one

J: Yes, the most important risks I have worked out along the line of privacy.

S: Okay.

J: Because I really think that that's where the most important risks lie.

S: Yes.

J: Eh, because that's what it is. Look, a municipality has a lot of orders to take when they introduce eh cameras with facial recognition. Eh and privacy is one of the most important of those. On the one hand, a little bit what I just said, compliance with the laws and regulations that exist in the field of privacy. Um, that is more of a legal issue. At the same time, however, there is also the "management of society's expectations" (5.6) because, eh, "you can come up with something juridically valid" (5.6), but when it is six months and some journalist writes a piece about that there is a certain application and the whole of "society feels surprised" (5.6), eh. Did not realise sufficiently what the consequences would be or the municipality did not communicate sufficiently eh what they intended to do. Yes then you get half the world over you in "terms of public opinion and politics" (5.5).

S: Yes.

J: Eh. And then above all you get the activists all over you. Who are indeed very much aware of the phenomenon as people are wrongly recognised as someone else, the chilling effect, that you also just ignite the fundamental discussions with the congregation in that area. Eh concrete example. The municipality of Amsterdam, or many municipalities in the Netherlands that have introduced parking by license plate. What actually means eh is that there is a central database which states eh Person X has parked his car in district A of the municipality of Amsterdam and he has bought a parking ticket from 7 o'clock in the evening until 8 o'clock in the morning. There is just a database of that. Eh, it should be, because yes, perhaps it should be possible for vehicles from the municipality to pass by and they should be able to check whether someone has paid or not. There are no more parking tickets behind the front window.

S: Yes.

J: Yes. So that person scans that license plate and checks against the database of this person has paid or has not paid. Wherever the discussion comes up about yes you know we used to have parking where you just paid with cash. You pulled a piece of paper out of one of those machines and put it under your windscreen. So there was no database recording what you parked there. In fact, digitisation is, is it records more data and is an additional invasion of your privacy.

S: Yes.

J: The municipality of Amsterdam was involved in several lawsuits by interest groups that have challenged this. And having said you know this infringement is simply disproportionate in view of the goal you want to achieve because you used to be able to do without a database and now you need a digital database, my privacy is being infringed more heavily. Eh what is this for? This is all illegal. Well, that interest group has been proved wrong. Um, I find something of it myself but, at the same time, you see that and that these kinds of issues within municipalities, that legal action is really being

taken on them, to say the least, if only to create awareness among municipalities that take decisions on these kinds of issues.

S: Yes. For example, I also contacted the city of Amsterdam and they said that they had decided not to do it. I don't know why or how it went, but I thought maybe that's an interesting case study to see what risks they took that they thought yes is the decision not to do it.

J: Yes.

S: That you get some sort of eh understanding of that yes.

J: Yes, in cases like this I am always curious as to whether the decision not to do it was made on the basis of what reasoning. Whether or not it was we think this is a bad idea because we hit our citizens eh disproportionately hard or eh yeah you know it just costs too much money versus the proceeds. So it does not give us anything ourselves.

S: Yes.

J: So have they reasoned more out of self-interest that it does not make sense or have they reasoned out of someone else's interest that it is a bad idea. It can also often be the first one, because municipalities sometimes just make a mess of things in this area. Yes, they do. It is often the case that governments reason very objectively from a legal point of view from a business case and do not reason at all from an ethical point of view.

S: Okay.

J: Then the question is because they themselves may not even realise that it is an ethical issue. They just see this is a useful idea eh this costs money, this gives us a lot, so we are going to do it. They do not even think that this is sensible for the future. Do I have to go down this road at all, given the possible consequences that may arise?

S: Yes. Yeah, that's why I thought I saw this gap that the risks are simply not mapped out in municipalities either. That that is actually the first risk in itself.

J: Yes. Well, according to eh. If you just look at what is legally required eh. Just take a look at the AP website. The personal data authority. Eh, in my opinion, supervision is in the public domain. So large-scale supervision is one of the reasons why you are obliged to carry out a data protection impact assessment. Eh so it is “mandatory to execute an analysis on privacy risks” (2.12) for the people you are monitoring.

S: Okay.

J: You are obliged to do that.

S: Okay, so municipalities have to go through that anyway.

J: Municipalities have to do that anyway.

S: Okay.

J: The only question is, are they doing it well?

S: Yes. Okay, that changes my view a bit, you know. Look, that's something they have to go through anyway, but yes, it's a good thing that it might also be interesting how they do that and what is then described in such a framework.

J: Yes. Eh are they indeed just filling it in purely, in other words, are they indeed standing still for a moment to reflect. Whether and how well, how qualified is “the person who executes the analysis” (2.19), because that can become very “in-depth, juridical and moral discussions”, if you want to do it well. As you know, we simply charge you 20 days to find out, but then you know exactly where you stand.

S: Yes.

J: In other words, do you really stand still in order to “reflect objectively” and to say that this is a good or a bad idea or do you use “applied goal reasoning” (1.4). Eh we are just going to do it. I am an authoritarian driver. Eh DPIA is just some mandatory annoying order I have to take. You know the result is what I want to get out of it. That happens sometimes. And then sometimes you're reading absolutely shit.

S: Yes that they just fill in ‘something’.

J: Yes, but well you have fulfilled the legal “obligation”. Check we have done a DPIA. Yes it does not say that it has to be a good DPIA. We have done a DPIA.

S: But what else would you do based on your experience? What would you recommend, for example, to fill in a different framework or other aspects that they should take a closer look at?

J: Yes, as far as that's concerned, that's a bit of the problem. There is in fact already a big part in such a DPIA because it is precisely the intention “that you take a very broad view of the consequences for the citizen”. A good thing, however, is that when you turn it into an internal party, you always run the risk of the quality suffering. Eh because yes, you depend on the competence of “the person who executes the analysis” (2.19). Eh there may be administrative pressure, eh it is forgotten. ‘Forgotten'. Eh you know all that can suffer from the quality. What would be most practical would be to just say we try to objectify this issue as much as possible and we try to get the analysis and “the independent view out of the direct field of those involved and the importance” (4.1). Eh and we let someone look at it independently.

S: Yes exactly.

J: Well, for example, the city of Amsterdam has a privacy committee. In administrative terms it is completely dependent on the rest of the municipality of Amsterdam, but in that respect I think it is interesting to know that the municipalities themselves are also united in what is called the Association of Dutch Municipalities (Vereniging Nederlandse Gemeenten, VNG). That is also a separate legal entity and it facilitates, a lot of security, privacy and technology developments by saying that we either develop or we do something once and that is then usable for all municipalities. Eh because, yes,

look, municipalities like to pretend that they are special. Eh and you know, in essence it comes down to the fact that “there are a lot of things that one municipality has to deal with that you can easily duplicate to another municipality”.

S: Yes. Yes, what you said already in the piece you typed.

J: Exactly. So “the basis of such an analysis or a lot of important building blocks”, take this into account, take this issue into account, yes, you could already do this across all municipalities.

S: Yes.

J: And at the moment you're just being very critical. Yes, then the municipality will have to explain later why they have deviated from what is already the highest standard of eh quality standard of the DPIA, because they wanted to push their own interests through.

S: Yes.

J: And then you have a completely different discussion.

S: Yes, because that was also a little doubt in my research or I. In the first instance I wanted to go out to several municipalities and ask how did you go through that decision-making process, what did you run into eh and what kind of framework did you use or not? Anyway, I have come to the conclusion, after consulting with my professor, that it might be more interesting to immerse myself in one and actually test it with what I have already found in terms of frameworks and risks. Whether they are there, have they seen them? Eh what has been filled in and what maybe not yet. Eh that you then actually get a lot more information than when you would do several.

J: Yes, well, you would. If you look at an organisation that perhaps has a great deal of overview across all the municipalities, it's probably VNG. The VNG.

S: Yes, I wrote that down.

J: Yes, so it might be interesting to look at and also as an example of how more people are working on facial recognition at the national government level. Also this one. [link] A lot of questions are being asked about Clearview at the moment. This is a message from two days ago.

S: Okay. Yes because a lot is happening so I also have the feeling that sometimes I don't even keep track of everything. Because for example IBM stopped developing. Yes, but that's a good thing that makes it interesting, of course.

J: Microsoft has also stopped, I think Google has also stopped. Eh, but yes, it is also a question of whether or not this is temporary.

S: Yes, exactly.

J: I don't know whether I had already sent this on, but eh Last Week Tonight.

S: Yes, I think I have that eh.

J: He also had an episode about Clearview and facial recognition two or three weeks ago. Eh it is of course American, but at the same time, he is very clear about the essentials of the issues.

S: Yes.

J: I think there is an episode of it on YouTube. And others you just have to [unintelligible]. I think you have a pretty good network there in Twente.

S: Yes. And what would you eh. I actually want to look at a framework in order to find out what the possible risks might be, so that they already have a piece they could look at and then also be able to look at what risks there are for us and can we cover them? That there is a kind of yes that they have support for the decision. But who do you see as eh experts to give input on this, for example? You said yes to the municipality, but the question is always whether they really have the knowledge or the eh.

J: Yes. Is this more of a question for your research now or at the moment that a municipality has to deal with it?

S: No, more for my research as well. Yes.

J: Yes I think you should take a look at the, that's a good question. Um, I don't know who in the Netherlands is the expert in this field. Um yes, I'm not that deep into it, but look at some professors who are very involved with privacy. Person X is one of them. He is a lecturer in Groningen.

S: Oh yeah.

J: Person X is someone from the University of Tilburg.

S: And I thought so myself. In Enschede there is also an eh who is no longer a start-up, but who also developed facial recognition. Maybe it's also interesting to ask a developer how they see it. So that you also have some kind of insight into this.

J: Definitely. You know, it's a bit of a question of knowing which way you want to go with the research. Do you want to explore the technology or do you want to explore the issues of what does it mean for us as a society and what consequences does it have?

S: Yes. Yes, indeed, I want a municipality to have insight. Eh what kind of risks there are on the basis of which they can make a decision towards usage. That is actually an overarching issue. And yes, in the first instance I would have preferred it if you could map out as many risks as possible, because I am aware that privacy, for example, is a very large area, and perhaps in the technical area you can also find things, and in the legal area, what is possible and not possible in terms of legislation, so it is quite a broad issue, perhaps. I am somewhat searching for a general picture, or should I still need to zoom in, yes.

J: Hmm, that is a good question. Eh. Yes, look. You see, I can't imagine that there haven't been very clever people who have put all their thoughts on paper.

S: Yes.

J: And, you know, in that respect there will be quite a bit of science to be found, eh. I don't really have an organisation or a person in mind who's really deep in this or says yes, you know, that's the authority that writes about it. The perspective that always springs to mind, but that is also just my perspective on a lot of issues, especially privacy and cyber security issues.

S: Yes.

J: And yes, there are also certain geo-political angles. Eh, but yes, that is a bit more distant, you know, for example, the eh battle between the economic power blocks that we now have in the Netherlands, eh in the world. So you know China versus America versus the European Union. China is sponsoring the roll-out of a camera network with facial recognition in Sarajevo. And that Sarajevo, eh Serbia? Well, in any case, it is Europe.

S: Yes, it is there somewhere.

J: At least the Balkans. Well, that corner. As you know, this is, of course, an angle in which the main intention is, to be independent of the influences they have on the Balkans, because, yes, the Balkans is situated a little between the European Union and the rest of the world. That is actually not a European Union at all. So yes, China is trying to gain influence in Europe. That is one and the second thing they are trying to do; they also have direct access to all those cameras and everything that goes with them. So they just see a lot of, uh, white males and females passing by and that is also something they use to improve their own products. Because eh traditionally you are an Asian country and you train your cameras on Asian people then they become very good at recognising Asian people, but white people and dark coloured people, they are very bad at that because they are not trained for that.

S: Yes. Yes exactly. Eh back to that risk assessment or identification for a municipality. At least then you have the DPIA that a municipality has to comply with by law anyway. Imagine you would have to make the decision together with a municipality about the fact that we are going to introduce facial recognition. What would be an eh activity that you would undertake in order to be able to make a decision?

J: I would eh I would very well “ensure that the entire security of that entire environment is in order” (5.1). Eh that also has to do with the risk I outlined of, for example, data leaks or, you know, someone else getting access to those cameras. Eh at the moment of such an incident, you know what? Eh then you are already three zero behind. And I would try it with a very good story and paying “maximum attention to communication and managing expectations”.

S: Yes.

J: And that, this sort of thing, I can't imagine that this sort of thing doesn't have to go through the city council, for example. “Before the municipality decides to implement it” (3.5), I can't imagine. I don't know exactly how municipal democracy works, but eh, you know, you already have words to overcome there and yes, that also means in public communication that your own inhabitants have to find something of it.

S: Yes.

J: They should not be surprised in expectations of yes wait a minute I did not know at all that I was being watched when I walked on the big market in Groningen.

S: Yes. Okay. Um, let's see if I've missed anything. Yes. I did a systematic literature review myself. I did that on the terms facial recognition and then public safety and risks. And I did this with different search terms, but a group of risks came out of which I would like to know from you which one from this list you would really see as highly relevant within this issue for a municipality. And which one you might not see as a risk at all.

J: Okay

S: As a piece of addition to literature research that would be.

J: Yes.

S: Um, but then I'm going to share my screen. I think that's useful. Does it do anything or not yet?

J: Eh not yet.

S: Oh. Yes. I think it does now.

J: Yes, I see what's happening.

S: Yes. Well it's not in order at all. It's just for each article what I found in it, I filtered out.

J: That's good. I eh. My question is whether you can make it a little bigger because eh.

S: Oh yes.

J: I can still read it reasonably well, but at the same time eh. Yeah, that's great.

S: Like this?

J: Yes.

S: And would you be able to read from top to bottom and if you see one that you don't think is a risk you can point it out and eh. If there is one among them that is really highly relevant to the decision of a municipality, then also point it out, but it could also be that they all are.

J: Yeah, you know.

S: If I have to scroll further than eh.

J: Yes, no. It's okay, I think for a moment you have to look at your definition of risk.

S: Okay.

J: Because eh as far as that's concerned it's eh. I don't always fully understand whether it's a risk or an objective or, eh, just a general subject with which something can be said.

S: Yes, like that. Because I've got it now yes maybe that's a bit too general as I had sent it in the preparation, let's have a look. Was that this one? Do you still see my screen?

J: Certainly.

S: And also what I select now or?

J: Eh no, not that.

S: No okay. Then I stick it in here.
This one was that.

J: Yes. That's fine. Look at that when you go through the list. Risk of discrimination, check. Definitely a risk. Eh legal, societal and ethical issues and privacy, eh check those are the risks you can associate with them, but those are mainly more the subjects. In other words, not a concrete risk, so to speak.

S: Yes.

J: Then you have privacy and data protection, eh those are subjects.

S: Yes, okay.

J: Eh by the way, my advice would be if you want to be just as pure, use the word data protection because the word privacy, from a legal and administrative point of view, does not exist.

S: Okay.

J: It is spoken language. But that is, eh.

S: Okay, because data protection is actually the data you already have, how do you protect it or not? Or does that also include how you collect it?

J: Eh that whole process and data protection is specifically about personal data. So, eh, in that respect it is, of course, about privacy, only the term 'data protection' is generally used more clearly, but eh.

S: Yes.

J: Eh. Trust between data sharing parties. Yes, I do not quite understand.

S: Yes, that has to do with the fact that the software, of course, comes from a supplier. The fact that they also have some influence on it.

J: Yes, so data then goes to a place where you might not want them to go or something.

S: Yes.

J: Or influence the data.

S: But maybe that's data protection too?

J: Yes. Technical issues. I can imagine. Um, I'm also trying to imagine that you have an environment where you would like to apply facial recognition. Absolute necessity, no discussion about the possibility and then the whole infrastructure breaks down. Yes, as a local authority you run a risk. Because, yes, you can, and that can have consequences if you fail to identify people whom you definitely do want to identify. That idea.

I don't have any examples, but that would be something I can imagine.

GDPR yes, that is, that is also about personal data, so that is also privacy.

S: Does that also have to do with the framework which, oh well, I have lost the name you just mentioned, the D....?

J: Yes. The GDPR is the European regulation eh for the protection of personal data. It came into force two years ago and is also directly applicable in the Netherlands. We use the word General Data Protection Regulation (AVG).

S: Yes.

J: It is used for the Dutch translation of GDPR and the abbreviation AVG. Eh and the obligation to carry out a DPIA on certain subjects stems from these regulations (2.11).

S: Okay yes, clear.

J: So this is the overarching law that provides the framework for the processing of personal data, certainly for municipalities, certainly for this context and certainly for facial recognition.

S: Yes.

J: [reading]

S: I think that is what you said about the chilling effect. That people are going to put on masks or behave differently, yes.

J: Yes, exactly, and you know, it's funny because that example was also featured in John Oliver's film. Eh he had an example from the United Kingdom where someone indeed put a cap on and a scarf in

front of his mouth, in front of his nose, so it was unrecognisable. Eh what is legally his full right, I think, but at the same time he was arrested by the police and fined 90 pounds. Because apparently that is not allowed and you have to walk around in that area in front of facial cameras recognisable. Yes, then that really is an example where John Oliver, for example, also asked the question of yes, that does not go much too far.

S: Yes.

J: And you should also take a look at that Brit's reaction, because it was absolutely furious.
Quality of the facial captures can affect performance and effectiveness' yes, that works both ways. If the quality is not good, it will result in “the municipality not reaching its objective”, but then you also have “mistakes that will have adverse effects on the citizen”.

S: Yes.

J: Accuracy, plastic surgery, non-intrusive....
Yes plastic surgery yes is that a risk? In my opinion, does everyone have the right to change their face?

S: Yes, no. Yes, perhaps it should be rephrased in such a way as to increase the risk of errors in the system, of course. If, for example, someone gets a different nose, that face no longer resembles who that person is.

J: Yes, this is a reasonable line of reasoning from the point of view of the objective I want to make a very recognisable, say, very good match between the person I have on camera and the person I want to match it with, the profile I want to match it with. And what are the risks of that not succeeding?

S: Yes.

J: That is more the risk for the user, for the municipality and not so much for the citizen.

S: Yes.

J: Speed, accuracy. Faulty decision-making Yes, we have already talked about that. Performance of the system.

S: Yes, it does make things difficult, doesn't it? In this piece, which I actually came up with, there are, let's say, very different levels. I have also tried to make it into groups or to see if you can make cups with different risks underneath. But anyway.

J: Yes, what you might be able to do is perhaps “start reasoning from the objectives” from the perspective of “the various stakeholders that are involved, including the data subjects” (1.6). So to put it another way, the categorisation is in fact the objective of the stakeholder. So you have, say, the stakeholder, those are the people who are being watched. Well, they have certain objectives because they want to protect their privacy. Eh, and you have, so to speak, the users of facial recognition.

S: Yes.

J: They again have their own objectives “which they wish to achieve through the application of facial recognition, and what are the risks which stand in the way of that objective?” (1.6). If you look at it, there may be one more category, but that just doesn't occur to me. I think it is possible to separate these two main points in broad terms.

S: Yes.

J: And that would, that might help you a bit to understand exactly what you're talking about.

S: Yes, because I think it is, because at first I thought I had to exclude it from the risks of the user, but it isn't, because if that risk exists, it is indirectly a risk for the municipality as well. So I was like, 'yes, that must also be transparent', so I thought, in fact, I wanted to keep it as broad as possible.

J: Yes. Yes, no, you know, in that respect, I have a little bit of an approach to privacy, so the interests of the citizen are very much in mind. Eh, but that does not mean that a municipality cannot have a very super legitimate objective to apply facial recognition in a public space and that absolutely nothing should stand in the way of this facial recognition being as effective as possible.

S: Yes.

J: I just find it difficult to figure out what those specific circumstances are. Eh look at the moment someone walks into the front door of the Dutch bank or eh very specific limited public or eh limited physical environments say, I can imagine something about that. Eh defence base, the Dutch bank, Jewish church in Amstelveen, I just mention something. There are also threats there. Eh I can imagine something about it, but at the moment it's really about a public environment as you know the market in Groningen or the Dam in Amsterdam. Yes, you have to come up with a very good story if you really want to apply facial recognition there. Because, as you know, this is in fact also a bit of a trade-off, at the moment you apply facial recognition to the Dam Square in Amsterdam, you are actually talking about a very large dragnet. Eh and I am going to see what comes out of it. Versus, yes I have “a very limited physical environment” that I want to secure and I am going to put “very specific emphasis on every person who walks in”. That's, yes, that's very specifically individualised and that “creates a better story for that limited environment” than applying a trawl net to Dam Square.

S: Yes, so that is actually it. Because what I'm hearing right now is the purpose and size of the area where you want to apply it. Are these decision points that you actually take into account even before you make a risk inventory?

J: Yes eh it is always a discussion of, but that is also a privacy discussion, eh the moment I apply facial recognition, do my interests as a municipality outweigh the interests of the person whose rights I am infringing? That is always the balancing of interests that has to take place. And if you do that in a very limited environment with a very specific purpose, with a very specific interest. Then it is easier to explain than when I say, for example, a dragnet eh and apply it to Dam Square in Amsterdam. You know you can actually apply the same discussion to Telekom data. Eh it has been customary for years that at the moment when we signal eh there is a police investigating a drug gang. We know that person A and B are involved and we know that person A is the leader. Then it is very easy to say we are tapping his phone.

S: That is allowed?

J: That is allowed because that is very specific, it is aimed at one person, no more data is collected than is necessary and there is simply a reason for it. It is very easy to demarcate. In recent years, there have also been various legislations which have said that we simply store all data for two or three years. Yes, that affects all of us, so everyone can see who has called who, for how long and so on. I am not a criminal and yet my data is collected. Yes then you have a much less good story, much less powerful story to explain to me why my data is collected.

S: Yes.

J: Yes I could possibly commit an eh murder the day after tomorrow. Yes hey good story.

S: Yes.

J: But yes. Then you get into that kind of discussions. Weigh, the public interest outweighs the benefits for the public interest that outweigh the individual interest of me as a person and the rights I have.

S: Yes. It often remains very philosophical, doesn't it? It is difficult to get specific risk points in that respect. At least I only get that feeling a little.

J: Yes, you know, these are also difficult decisions, because you know the view of the person, the minister and the head of the AIVD. They have a completely different perspective on the world and on the need for a legislative proposal of this kind because they do. They are right in the middle of it, they cannot tell us why they are submitting a legislative proposal because, yes, you know all the terrorist attacks they are stopping, in fact, they are secret. You do not know what has happened. Um, but that makes it very difficult for me to understand what the need is for such an invasion of my privacy. Eh and it is fair to say that the head of the AIVD that would never be the person who let it be said is also an advocate of privacy. Otherwise, he would probably never have become head of the AIVD.

S: No.

J: So, you know, it's also often very individual depending on what is actually your perspective on privacy. And some people find that very interesting, is it really just know your fundamental right of every individual eh a human right and treat it very principled. While someone else would say yes I don't find privacy very interesting, privacy is long dead. Um, you know this is just interesting for me and we should just continue with this because I think it is a good idea point.

S: Yes.

J: And everything in between from disinterest to eh so yes that makes this kind of discussion very difficult.

S: Yes. Eh well it is eleven o'clock so I just want to put an end to it. There is a lot more to tell when I hear that, but I think that we have gained a good insight into the risks that are there and I have to categorise them myself. I think that I can make a nice overview of it with the additions you have made.

J: Is good.

S: I don't know, do you still have any additions or additions yourself?

J: Eh yes is more of a suggestion. It might be useful if you could talk to Person X for an hour.

S: Yes, yes, I sent her an e-mail.

J: Yes, because she really has done a concrete assignment for the city X as well. In any case on camera surveillance. Not on facial recognition, but at least on camera surveillance, so I think he knows that perspective a bit better.

S: Yes, yes, interesting. Eh yes, and about the anonymity of this interview, of course. My eh thesis will of course be present at the University of Twente in any case. Eh what can we agree on? How, for example, will I name you in my report as an eh expert on privacy at PwC, or may I just mention your name or eh.

J: Yes, you can mention my name. That does not matter to me.

S: No, but you will also be able to see how I work it out. That is of course the most interesting thing.

J: I would like that.

S: Yes. No, but anyway I'll keep you informed about that.
Eh and yes, I also hope that if I do come up with questions after all, because yes, I still have to specify something, as you might notice, it is still quite open. I hope that I will be able to approach you again when necessary.

J: Yes, come on up.

S: Yes, well, thank you very much.

J: I will be on holiday for three weeks from 27 July, so in that period I won't be available for a while.

S: Yes okay. Good to know, thank you.

J: I hope it will help you a bit.

S: Yes I hope so too. I'll take that as a starting point. In any case, thank you very much.

J: You're welcome and I'm curious to read the final version, so if that's all right, you know what you're getting at.

S: Yes, certainly. Yes we are going to do that.

J: Okay hey good luck.

S: Yes thank you.

J: Bye.

S: Bye.

Additional information sent before the interview:

Potential risks:

I see it particularly in the area of Data protection (privacy): data collection that a person was at location Y at time T, during period Z and there XYZ activities.

Sub-risks:

- The data collection is stolen: this can have significant consequences for the person in question which cannot be undone (e.g. the consequences of the data breach at Ashley Madison). “Municipalities are vulnerable because they do not always have mature security”, enough examples of hacks.
- Scope creep: the “data collection is used for purposes for which it was not originally collected”. Again, this can have negative consequences for the person in question. Example: the Tax and Customs Administration that uses the database that the National Parking Register claims (meant to check that you have paid to park somewhere and pay financially between e.g. Yellowbrick and the municipality), but which is used to check that lease drivers do not unduly use their business lease car privately (because for income tax purposes they only use it for business purposes).
- Public opinion: “there is a lot of resistance to facial recognition in the Netherlands on the basis of principle”. “If there is a meaningful application, then as a municipality you have to communicate this very well in terms of stakeholders' expectations, otherwise it” (5.5) blows up in your face in terms of public opinion and politics.
- Risk of 'false positives': A person (Piet) is incorrectly 'recognised' as another person (Klaas). If Klaas is a criminal and is wanted, it can happen repeatedly that Pete is wrongfully arrested. This is particularly a risk depending on how the algorithm is trained, see: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

The problem is that an algorithm is as good as training, and if the Chinese government trains its algorithm with people of Asian origin, it will be good at recognising Asian people, but not in other demographics. In particular, false positives occur in other demographics.

Analyse the risks together. The Use Cases are largely the same across the municipalities, which is why the analysis of the risks will also be very similar. Do it once with the best professionals involved, then everyone can make use of it.

DPIA. There are also a lot of whitepapers by renowned (scientific) institutes that provide insights into the risks of facial recognition.

Expert Privacy and Security (2)
Name: Frank Versleijen
Organization: PwC
Date: 13-07-2020

F: Let me see.

S: Would you like to introduce each other first?

F: Yes, certainly. Go ahead. Yes, good. Shall I start? Or do you want to?

S: Yes, no, go ahead.

F: Eh Frank Versleijen. I am eh director within the same group as person X eh within PCPS. And I've been with Pwc for thirteen years now and before that I worked as a software developer, among other things, but also as a team leader of a helpdesk at a software supplier. I've also been doing that for five years. So I have also a bit of a picture of what's going on on the other side of the table. Eh and in terms of profile. I am actually completely eh focused on the public sector and in particular IT audit services and everything that goes with them. I also have a specific focus and specialism on security and privacy. So, for example, we also do company X audits, well, that's the part I take the lead in. I have quite a few large municipal clients as a customer. Including the municipality X, but also X, X, eh X, and X as well as some smaller municipalities, so I understand that person X sent you to me as well.

S: Yes okay.

F: Eh yes I live in Noord-Limburg. That is the other side of the Netherlands. Together with my wife and two children, a son of nine and a daughter of seven. They will all be a year older next month. And eh yes that. They've been at home for a while now, but that's no different than it is with you.

S: No, exactly.

F: Yes. Hey and who are you? And I'm also curious to know how you get to this subject, so eh.

S: Yes. Yes I am eh Stephanie. I am studying at the University of Twente, the Master of Business Administration. I do the double degree programme there, so I also studied for a year in Berlin at the technical university. Now, how do I get to this subject. I myself was interested in the subject of smart cities. So I wanted to know more about it. And then I ended up with a professor who was very curious about what image recognition actually meant for an application or perhaps even risks for smart city development. And then I had to focus further and ended up with facial recognition because I also thought that, yes, there has actually been a lot of discussion about this recently. As far as, of course, Corona is concerned, for example, or eh. In some places it is already being applied and in other places it is not. What is actually allowed and what is not allowed, so that there was also quite a grey area around this topic and I think that's what I found interesting, the question if there is already a kind of overview of the risks involved. So that is how I came to this topic. But also, eh yes, in the study programmes that I did and the subjects that I followed, yes, the technical aspects always appealed to me because I'm just very curious about everything that changes so quickly and also how people react to it, so eh yes, I find it very interesting. Yes.

F: Well then you have chosen a good subject because there is quite a bit of eh to do here and also quite a lot of reticence. And eh yes well let's see how I can eh how we can talk about this and eh how I can help you.

S: Yes. Yes exactly. Eh I can first eh, maybe for your imagination, a little bit more shape the definitions in my research so that we are both on the same page.

F: Seems good to me.

S: Um, because the main question in my research is actually how to design a risk assessment framework for municipalities to support in making a decision on the use of facial recognition for public safety. Well then, facial recognition in my research is the application of that software and its use, everything that goes with it. Um, but a more important definition, I think, is the risk. I see that as an aspect that has a negative impact on the municipality itself, either directly or for society, which is therefore an indirect risk for the municipality. As a result of the decision to apply facial recognition. So that is somewhat the framework in which I have specified it. Yes.

And eh well then actually the first question eh what is your experience with facial recognition and then in work experience, knowledge but also what is your view on it.

F: Yes. Well I haven't done many specific assignments around this subject eh. I did discuss this with clients, including municipalities. And then the issues immediately comes up, eh, is that “there is quite a lot of reluctance” (5.2) to use this new technique. And somewhere I do understand this reticence. Look a lot of municipalities are really in the competition to make the municipality as pleasant as possible. And of course there are quite a few factors such as crime, but there is also unrest. I already told you that the city X is one of my clients. There is always something to do there. Whether it's football matches or just neighbourhoods where it's just a bit less pleasant to live, where there's a lot of youth hanging around and all that. But the only important issue I think about the use of technology is the ignorant factor. So “how is it for me as a citizen in my municipality, how do I know what the municipality does with the information that is collected and how is my privacy guaranteed, but also how do we avoid me being falsely accused” (5.3). One example is the increasing use of video images and facial recognition at football matches, which means that people are being banned from stadiums. The past few years since that happened, you sometimes see that there is jurisprudence on the subject and so on. The fact that this is based on images that are, after all, too grainy and have been matched, either by software or by people, to “the wrong person”, and yes, that this is also an issue. And yes, most municipalities really do have a problem with that, where it initially seemed like a very good idea and there are quite a few suppliers who were willing to put all their efforts into this. Because it makes life a lot easier based on that philosophy. It makes life a lot easier based on that philosophy. Creates some hesitance, which I can sense in the conversations I have and also when I think about it myself, that yes. “Surely, here in the Netherlands, we are quite fond of our freedom and also of our privacy” (5.3), and people think that this becomes a bit complicated the moment such techniques are used, but especially when they want to understand why. “The fact that there is a great deal of uncertainty about facial recognition” (5.3) and that is not something that only happens in local authorities, by the way. I also read an article this weekend about columns where, in fact, for the Corona, eh organization X I thought, that is in your region, eh hospitals you should perhaps visit. Those eh use information pillars where you have to show your identity card to do a check if you are you, do you live near here, are you registered with us in the hospital, so you come here with a good reason, or not. And then the whole discussion about the hospital's eh statement was about yes we do not store this data, we only use it for the check now to determine whether you are here for a good reason or not. But only if you use facial recognition, for example, to monitor what is happening on the street? “What is being done with the data and there is no clear goal for using it”? (1.1) I find this discussion very interesting myself, but I also think that if there is no very clear goal, so what really matters, for example, is the specific tracing of certain people, that it then becomes very difficult to apply it.

S: Yes. Okay. And do you see any improvement in the future? Or, difficult?

F: Well me. What I eh. What I think is that at the moment “there is a very good reason for using” (1.2) that you “would make it possible to better justify” (1.2) the use of facial recognition. Suppose there really is a lot of crime in a neighbourhood and you would ask everyone, do you think it would be good if we put up camera's and then just point out the people who making trouble here. The moment you live in such a neighbourhood and this. Well then I think you are more inclined to agree with that.

S:Yes.

F: However, a lot of public street life is already being filmed, and there is a lot more being filmed and there is already a lot more, eh wifi tracking, eh you name it all, without us knowing it we already give away a lot of our privacy. And even the moment you walk into the Bijenkorf and have the Bijenkorf app, they follow you through the shop or can, in theory. They have somewhat come back to this. So I am very afraid that “the more people become conscious of the technical possibilities, the more reticent the response will be”. And we are simply not as a Dutch state as kingdom or as a municipality there is not as much authority as in China, for example, where simply yes this is a non-discussion there because this just happens.

S: Yes.

F: You are just required ID we are going to scan your face and you want a new ID now, we make a 3D scan and you are followed everywhere and you don't want it.

S: Yes.

F: I find that very interesting whether “our societal vision on the topic” would change, for example, in five years' time we will reach a point where either “the state is able to impose it on us”or whether there is a yes. “Imagine this pandemic spreads, just to take an example, and it gets so bad that we just want to be able to detect people infected with the virus very quickly”. Does that change our social view of this issue, then? I do not know.

S: No. Yes, and then perhaps it also has to do with the fact that everyone here also has their own opinion, so maybe you also get divided groups in this or yes.

F: Absolutely. Hey look what we are proud of as Dutch people is eh “freedom of belief”, “freedom of expression”, and this and that's why you certainly see around privacy issues that it is sometimes complicated in the Netherlands. I think the electronic patient file is a very good example. Where there are really just two tough camps, one of which says when I enter a hospital and I have something please. Here are my medical data and another one says yes but de facto I don't want that. Even if that would result in me, or my child would not be helped properly, from a privacy point of view. So I think that's “the main driver or risk perceived by society”. Personally, I think information security is also a very relevant issue. So suppose I am willing to have my face and my movements tracked for the safety of the neighbourhood, with the aim of catching criminals, but at the moment the data is registered and “is not safely stored, then” what happens to it? Because eh yeah suppose a “malicious person” knows exactly what time I come home every day, “in order to recognize what my pattern” looks like, that once a month I am away for a weekend at my holiday home, I just mention something. That is of course very valuable information for people who want to “break into my house or want to

know something". And I think that that aspect is still a bit, uh, "underexposed in the public debate on facial recognition".

S: Yes, perhaps this is also a sort of second step, because if you, your users, are not in a position to allow it in the first place, then the next step is, of course, data security.

F: Yes. You see and that is not so much facial recognition eh, but you do see more and more use of smart techniques and cameras. City X, for example, has had scanning cars for the parking lot for years. That is generally accepted because they know that those cars that scan license plates.

S: Yes.

F: However, there is also a piece of security behind it. Part of it is also privacy. Eh parking apps the same, they know exactly where you were. You can't go anywhere almost anonymously anymore. But yes.

S: Yes.

F: To what extent does that still apply at a time when we all have smart cars connected to the wifi? So.

S: Yes.

F: We're talking a lot about facial recognition now, but I think "it is almost to avoid sharing more and more information" (2.2) and I'm very much in the race of "how can I now partly determine myself what happens to my data, but also what remains registered and what not, and for what purpose?" (2.2).

S: Yes.

F: And I think that this can hardly be made transparent in the current situation. So that you very much like the municipality says we are going to use this eh Stephanie we are going to film your street with this purpose that is very difficult to prove. And so on the one hand this may require a very good consideration at the front, but on the other hand it also requires something at the back. There is also "a question of trust attached to" this, and how can I, "as a local authority", "demonstrate to" (1.1) my "citizens" or to society or to the supervisor "that they do not store the data or only store it for a specific purpose" and remove it again after a certain time? (1.1) Can I obtain a certificate of this? How do I do that?

S: Yes. And then, oh this is something else, by the way, but a certificate like that would that be something that PwC, for example, could check and then supply?

F: Yes, that would be possible, but the question is, what is the level of "transparency" of that and is it "measurable"? So "a certificate" (4.2) of this kind only makes sense if there is a very good framework with which the organisation itself can demonstrate, this demonstrability.

S: Yes.

F: And eh yes, suppose I want to do facial recognition with Chinese software where I don't even know where the data is going, you know.

S: Yes.

F: But precisely the logic for facial recognition is of course the intellectual property of that supplier and if you, it only becomes very interesting if you can make connections. Between data and different sources at the moment that they detect a face that not only checks, this person now has a stadium ban, but he also has something else on his mind. Assuming for a moment that you want to use it to increase the safety of citizens, then you want to consult several systems, but yes.

S: Yes, you should be able to show that openly.

F: Yes, you should be able to do that very openly and what happens when the software is in doubt? Do I fall into the right box or will I then be taken more, eh, as a potential risk?

S: Yes.

F: And that's the example of people being banned from stadiums because on the basis of video images that she looks like someone, she is seen doing something that is not allowed. Eh yeah, how does that work? “Can someone object against” to this at the moment you can prove that I wasn't in the stadium at all, I don't know. Eh somewhere else, so there is also a risk in terms of jurisprudence.

S: Yes.

F: So “what rights may the municipality or I, as a citizen, derive from the images on which someone is recognised”?

S: Yes, those are all still there. Yeah, that's not set up, of course, I hadn't thought about that at all. But of course if you get a fine now, you can also claim it, so as far as that's concerned, maybe it would be yes....

F: Yes.

S: Okay.

F: Yes I compare it with a speed camera. In Germany you always get a picture of the speed camera. They also cut it from the front so you can always see if you are driving, but you do have an opportunity to object.

S: Yes.

F: Hey if you say yes but that's not me because that was someone else driving my car or eh. Well there is no facial recognition possibility yet, but now imagine that the government has a 3D, hey they have a picture of me, because that is my ID and they have software running and that says yes sir we just see that it was you. So we have compared your ID with the photo of the speed camera and we have established beyond of a doubt that it was you.

S: Yes.

F: You may not object (...) or we reject the objection.

S: Yes, but of course the software has to be 100%, otherwise you get yes.....

F: Well, you know, that's where it gets interesting for me. What purpose will you use the software for, what rights will you derive from it and is it sufficient evidence in this case, for example, to “attribute an offence to somebody”?

S: Yes.

F: We are simply talking about a traffic fine, but you can also imagine that it goes much further than that. If we stay on the safety playing field for a while, there can also be hundreds of other different applications for facial recognition, because in the hospital, as I see it, it is actually a positive thing. We only want people who have something to look for here, we within the hospital want to....

S: Yes.

F: ...have. But the role of the municipality, which is actually about the public yes space, is very interesting.

S: Yes.

F: And the smarter cities are going to become and the more information is going to be exchanged. I think the more interesting, but also the more scary it gets.

S: Yes. Yes, you can keep track of it all.

F: Yes that and eh I don't know if you are going to speak or have spoken to Gertjan Baars?

S: Yes. Yes. I did.

F: As far as smart cities are concerned, he is the one who knows the most about the technical possibilities and has helped several municipalities with this and eh yes.

S: Yes, yes. No and eh I have, I actually started my research with literature. I did a systematic literature search and in combination with eh facial recognition, public safety and risks. This resulted in a number of articles, from which I actually filtered which risks they refer to. And I have made an overview of these and I would like to show them to you in order to gain a little inspiration, but also for you to indicate this I do not see this as a risk or as very relevant to this issue. So I am going to share my screen.

F: Yes.

S: Let's see, can you already see something? Oh very small.

F: Yes I can see something.

S: Shall I zoom in for a moment?

F: No I can put it here on my bigger screen eh so that goes well.

S: Okay. Well I have made the authors a bit smaller because I found that a bit less interesting for now. But eh on the right are the different risks that are actually mentioned.

F: Yes.

S: And eh yes, maybe you can scan through them and indicate which ones you think are highly relevant for municipalities, especially to be taken into account when making a decision.

F: Yes, of course you know the first one. There have been quite a few incidents in recent years "concerning ethnic profiling". Certainly in America you have to "take a closer look", I think more research has been done there, even if it has been demonstrated that facial recognition software, for example, contained a bias.

S: Yes.

F: Eh so that. Well, we have already discussed a number of them. Legal, social, ethical and now privacy. What I see so far is actually eh almost all yes I think applies but also eh. Yes, yes privacy in personation. Yes, that is also true. That quality of the facial captures can affect performance and effectiveness. The better or worse it is able to recognise my face, the more likely it is that I will be falsely accused. Just to draw a goal.

S: Yes, yes. Yes, and I am also aware that this must of course be grouped together because it is also at different levels in terms of risk, because how a face is stored and then used is, of course, more on the software side, so that is, yes, that is an indirect risk for the municipality, of course.

F: Yes, but I would also just classify more around eh. Under the block of information security and "speed" which is the very last, or at least the last of this page. I think that is much more of a "functional requirement".

S: Yes, it is precisely this functional requirement that you place with a "supplier"?

F: Yes, there is a risk in that, but only if it means that you are not "able to act fast enough". That is the same with how accurate the system is. That results in risks. Well, you may not be able to achieve your functional objectives and that is, for example, preventing terrorism just as much. Prevention of crime, eh. Yes, but you could also frame it positively. I would like to know which people are using this public space and how old they are and where they live. So I have a park in the city. Just as an example and I would use facial recognition software to see which people from the city are now in that park.

S: Yes.

F: So that I can, eh in my area development, take better account of which facilities should be in that park. Now we have nothing to do with crime, but I'm going to scan everyone. Yeah.

S: Let's see, I still have one more page. That's also the last one.

F: Yes, that bias decision making. I think that accuracy is the main theme and I see it several times. Eh I would translate it as in the risk of what are the potential consequences if the software is not accurate. And eh precisely because there are potentially municipalities that want to use it precisely around the theme of safety. Or something attached to this that is actually the result of this, but bias decision making, then there is also an algorithm, there are often algorithms attached to it that determine what people are walking around in this park at the moment who potentially commit a criminal act or are going to do something, but you do want the software to behave as well as possible.

S: Yes.

F: But yes, and it has actually already been proven that quite a lot of mistakes are being made in this respect.

S: Okay. Yes, yes, of course, it is not for no reason that it comes up so often.

F: No.

S: Yes. Okay.

F: Yes so this is recognisable.

S: Yes. Good then I'm going to close it again. Um yes, I found this piece difficult, let’s say, because from scientific research they want you to build on literature. So I ...

F: Yes.

S: ... I wanted to find an overview of the risks that have actually already been described and there are more practical studies in which it really is described.

F: Yes. I was also looking for you and then you see, for example, that IBM, one of the largest software suppliers after all, just stopped working with facial recognition on 9 June.

S: Yes.

F: The reason for this is ethnic profiling. Well, we all know what is happening in America at the moment and they are not really saying that they don't believe in the technology or it is not possible, but this is promoting ethnic profiling.

S: Yes, yes and even more. I spoke to Jan Visser last week, I don't know if you know him too, but he ...

F: Yes, I know him too.

S: ... he also pointed out to me a video of, oh well, I don't remember the name, but it did indeed emerge that Microsoft has also stopped and Google has also stopped, so in my opinion it is quite a big deal, yes.

F: Yes.

S: And further on. Imagine that you yourself would get a case from the municipality. How would you recommend eh to map out the risks?

F: Well, I would like to "get a very clear idea of the purpose for which they would like to use this software for" (1.2), because I think that is quite decisive for "what risks are involved" (1.2) and what I would find very important is not only the "internal risks" (2.8) that they identify, but also the internal risks that it doesn't cost too much money, "does it deliver the right" (2.8) results. The municipality is there primarily for the citizen. So I think that "the perspective of the citizen/society is important" (2.8) on how they view the use of this type of software. I would like to see that point of view "reflected very specifically, because it is also community money that is spent" (3.6).

S: Yes.

F: So why, what is the benefit, "which risks are there", the municipality "should be transparent about that", and anyone involved should actually be able to explain this to the citizen.

S: Yes, and would there be a certain working method for this? How would it be possible to map out this yes or, eh, what kind of action could a municipality take?

F: Yes, I find that difficult. Of course you could also discuss this with "discussion in a kind of focus group or a survey to figure out how people think about" (3.3) it. I can imagine that "if there is a certain generic goal in which the citizen does not directly see the benefits" (1.1), it just becomes a difficult story.

S: Yes.

F: But as soon as you indicate in the problem area, we want to put up cameras and facial recognition to bring crime to a lower level eh yes. Then I do expect you to get more support for this and some people just don't think from such a principled point of view.

S: Yes.

F: I do think there is "not one good method" there, just because of the "sensitivity of the topic". Whether it is about ethnic profiling or insecurity or the privacy aspect, yes, "there should be a really thorough analysis" that I think covers as much, "cover the risks as broadly as possible in order to ensure that data is not misused" (3.1), [unintelligible].

S: Oh you're dropping out a bit.

F: Well look, do you hear me?

S: I think I can do it again, yes. It was very bad indeed.

F: Yes indeed it was very bad yes.

S: I didn't get anything either.

F: Yes, that's because of the facial recognition software that is running.

S: Yes, I think so, they just turned it on. No, they didn't.

F: Yes, yes. Eh I don't know what you just got from it, but eh what I said anyway. What I would recommend is to do an eh a risk analysis as broad as possible. Precisely for all the reasons I have just described. I'm sorry about my printer eh.

S: It's haunting you.

F: Yes. Eh but just to get that clear.

S: Yes. I have also taken a closer look at the Artificial Intelligence view in general from a piece of literature research, because eh governance frameworks have already been created on that level. And that's actually where the layer above the risk inventory is also divided into three groups by one professor. This also indicates your focus on society, ethics and then law and regulation. The fact that, from these three groups, you are actually going to make an overall picture of what the risks are, what the benefits are, eh in that way, yes. And then perhaps this will indeed involve bringing together a group of people, eh, yes, who might also be able to put the citizen's perspective a little more forward, eh.

F: Well, I guess so. And, eh, you just say as the thread running through the various studies. For sure ethics and privacy and legislation. You can actually expect this to be looked at carefully enough, because it complies with the law. “On the other hand, you see that the legislation is not always clear about what is permitted and what is not” (2.16).

S: OK, yes. Yes, because Jan Visser also gave a framework. That there is, um, a legal one. Yes, I don't know whether it is a framework, but a legal framework in any case, which municipalities have to comply with for data security or eh. Security of information.

F: Well. I think he is talking about the BIO.

S: Could be. The DPIA or so. Something like that?

F: Yes, that's a Data Privacy Impact Assessment.

S: Oh yeah.

F: Um, but in general “a municipality has to comply with the baseline information security government (BIO)” (2.14).

S: Okay.

F: Let's have a look. That is this one. I put the link in the chat.

S: Yes.

F: And DPIA eh that is a yes a privacy impact assessment. And you can also find another example, and I will now put you through that on the website of the personal data authority. That is actually if you have a new software package or, for example, an algorithm or, in this case, facial recognition software. In that case, you actually have to do a privacy impact assessment and then you just look at the risks.

S: Yes.

F: Well, the supervisor has also drawn up a list of all the things you have to think about, and I do not have it in such detail at the moment, but I can also imagine that there is something here that offers you a starting point.

S: yes, those two, eh, yes, that baseline and that personal data authority are two frameworks that are in any case probably also necessary in order to be able to assess, eh, how risky it actually is.

F: Yes, and the baseline that says these are actually “the rules of the game, which we have agreed on with each other around information security” (2.14), and a DPIA writes much more ... Look, “the law is decisive for a municipality and they must comply with the GDPR” (AVG). General Regulation for Data Protection.

S: Yes.

F: And eh “the DPIA is an important instrument to start” (2.13) with at the forefront of a new development, suppose we go use facial recognition software to decrease crime in problem areas. Does that solution now comply with the “legal framework of the GDPR (AVG)” (2.13) and that often starts with a Data Privacy Impact Assessment.

S: Yes.

F: Is privacy already sufficiently guaranteed in our design?

S: Okay. Yes. And, uh, we were just talking about what you, uh, would do to inventory or identify risks. And that is actually quite a broad approach. It is possible to take the three subjects and then to brainstorm with different stakeholders in order to arrive at a kind of risk overview and, as you can see, would that probably be different for each context?

F: Eh yes, that is possible. Just depending on which part you are looking at. Look at the “technical requirements are not so important to society” (3.6) of course, but how certain data is handled, how long it is stored and what is permissible. I can just imagine that eh that they think something of that.

S: Yes. Yes. And, uh, are there any risk assessment tools that you would, uh, recommend that you include them in such a decision?

F: Well, I don't really know a tool or something. I think the requirements in the law and these are in line with what Jan says eh I think specifically for municipalities eh relevant matters. Eh but I yes I can't really just mention a certain risk analysis. Precisely because the risks here and, in particular, how topical a number of issues are, I think that, looking at this ethnic and “ethical aspects”, today's yes really is a different situation than it was five years ago.

S: Yes. Yes, these developments mean that it may not even be applicable any more. That is possible, of course. Yes.

F: Yes or yes, but under very strict conditions and I think that's a bit of the “balancing act for municipalities” (5.4), which I think is also in that Volkskrant article. Everyone is a bit hesitant, this one is watching.

S: Yes.

F: Everyone calls it “a pilot” (5.4) project. “Politically now one dares to say something” (5.4), because that's something. What a municipality, of course, certainly important decisions are taken by the council. Of course, there is politics behind that too.

S: Yes.

F: Councillors are elected, if you are unlucky someone stays for four years, so “who is going to be decisive when there are no clear guidelines from the national government”. “Municipalities have a lot of autonomy as long as they follow the guidelines of the law” (5.4).

S: Yes.

F: Obviously. And to all the guidelines that exist for municipalities to make their own decisions, only yes, is someone really going to say ‘we are going to use facial recognition eh for subject x, y, z here’. I honestly don't know.

S: No. Well, because do you know if there is a municipality that has gone through such a process to see if they can apply facial recognition or maybe even do it? No?

F: Not within the organisations I come across. As far as I know.

S: No, because I think. I can't quite figure it out yet, so to speak. You can see some things on Google and, for example, at city X I read that face comparison is used. But that's a good thing, that's also just recognition of course, but yes. It is an eh.

F: Yes, but then the comparison with a certain list or with a specific purpose. Then it becomes more vague. Yes. And I also think that at the moment this is really a very broad or big plan, you often find that there will be documents in the public domain or that it will be discussed somewhere. In the council meeting, well then it's put on an agenda and you can often find it there. But that actually says something. If there is very little to be found about it, then it is also a question of to what extent people are taking this very seriously in various municipalities, for example.

S: Yes.

F: I think that is disappointing.

S: Yes. Yes I have eh I have one contact now with the municipality of city X and they have made a decision and that decision was no, but eh that could also be a case. I would like to talk to the people who made the decision about what steps you went through and what made you not go for it in the end?

F: Yes.

S: Well and Jan also indicated that I could get in touch with the VNG if they might have a more complete picture of this and I also saw that on 1 July there had been an event about a similar discussion. So I was actually rather disappointed with that. I wish I would have looked at that site a week earlier, but yes. So yes.

F: Yes.

S: But that part because at first I thought I would interview experts, then I would interview different municipalities and compare them with each other, but the municipality part is still quite difficult. Actually. Yes, I've had two reactions. One from the municipality of city X, they weren't actually working on it at all, and city X was, but yes, I don't know the people I'm in contact with either, so that doesn't run very smoothly, but at least there is contact.

F: Okay. Yes I understand a little better now of course what you are looking for. So I can also check if I can use my existing contacts. That's not going to be this week anymore, but if the situation is there, I'll ask you about that as well.

S: Yes, because I am also thinking. I also have someone at company X. That's a startup or was a startup in city X. Eh of facial recognition software and I'm also thinking about maybe inviting them to join such a focus group. That you also get a kind of perspective from the people who actually develop the software themselves. What is actually their vision of how it could be applied or where do they actually see the pitfalls and if you would then bring together such a municipality and perhaps the developer himself and an expert and enter into a discussion like that, then I expect interesting things might come out.

F: Yes.

S: But yes.

F: Yes.

S: And what is your reaction to that? Those three target groups do you think could give a representative picture?

F: Yes, representative is always the question, of course, but at least you have three different perspectives.

S: Yes.

F: Eh where you can, of course, set the interests against each other. You can imagine a bit how that supplier will sit in the competition. I think that the municipality is still a bit more doubtful and reserved, and yes, people themselves, that can go in all directions.

S: Yes. Yes may be, but I think it is also a challenge for me to structure something like this. Because yes, I mean my knowledge of facial recognition also is there because I am reading a lot now, but actually I don't have any real knowledge or experience with it, so yes, I find that rather difficult. I still have to think about that.

F: Yes.

S: Yes. Eh yes I actually got a pretty good picture of eh yes the knowledge you have and also your vision on the two parts actually 'what are the risks' and 'how can you maybe map it out' yes what are the important interests in such an issue eh. I don't know, do you have any further additions at the moment or?

F: No, I don't have it yet. I will also go through your document eh. We have gone a bit off the main topic, but I think we have hit the most important core.

S: Yes yes. Because my questionnaire consisted of two parts. Especially a lot of those risks, which ones are there and eh yeah part two was very much how can I map those risks at a municipality and how can you possibly assess them. So I think that we touched a lot of subjects.

F: I think so too.

S: Yes.

F: No, I'll check if I'm, uh, still meeting with people from the municipality in the near future. Or at least in the area who would know something about this if they were working on it. Not in the short term.

S: Okay. No yes I also have something like I just want to do my research well and suppose that now this holiday period is just becoming too difficult for having further interviews then that focus group interview will come a while later yes.

F: Yes I think that maybe if you want to have some people together, be it interactive or this, that yes is now a risk you run eh.

S: Yes exactly. I was also aware of this, because I have e-mailed a number of municipalities, but they haven't really responded to that yet.

F: No, some of them are also going eh, that's going to be quiet now.

S: Yes, yes and perhaps also the subject that is so much discussion about now that it makes it extra difficult for me.

F: Yeah, maybe they are thinking about, so let's not start with that.

S: No, exactly, yes. So eh well and with regard to the anonymity of this interview. Eh is also a small point which we should perhaps discuss. Well, it will in any case be public within PwC and then for my university, which will of course have to check it. But to what extent do you think it is a problem that I would, for example, mention your name or your position or how far, um...

F: Eh you can mention my name. I don't think that's such a problem. Eh well hey my statements are my statements.

S: Yes.

F: On a personal note, I think it is important that you state that explicitly. That it does not express the opinion of PwC.

S: Yes, exactly.

F: And eh for the rest, it's fine to use my name then.

S: Yes, and I'll send you the documents as well. It might also be interesting to finally see what I've done with them.

F: Sure, sure, yes.

S: Well, well then eh.

F: He can you move forward with this?

S: Yes yes. I've had at least two nice interviews now, so at least I can build on that again.

F: Well, that's good. Well then I wish you all the best and if there is anything else you can send me an email.

S: Yes. I will do that.

F: Then you will get a reaction from me. Yes?

S: Thank you very much!

F: Okay. My regards. Bye.

S: Bye.

Expert Municipality - AI researcher (3)
Name: Maarten Sukel
Organization: Municipality of Amsterdam
Date: 21-07-2020

S: That might be eh convenient.

M: Yes. Yes of course I have already received something, but I'm only now reading through the instruction. I was a bit busy, but eh.

S: Oh that's all right.

M: So feel free to introduce yourself and eh I'll read myself.

S: Yes. That's absolutely fine. I am Stephanie Roorda. I am doing the Master of Business Administration at the University of Twente. I'm doing the double degree programme so I also studied the Innovation Management Master in Berlin for a year. Eh and for both programmes I now have to do this graduation research. And I'm doing it in collaboration with PwC and, if the situation had been normal, I would have been working at the Zwolle office, but unfortunately I was only able to do that for a week. Eh yes, it is for the Risk Assurance department so for that reason the risk topic and eh yes, I think that's a bit about me. Perhaps you could introduce yourself?

M: Yes, certainly. Maarten Sukel AI lead at the City of Amsterdam, so I'm actually working on all the innovations around AI for the entire city. I am also doing a PhD in Computer Science at the UvA. So actually I'm working on those two. So I think I have something to say about this subject.

S: Yes. That was my expectation as well.

M: Yes, yes. Okay yes, that was it in short.

S: Yeah well I'll start with the first questions, what is your experience with facial recognition in terms of work experience, but also knowledge and yes what is your view on this.

M: Eh so technically I have never developed it myself, but I do know how it works. Pretty well. Eh yes, my knowledge and vision is very much in line with the vision of the city council, which means that in city X, yes or “there need to be really compelling reasons to do it”, but as a municipality we don't do it in principle. Eh, “that actually stems from the coalition agreement of 2018”. Eh “that every citizen should be able to move around the city without being spied on”, and city X is a free city. Eh and the registration of faces is not in line with that. And that is also my “personal opinion on this subject”, so that is a good thing. Yes, it is.

S: Yes okay. And then it might be interesting to know if you also participated in the decision-making process yourself? Has it really been a point of discussion whether we should use face recognition or was it more about camera surveillance?

M: Yes, no, that is indeed more general about camera surveillance, and since facial recognition is actually a further form of this, it is of course ultimately decided on an official basis from now on, so we are certainly not going to do that at all. Eh yes, of course, there is a translation of the political choice into practical implementation. As far as facial recognition is concerned, we are, of course,

conducting research into its ethical side, would it be desirable. And sometimes, for example in the case of pilot projects with “partners, at the arena, with the stewards who work there”, who were able to get in more quickly with facial recognition. So we do carry out experiments in this area, because we very much believe that, yes, you have “to be able to understand the technology and be able to continue to pass judgment on it”, and so what I am actually saying about us not applying it at all is not true. But we do not apply it in public spaces. In other words, we do apply it in that form.

S: Yes.

M: So that's also more of a question of ensuring that in the event of another new coalition agreement, and we actually need to translate it in such a way that we also have the technical expertise, or at least the experience, to make the right choice. Yes.

S: Yes, exactly. And do you also have a kind of overview of the risks that exist, that you have, ready at that moment?

M: Eh yes, that is the colleague I was referring to, person X, who did indeed carry out an extensive study, which was also a graduation thesis study, eh on facial recognition in public space. That is why I made that link, which seemed to me to be a very interesting one. What we have done, above all, is to use a, if you could call it like that, a 'talking plate'. So we held presentations to see what the reactions were to this, what does the citizen think of this, eh well and also “internally within the organisation” (3.7), of course. In addition, we may have seen that we still go outside with it from now on, this is our position on, as a municipality, facial recognition. Only that, of course, is a bit awkward. It is indeed a risky subject, eh, it is not one where you very quickly find a politician who would “want to give a clear opinion or wants to speak out” because it is after all a somewhat more controversial subject, yes.

S: OK, yes. After all, what, for example, were the decisive risks or disadvantages, eh, that the municipality actually said yes, we are not going to do this.

M: Eh yes, that is mainly due to the restrictions on personal freedoms that are associated with it. Eh possibly seen. I think that that is actually the main consideration so that the municipal council has decided in favour of simply not wanting that in that respect, so then yes, and since we know what is linked to it, eh, that choice has been made.

S: Yes, okay, and eh if you now specifically think of facial recognition from your own experience. What kind of risks would you add to that if you were to discuss it?

M: Eh nou very practical, legal risks. “When using facial recognition, you are working with personal data” (2.9), eh. In my opinion, that is not quite my cup of tea; the legislation surrounding the fact that it concerns biometric information about someone, eh is that, that “is withing the privacy regulations” (2.9). There is, therefore, a very great risk that you will simply do something illegal and, as a government, you simply should not do that. Nobody should, but certainly not us. That is a very practical risk. Yes, it is more ideological if you can follow someone at that level automatically. Yes, of course, you can go very far in controlling people in that area, in their behaviour. So you should not want that either.

S: No.

M: At least here in the city we don't want that.

S: No, exactly, eh because you have done some kind of risk identification, if I understand it that way.

M: Uhu.

S: Eh by giving those presentations, for example, eh.

M: Yes, yes.

S: Did it actually come out, for example, to the stakeholder who was defending the citizen eh, let's say, eh, what certain risks are on their part?

M: Can I not tell you no, then I really have to have eh person X yes.

S: Yes, I also sent her a message, so I did.

M: No answer yet, is there?

S: No, not yet.

M: No.

S: But well I also thought it is of course holiday period so it is also eh...

M: Yes. Yes. Yes, you have to have her soon because I know she will be working somewhere else soon so that's eh.

S: Oh okay.

M: I, maybe I will send her an email.

S: Oh that's nice, thank you. Um, because can you also tell us a bit more about the identification of risks at the time? In what form?

M: So I wasn't personally involved. I'm a bit broader in AI and actually the moment we say, we don't do facial recognition, eh then it's already done for me. Then I won't be doing a lot of R&D or setting up projects. We do, by the way, we do follow crowds of people, for example. So we actually do mass monitoring, but that's more about crowd counting and movement flows. Eh where there is a big difference between recognition and detection. So we don't recognise the person, but we do detect them, so that's, to me, the eh, the limit of how far we can go. Which is also a nice reference, I think, we have a manifesto on how we want to work with data in general. That is the Tada manifesto. It actually says…, and it has also been signed by the municipal council, so you can also see in it what these considerations are ... Yes, the reasons for this. Eh then you just see that the values in there, they are almost diametrically opposed to facial recognition, eh you can find more on tada.city.

S: But is the data manifest? Or how?

M: It is a manifesto about how to work with the data eh so that is. It is called the Tada manifesto. And that is signed yes by the Waag eh, and eh our alderman.

S: Yes, I don't quite understand the beginning.

M: The Tada. Dates flipped, yes I don't know why it is actually called but eh yes.

S: Oh. Dates reversed. Okay.
Yeah, I can look it up.

M: Yes, you have a source.

S: Yes.

M: Eh there is no chat or yes. Oh there is.

S: Yes.

M: Look I can do that.

S: Yes, because I did indeed have previous conversations, I have eh. Yes, I divided up my research and I questioned different perspectives about the risks, so then I have a number of experts on cyber security, but also on privacy and, well, I try to find out what their vision is, or what has come out of it, how do they do it now? Eh I have someone from a company who has developed facial recognition himself. Well then I have indeed heard from those experts that there is a DPIA. Which a municipality must indeed comply with, and also a certain framework from the VNG, but also certain agreements that have been made to that end...

M: There are undoubtedly a great many agreements and manifestos of this kind, and eh yes. Yes, there are.

S: Yes, because I understand that your job is to come up with ideas and investigate what can be done and then the follow up, the decision-making process is continued by the municipality.

M: Yes, of course I do inform, but my position is also based on R&D and technical knowledge. So it's more about the development of the ideas than about the actual decisions. In the end, the decisions o be taken are again with the municipal council in this area.

S: Yes, because are you a sort of, is it a separate group, the AI eh, because there was also some sort of lab or something, right? I have read something, but.

M: Yes, that is indeed the lab. We are part of the key technology office, so they work together a lot, but that's another department. So that's eh.

S: Yes.

M: I don't know how relevant the municipal structures are here, but that's, uh, quite complex, but that's a bit of the same angle, so that's more the, yes, the development side than the. You also have the CiO office. That is a bit more the policy side. Eh, I could also make a link with that if that is of interest to you. They will tell you more about the choice not to do anything with it.

S: Okay, yes, that is interesting.

M: But person X is actually the beautiful link there.

S: Yes. Who knows? Yes, that would be a good thing because other questions that I did want to address, more from the municipal perspective are: how do you assess the risk and say this weighs heavily or not for us and how does the process actually go? I notice that this is something that lies more with the municipality than with, say, this AI lab, yes.

M: Yes, it really is also just a political choice. I think that is a very important one to not do that, but of course there is an enormous translation of the official mill between them and I think that is what you find interesting.

S: Yes.

M: Yes, I can tell you the outcome, but unfortunately not the exact processes involved.

S: But perhaps it would be interesting from your own perspective if you were to do research from now on, eh in this case facial recognition. Would that be something for our AI lab to introduce to the municipality? Would you do some kind of risk assessment or assessment yourself?

M: Eh no, actually with us it is. Eh we would like to do things that are “scalable and not too expensive” and with which we can really “make a difference in the city” (2.6), so “one of the strict criteria’s” (2.7) is that we don't do anything with personal data because as soon as you start working with personal data as a government, you actually get a concerned with lawyers, who are perhaps even more expensive than our developers. “These juridical costs would probably be more expensive than our own development costs” (2.7), and that actually already makes the decision a no. There are also many things that are not sensitive, with which we can really make a difference. In other words, we need to put more capacity into this. So that is actually a very simple consideration of why you should start with that when there are also a lot of options for which this is not a problem at all. So I think that was a very practical consideration.

S: Yes, the added value simply does not eh outweighs the effort you actually have to put in and how much it will cost.

M: Yes, yes, yes.

S: Okay. Yes. Yes, and does it also have to do with the fact that perhaps the risks are still very unclear? Suppose it would be very bite-sized.

M: Yes, look. I think the risks are clear to me, you get out of the camera who someone is, eh yes, the risk is already in there, so what you can do with that is, of course, endless links that you can make. So

the risks are not very unclear to me, eh well you will of course also know the reference at the English stage. I do not entirely agree with that article, but what a bit of an anecdote that goes around, eh, of the one hundred criminals that they caught ninety from them were none, was that person not at all. Eh because, for example, they were selected on the basis of skin colour, so that sort of thing. So these kinds of systems are also very sensitive to those more biases. So yes that the risks are not clear, I actually don't think so. I think they are very clear. There are still problems on all sides with these systems.

S: Yes.

M: Less often than, you hear that, but the fact that something like this happens 1% of the time is really too often already. So even if it happens one in five thousand times, let's just say, that would already be very bad. Eh and especially if you were to roll it out on a large scale, eh, so I think the risks are clear to me. So eh.

S: Yes, they may differ from situation to situation, because facial recognition is used in certain places, for example?

M: Yes, yes, so it is purely for the sake of having this kind of discussion about evaluating it as well, is it really correct, those assumptions that we have made here? I mean if you base everything on a blog that you've seen on the internet, yes eh so sometimes thorough research is done, but it's always good to keep verifying things. Eh so that's why I think you should never throw things completely overboard. Um, but yes, we are certainly aware that these are actually the problem areas and sometimes it is also good to do something, eh, to go public, well, we do this and ultimately we do get a very clear response about no we do not want this. Eh then at least you know that your eh that people agree with you so that is also an advantage of it.

S: Yes, because in eh in what situation, for example, is it applied?

M: I know that eh with the police, so you could see that as a partner of ours. Eh they have, I think, done it in places where, for example, there was a threat to a certain person to a certain address. That they hung up cameras there which were actually constantly scanning for that person. Eh well, that is, they store a profile of someone and then they look at eh is that person around here and then the alarm bells go off of course, but they are not saving anyone who passes by with mass surveillance, they look purely from someone they are already looking for, so I think that the police are allowed to track someone down. Um, I think that that is definitely not my area of expertise, but it is allowed, so that is less massive.

S: Yes.

M: Then they are just really looking for one person then I think they have the authority to do that. Eh I see you nodding in agreement, what is eh.

S: Yes, of course I have spoken to more people and I notice that if a goal is very specific or an area is very specific, then it becomes easier or it can be applied because it is…

M: Yes, well, that's what I think and it's often also, what I know from other projects, for placing a camera is that we “need to have purpose limitation” (1.3). They can't just go and do something like that if a camera is already there, but I can imagine if the police put a camera in such a temporary place

eh that it becomes easier for them to do experiments with it because they say it's okay this camera is here and it's only there for a week and that's with the purpose of keeping this person away from here. Eh that, then I think that is possible. If they have a good technical story about this, we are not registering everyone who passes by here, because that is not allowed. Eh.

S: Yes.

M: So that all sounds very logical to me that is what I see happening yes.

S: Yes and for example at such a stadium that you detect everyone who comes in and see who it is, but well you choose yourself to go inside so of course you have.

M: Yes, those are the people who work there, so they will have agreed to that happening. You can go in faster if we can scan your face once. So there is also a 'yes' to this.

S: Yes exactly. Yes.

M: I am sending an e-mail to person X at the same time.

S: Oh, thank you.

M: Not that you think what is he doing.

S: Yes, I also have the feeling. I also had a conversation with someone at a company who also indicated that there was a colleague who had indeed helped with a risk framework for camera surveillance at a Dutch municipality. It could be that they worked together.

M: That would undoubtedly have been with our department. It is our job to get involved in this. Eh so that's “CTO”, “CIO” (1.7) in that corner.

S: Yes.

M: Yes a lot of colleagues are now or eh going to the ministry to help with all the eh Corona technology or are now on holiday. Eh just a bit of an unfortunate period. You can notice it on me too. I was hard to eh to get a response from, I think.

S: Well good. The rest of the municipalities are even more difficult.
But yeah, I was expecting it too. Look if I don't manage to find the right information now, then I'll just have to wait until September. It's no different than that.

M: Yes. And because it's summer now, that's usually the case.

S: Yes exactly yes everyone.

M: Especially people who are involved in the decision-making process, because they leave when the politicians are gone as well.

S: Yes.

M: Because otherwise you get calls on your holiday, so you're just unhappy.

S: Yes.

M: If I just give it to you as information, you know it's because of that.

S: Yes.

M: Okay, at least I sent that e-mail. I don't know if you have any other questions that you think I can answer?

S: Yes, I do have a bit of research focus, actually. What I have tried to do is, uh, to make an inventory of the risks from literature, so I did a systematic review of the literature, but what struck me a bit was that, in my opinion, many risks are not described in science, but more in practical sources. So, that this is not really described in literature. So yes, I was curious to find out whether you might have an insight into this, or points of considerations.

M: Yes, my research will focus more on its technical operation. Eh that is more my scope to eh and they will not talk very much about the ethical risks. Not enough in any case.

S: No.

M: Eh and a lot of this research is being done in eh China. I also have a nice story, I once had a professor who came to Amsterdam. That's a Chinese professor and someone asked a question of yes what about eh privacy? For a very long time he was looking surprised, then someone translated it into Chinese, it really was three full sentences, eh of what the question was and then he said 'that is not our “top priority” here'. So yes.

S: No yes.

M: So I think he didn't know the whole concept of privacy.

S: No. That is particular.

M: Eh and “this is the setting where the research is being done” after this so that's an eh yes that says a lot to me.

S: Yes, and of course it goes very quickly because they don't keep that privacy in sight, so yeah.

M: Yes. Yes.

S: That's a bit of a thing, yes.

M: Yes if their R&D teams already make other considerations. I think that if you don't have all the legal costs, and if at the same time you get the assignment from us, we want to keep a close eye on our people, then facial recognition is a very good thing to focus on.

S: Yes.

M: And you can also see that developments there are also going much faster in this area.

S: Yes, exactly. No, but I found a professor in Germany who writes in public administration, who has an eh risk governance for Artificial Intelligence and that includes the three layers of ethical, technical and also the law and regulations. And beneath that is also the risk assessment that they actually want you to do with the various stakeholders. So, yes, my idea is to get a kind of risk overview, which in turn can add value. Yes.

M: Yes, yes. A bit from the literature to the practical side. I think it's a tricky one here, eh.

S: Yes.

M: You have the policy documents in the literature and then more the technical developments that are going very quick and they are also difficult to keep up with. So eh.

S: Yes yes and also everything that happens during because I started in March and last month everyone stopped doing research into facial recognition. So eh there is news popping up all over the place. Yes it is.

M: Yes.

S: But does also make it interesting for me again of course so yes.

M: Yes, we do “face detection”, but that's actually just to “remove faces”, so I always like that. The first step of facial recognition is also where the face is in an image, eh we do that, but just to throw away those pixels because we don't need them. So up to that point I also keep track of technical developments. Eh beyond that is actually not relevant to me because I don't want to do anything with it anyway.

S: No, and is it detecting, this a person?

M: Well, you know you can count, of course. If you delete a face, you can also keep track of the number of times you erase a face, of course, so that's all there is to it.

S: Yes.

M: Um, but in principle we don't do anything with it because it feels a bit like looking at where people were. So that's not a good first start for a lot of projects. We have projects where we are working on something else. So in order to “prevent the data we store being used for other purposes in the future”, we are already throwing things away. So we are also actively working on this.

S: Yes, because that detection and erasure is already being used?

M: Yes, yes.

S: Yes, and how does the public respond to this?

M: Eh positive. That is, of course, yes, you can use the same techniques here. It is not the same as facial recognition, but its detection. Eh why? To guarantee privacy. That is also what I just wanted to say about yes AI is not just what can really ruin your privacy. It can also guarantee it. I mean a camera that instantly removes a face is better than a camera that does not. Eh or even the example if you have hundreds of cameras hanging around and someone is constantly looking at them, looking at the people. Eh what would you prefer, that a person does that or that some algorithm does that, that doesn't store anything. So it is, there are already more flavours possible than how it is sometimes put down. Yeah, that's more within the AI. Facial recognition itself is of course always the same as the recognition, so that's where you are already wrong in this area.

S: Yes.

M: What most people are afraid of.

S: Yes, because how would you yourself, if you had to do a project yourself to map out or assess the risks with a local authority they would like to use. What steps would you take?

M: I think I would eh yes “look for someone” from your profile, in terms of masters, and “make it an assignment to sort” (3.2) out. So I also think that somewhere in there with you that choice has been made as to whether it comes from yourself, but that is actually what we did with person X. I think that would be more of a step. If I do it myself then I know that this will never really be fully investigated because I don't have time for it. Um yes.

S: And how, for example, do you get an image of the citizen, how do you get that insight within the municipality? How do they take it with them?

M: Yes, that's actually eh. A bit like the historical political processes. Historical is not the right word, I think. Eh from the point of view of “the elections” (3.4), from the “point of view from the parties” and what is their point of view.

S: Yes.

M: Eh that is the biggest one. Eh, but also “being transparent about image recognition, where does it happen, organising meetings about it and see the reactions of” people (3.7). Eh yes that way I think, those are a bit the main ways.

S: Yes.

M: And of course we also keep an eye on the news. So that's eh yes.

S: Okay. I think I eh.

M: I am always short with interviews so eh.

S: Yes, you talk directly. Well, that's nice on the one hand. I still have to transcribe it all.

M: Okay, yes. Super.

S: But eh I do want to keep you, eh yes, do you have any further additions or tips maybe if you hear what I'm doing.

M: Eh no. Yes, I like your approach. You send a bit in advance so it is eh. Let's get the people. That is difficult now. Everything goes online as well. So that eh yes.

S: Yes. Well, I'm going to experience it and otherwise it will take a bit longer. I don't have any, well then it is like this and I cannot change it. Eh and finally a piece of anonymity or not eh may I use your name. What can we agree on?

M: Eh yes I would like to see it before you... I don't know if it will become public, but if things do become public, I'd rather be able to check it for correctness.

S: Yes, exactly. I think that if I were to get a green light at some point it would be good. Then you can choose at the University of Twente whether it is only visible to the university or it is public. Well, at PwC it will be. Eh I will indeed tune in so that you can just read it. Before it is going somewhere or being published

M: Yes, that's fine. No, but if you can find it, I'd like to see if it's correct, if I agree with it.

S: Yes, exactly.

M: Certainly with this subject in my role it is eh.

S: Yes. I think everyone in general. I notice that everyone says so, a lot of reticence and of course everyone finds something else. In the Netherlands everyone thinks the same way, so it is eh yes.

M: Yes, if it definitely says that I'm not going to do anything about it, then I'm happy.

S: Yes. I think you have clearly indicated that.

M: Yes, yes. Top.

S: No, well then thank you very much and eh for your help in getting in touch with me as well. And eh yes, if I do have any question or if I have something, I hope I can send you another message.

M: Yes, fine.

S: And eh yes, you will receive the thesis by the time it is finished.

M: Good. Good luck with it. Have a nice day.

S: Yes, thank you. Have a good day.

24-11-2020 message on LinkedIn:
"There is a variety of computer vision techniques, where we think there are a lot of opportunities, but we will avoid the use of facial recognition because of the mayor concerns about privacy".

Expert Facial recognition - researcher/ supplier (4)
Name: Tauseef Ali
Organization: Founder of 20Face + PhD research facial recognition
Date: 21-07-2020

S: Shall I introduce myself?

T: Yes sure.

S: Eh I am Stephanie Roorda. I am a student from the University of Twente, from the Master of Business Administration and eh I am working on my thesis about facial recognition within municipalities and I want to figure out what the risks are around that topic of area and if I can develop some risk framework about that. Eh and as you mentioned maybe Robin Effing is my first supervisor in this project. I think you know each other. Eh.

T: Yes.

S: Also, I am doing the internship at PwC in Zwolle at the risk assurance department. Yes that is a bit about me I think. Maybe you can also introduce.

T: Yes so eh I do the PhD in facial recognition from University of Twente. In 2014. Then I worked in Saxion University for one/two years. I worked in a company for one/two years eh and then I started 20Face and 20Face is a company mainly focussing at facial recognition for different applications. Like access control, ticketing, or in all houses providing convenience to people. We can recognize people, we can eh play different kind of personalized videos so different kinds of applications that we are working on in 20Face.

S: Okay.

T: We are almost three years old now, the company and eh with around 10 to 13 people working. Eh some working on software development and some project management. So, it is a mix of researchers on facial recognition.

S: Okay. Nice. And do you also have an area focussing on the public security applications?

T: Eh not really. We are privacy proof by metrics so we make sure that every project or every application that we do. It is privacy proof and eh will we take examples of like police surveillance or a CCTV camera's, those applications are still not privacy proof. They are scanning people and everybody is scanned. So we avoid those kind of controversial applications. Eh.

S: Ah okay.

T: If you look at our logo it says eh privacy proof by metrics so we make sure that eh privacy is the first point in every project or in every product that we deploy. So we have a platform where we ask

people to self-enrol, so “only if a person enrols himself or herself by a phone, then we recognize them” (2.4).

S: Ah okay.

T: So “the end user is given complete consent on” our “data and on the photo” (2.4).

S: Okay.

T: So “nobody else can enrol someone else” (2.4). That is why we ensure privacy of consumers.

S: Ah okay and do you maybe have municipalities as clients or?

T: Eh we are doing a kind of POC (Proof Of Concept) with Rotterdam Gemeente and eh they want to compare photos eh when someone comes in and they want to get a new passport for example or they want to get a new driver’s license. So the people at the city hall they manually look at the visitor and they look at the database photo and to see if the visitor is the actual, the authorized person for the application.

S: Ja.

T: Eh that is a human comparison of one-to-one comparison. So “the database photo and the visitor. And they want to build an app that can access the employees at gemeente too. So they can double check if the person who is getting the passport or getting the driver’s license is actually the authorized person”. So they can manually look at it, but they can also use app to double check.

S: Yes. So actually there are some eh situations where recognition is already used?

T: Yes. It is, there is a debate in research community that whether computer is better in facial recognition or whether human is better. So in some situation computer is better than human. It is for them to verify because make up for example or age or different hairstyle, it can change the appearance of face. So it is very useful then to double check with automated method.

S: Ja.

T: So it is currently used there. We have, we build an app, they are currently using it and they want to find out if it is really useful and if it is really accepted by people eh. I think it will run for a few months before we can start building the product.

S: Okay. And are there some kind of risks you identify before you can eh apply facial recognition? How does that process go?

T: Eh risks in terms of you mean privacy or data security?

S: Yes.

T: Yes there, so ehm. Data security is a big issue. Privacy is a big issue. And eh what we do is we build all kind of encryption methods in our platform. We have “a cloud based facial recognition solution”. And we are building “different kinds of encryption methods in” and one of them is homomorphic encryption for example. It is a kind of encryption method that we can use eh to encrypt data and when we don't decrypt it, the data stays encrypted and we can do a comparison of photo because and keeping them encrypted. A third party like our customer give their data to us, to 20Face. And if for some reason we are storing it in Google Cloud or Amazon cloud then we want to make sure

that the data is not visible by them. It “is only visible by us or by the clients”. So that is a risk that we try to manage when we store data at a third party cloud environment.

S: Yes and you as an eh as the supplier of facial recognition, you always have to store the data from the client? Is it always needed or?

T: Eh we do not store photos. We only store feature *rector* extracted from photo.
It is 512 numbers eh a range of numbers eh nobody can understand those numbers. They are extracted by our algorithms. The input through our technique, eh our algorithm, is a photo and then it extracts 512 numbers from the photo and those numbers are only meaningful for the algorithm.

S: Yes.

T: So we don't need to store the photos, the original photos. We only need to store the facial rector.

S: Yes.

T: “So that provides kind of security because even if someone breaches a platform, still they can't access original identities”.

S: Okay and from your own vision, the collaboration between municipalities in specific, eh. Do you also make an idea upfront about what you see as risks for that municipality or is that something which they really do on their own?

T: Eh you mean risk for them to store the data or?

S: Yes or to use it like they come up with we want to use facial recognition eh and but we want to have a base where we can decide on. How do we know what the risks are? Do you collaborate in that or?

T: Yes. That is, we have one project manager who is specialized in GDPR.

S: Ah okay.

T: And the privacy regulations and he is more experienced into applications where consumer data is really a key thing so closely collaborating with the gemeente Rotterdam and in other projects. He “looks at all the data flows in the system of the client and he also looks at our data flow and our cloud based environment. And he tries to manage that everything is very transparent to the end user and only the person who is authorized can get access to the data” (6.2).

S: Yes.

T: There are like three key things security of the data so there should be, nobody should be able to hack the system. That is the data security part and then transparency that everything happens to the data should be notified. Because the facial rector also belongs to the end user. So if it is accessed by any party or if it is modified or any oppression is performed then it should be notified. That is the transparency part of the process and then the end user should be given full control of the data. So he or she should be able to decide eh which party can access the data.

S: Ah okay. Yes. And based on your own vision if an municipality would start using facial recognition. Do you see yourself some risks, like in general if they would use it on for some purposes.

T: No I personally don't see any risks. It is more like we are being identified at the municipality. For example you and I go there eh if I have an appointment I can enter my data, I can enter my last name

and that chose okay to 15 pm I have an appointment at counter 15. So I am being identified at the counter. It is only, the facial recognition is only bringing convenience in that part. So if I am standing in front of that boot for example then I don't need to. If they use facial recognition, then I don't need to fill in data. I don't need to fill in my last name.

S: Yes.

T: It can be quicker. It can be more convenient. Eh. So it is more the party which is building the solution. They should be more careful in how the data is handled in the back end. And the GDPR things, “everything should be according to the GDPR and plus some more privacy concerns from end user” (2.10). If they address properly, then there is no harm in facial recognition.

S: Yes.

T: But some solutions like, so some solution like CCTV camera scanning or a police scanning everybody, that is a bit different. But using it in the gemeente I think it is completely, it is very useful and it can be built in a privacy proof way.

S: Yes and what is then the added risk in a CCTV situation instead of eh access or from passport in comparison. What is the difference what makes it more risky?

T: Eh because there is no consent, there is no permission from the end user from the CCTV camera application. It is scanning each and everybody eh people even don't know if they are being scanned or not. Eh but using it at gemeente then people know that there is facial recognition. They provide consent to use it. Eh so it is more asking permission from users whether they want to use facial recognition or not. If they give permission then it is fine.

S: Yes.

T: Like I use it on my phone eh, Samsung phone. They have facial recognition eh for me it is very convenient. I don't need to enter a pin code and when I start the phone, I can change the settings so I can choose if I want to use facial recognition or not. So if there is an option then it is very useful.

S: Yes. And would you also, as a supplier of facial recognition, advice the municipality in a way like, if they now would say we want to use is for CCTV eh would you then also be collaborating in that and say hé watch out there are some risks around this application or how does that work?

T: I really strongly advise or recommend to use it at the gemeente. It brings a lot of convenience. Eh facial recognition is coming, it is just a matter of time, five, ten years. Eh it is more giving people some time to adjust the new technology and giving experts some time to, to build proper regulations and proper design so that it is privacy proof, but it is coming and it's brings a lot of convenience like passwords, pin codes, eh people forget those things. But eh by facial recognition it is very convenient so I will definitely recommend it. It is being used in the city halls and other public offices.

S: Yes. Okay and is, can we maybe think of a way like, the risk framework I want to design, eh I want it to be supportive on the decision they can make like if they want to use facial recognition in that certain situation or not. So can we maybe brainstorm a bit about what would be risks or decision point they should take into consideration or how can they identify their risks in a certain situation? Do you have an idea about that?

T: Eh the risk in general for any application. The risks are as I mentioned, the data protection, or data security eh because if there is access by any unauthorized party, that is very, that gives a very bad feeling in any application. So it should be properly encrypted and ideally the photos should not be stored, so because algorithm does not require photos. They acquire facial rectors or feature points

from face. So that needs to identify certain feature points and only those points should be stored and then because they are not really meaningful for human so it is one extra layer of data security. Eh the, it should also be addressed that for example if gemeente is using it, then there should be a decision point. Can they access the photos, can they access the facial rectors? And what can they do with it. Only and only for that application we are working on multiple applications at the gemeente. Passport renewal or ID card renewal or address verifications, many of them.

S: Yes.

T: Then people should be given proper eh they should be given an option to choose from them. So it should not be really in force but it should be more as a convenient way of doing things. It is more like eh when we go to Albert Heijn and we pay, we need to pay by pin card. We can also just under 20 euros or something we just need to swap the card and then it is more convenient. So it is optionally maybe something, eh like facial recognition can be optionally in the beginning. And then with time 20 percent of people will start using it and then 30 percent people, then 50 percent people.

S: Yes.

T: I think that is the more gradual way of bringing it in and it also reduces the risk so because many people. They “are still afraid of using facial recognition” (5.2).

S: Yes. Is it because they, do you think. What do you think is the reason that people?

T: I think it is more trust or the privacy eh so *contagious* so people are still struggling with *contagious* I can imagine that some people there will also be reliable for bank permit or so. It is more a new technology needs some time. Like we *contagious* we have premium membership so people they use facial recognition access eh *contagious*. They don't need to print their ticket they can just walk in with facial recognition. And we give them the option who wants to use it. And then only 30/40 percent people wanted to use it.

S: Okay.

T: *contagious* So it is also like the *contagious*. It is very convenient and there is no harm in *contagious*.

S: So your connection is a bit bad. I don't know if you can check maybe?

T: Yes I will switch off the camera.

S: Ah that is maybe better. Yes. And what is your vision on that? Do you think that the trust will become more over time?

T: Yes I think it will be more and more with time it will be better and better because eh just recently the GDPR came in and people are a bit more comfortable now with the data protection regulation. Eh maybe with time there are more specific guidelines or by metrics. And now we are the company. We are providing privacy proof by metrics but there are many facial recognition companies who are just using it and they don't care if it is really GDPR proof or.

S: Yes then it is more the problem from the client? From their maybe?

T: Yes.

S: Okay. And how do you think that you, for example from my experience and that is not a lot but, there are not so many municipalities yet using facial recognition. Do you also think that will become better or how do you think it could be more promoted?

T: Yes I think it will be better after some time. I think or I hope because I am the builder of facial recognition technology so. Maybe I am not very unbiased but I think with time more and more applications will appear. Eh two years, three years, five years. We will see many more facial recognition based application.

S: Yes.

T: Whether at the gemeente or at supermarket or the parking lot. We will see many applications.

S: Okay. Because also I heard some few weeks ago that, I think, IBM, Google and Microsoft and maybe even more, I am not sure, that they stopped with research to facial recognition. Do you know what is the reason and how is your vision on that?

T: Yes so that is mainly the privacy part. So facial recognition if it is done eh in a. If privacy is not properly considered. Data security and privacy. Then it is eh "there is a big risk that many companies" doing it they "would be banned". Because from an end user point of view, it is really annoying if a company is putting software into CCTV cameras. Eh if a company is scanning every photo on Google and finding identities of those people. That is very annoying, it is not really a privacy. So that is "the main reason governments and big companies, are really not into this technology at the moment due to privacy".

S: Yes.

T: But for example Facebook and Google and eh. Facebook recently start working a lot on Morphic encryption and privacy reserve by metrics. So the only issue is the privacy. If it is properly addressed, then they will start again but at the moment there is some gap.

S: Okay. And that has, with what has that gap to do? Is it the person self, the user maybe or the person who is recognized, that the person has no influence on where the data goes or what is exactly the?

T: It is mainly both. It is like in the streets if people are being scanned and they are being matched with a blacklist of people or with mugshots from police. Those people each and everybody is scanned and they don't know if they are being scanned or not. 25:43
That is not really an application that should be used. Many big companies were focussing on that. So they were providing software to law enforcement agencies for eh security and investigations and there were some appeals and codes when they looked at the law. So the law will not allow police and those agencies to just scan each and everybody. So that was the main controversy around this facial recognition. But some applications can be very controlled like accessing for example in office building. If there are hundred employees in a building and they install facial recognition. They can properly control it. They can ask employees who wants to use facial recognition and they can ask, they can self-enrol in the system.

S: Yes.

T: So there are some applications which can be properly controlled.

S: Yes and is it then, how is it working then at the municipality if they want to identify if the person asking for a passport is really that person. Should the person standing at the reception also say, I am okay with you using facial recognition or?

T: Yes, yes. I think the concept should be there so there are for example three, five, six applications and they can choose okay they want to use facial recognition eh in these applications.

S: Okay and...

T: So “nobody should be recognized without their consent” (2.3).

S: Yes. Okay because if it is someone who tries to steal your identity then they can skan that person or is it then also that they have to ask them?

T: Sorry?

S: Or is it too in depth?

T: No let us think about the use case that gemeente Rotterdam has. They want to use eh facial recognition just for extra eh check. Just for a *contagious* check. So there is someone on the counter and she can look at the person face and this is the person, this is the passport and the photo they match each other. They can give them the passport but facial recognition is just one extra layer of verification.

S: Yes.

T: It is only verification. So one-to-one comparison and that is one way to do it. There can be other ways to do it so the person on a counter can ask the visitor five, six personal questions. So she can ask okay what is your data, what is your place of birth eh what is your... They have some three or four secret questions or something. So they can verify with other means.

S: Yes.

T: And then for example the post court. So asking these four, five questions is one way to do the second check or they can use facial recognition to do the second check. So there is also two-factor authentication like the digital ID eh when you log in you can do that with SMS. The second, the two-way authentication process but that can also be replaced with facial recognition for example.

S: Yes.

T: If people don't need to receive a SMS code on the phone and fill it in on the website.

S: Yes and may I ask like in this process of this case with the gemeente Rotterdam. Eh what kind of role do you as the supplier from the software have in this process. Like do you also brainstorm with them about how it would work or what would be struggling in the decision process or how far are you involved?

T: I am, I have a research background so I am the scientist by profession. Eh I am researcher working on algorithms and my main focus is to increase the accuracy of those algorithms and increase the speed of those algorithms. So I am doing more of the scientific work behind the technique. Then there is a CTO who is more commercial. He is also technical but he is more focused on product or solution. I am more focused on algorithms or techniques.

S: Yes.

T: And he is more focused on the commercial side. So the CTO is looking together with the gemeente Rotterdam to make sure that our solution can fit with their eh. And then we have a project manager

who is also a bit more specialized in GDPR and privacy regulations, data security. So “the CTO and the project manager, they are the key people who working closely with the municipality” (1.7).

S: Yes.

T: My role is mainly to design more and more accurate algorithms.

S: Yes. Okay. What I also did for my research is eh finding an overview of risks around facial recognition, focused on the public safety sector. So yes there is different applications within that field but it was my to focus my topic. Eh and out of that literature review, there came some risks which I wrote down and maybe we can go through that document so that we can check eh what kind of risks you say yes this is really something which is important in this situation from my perspective or maybe you see some risks which you think eh this is not a risk for this eh research.

T: Yes okay.

S: Yes okay then I will share my screen. Eh this one. Can you see it now?

T: Yes yes.

S: I will make it a bit bigger. So it is not categorized yet or something but maybe you can point out some if you see like this is not really something I would say is a risk at the moment or maybe something which is really relevant for yes the case or for the municipalities?

T: Yes. So the first one is risk of discrimination, race, ethnicity. Eh yes it is more eh. It is not really the risk of discrimination but eh some algorithm in facial recognition are a bit more accurate with Caucasian people and some are a bit more accurate with Asian people.

S: Oh yes.

T: Because they are being based on the training data. So the developer of facial recognition should be more careful to balance out the training data. Because nowadays machine learning is the main approach for facial recognition. So there is imbalanced training data into that algorithm. It can be a bit biased for. It can be more accurate with recognizing Caucasian people and a less, a bit less accurate in recognizing black people. So the “design of the algorithm should be more careful”.

S: Okay. So that is maybe then something municipalities can ask you like how.

T: Yes,yes. That is when we design algorithm. We test it on different kind of datasets.

S: Yes.

T: So we make sure that those datasets have black people, Asian people, Caucasian people to really make sure that the algorithm is equally performing well on all ethnicities.

S: Yes. Shall I scroll down a bit?

T: Then this is legal, social, data protection, trust between data sharing parties, technical issues. Yes these are the main issues like there is also trust factor. If “the solution is not provided by one party” then they should really work together to see “where the data is stored” and “who is the owner of the data and what kind of operations can be performed” by one party and by other party. So “all these things should be properly addressed”.

S: Yes.

T: Data protection is a big issue in almost every application. So not only facial recognition but any application.

S: Okay.

T: Proper data encryption mechanisms and it “should be protected from hackers”. So those issues should be addressed.

S: Yes. Is it maybe Artificial Intelligence also in general?

T: Yes. Considering GDPR guideline it is very important. So every company eh specializing by metrics. They should really have one person, at least one person eh really expert in GDPR and data regulations. Otherwise, the software developers or researchers, they don't know eh these things. They are only building software. So there should be someone who is specialized. Like data protection officer or privacy officer.

S: Oh yes. Sorry?

T: That is kind of a new role that is being introduced in companies nowadays.

S: Yes.

T: The privacy or data protection officer.

S: Yes is that also the person you speak to at the gemeente Rotterdam?

T: Eh it is also our project manager who is the data protection officer.

S: Yes.

T: Security and privacy related. In categories. Yes this is, surveillance cameras is not really the application that eh should be done. It is, we as a company we started as simply facial recognition company and with time, with a lot of things that came up. We learned that the only way we can move forward is to be privacy proof.

S: Yes.

T: So over three years time we changed our strategy. And we discovered that only in a feasible way we can move forward is to really be privacy proof. We explicitly say no to many projects and many applications.

S: Okay.

T: If we see that they are not really privacy proof then we don't do them.

S: Yes because would surveillance in a certain area and then with facial recognition would still not be privacy proof? Or?

T: Eh surveillance is more like eh you want to pick up someone from the crowd and that is yes, for law enforcement agencies very useful but eh there are a lot of privacy concerns around that.

S: Yes.

T: Yes that is anti-spoofing we call it. Someone can wear a mask.

S: Yes.

T: Of an authorized person to get access to a building or to spoof, to deceive the system.

S: Yes.

T: That is a risk factor but eh we in our software we can detect many kinds of spoofing attacks.

S: Okay.

T: Like if someone is “showing a picture to the camera”. Or eh “playing a video of an authorized person in front of the camera”. “Those attacks can be detected easily”.

S: Okay.

T: But “building a personalized customized mask of an authorized person, that is a different kind of attack and there you need 3D camera to really find out” if it is a face with mask of without mask.

S: Yes and maybe also in the applications where it is applied now, the facial recognition, maybe it also not really eh possible for a person to put on a mask, like at the counter of an municipality and you put on a mask then someone would see it, yes.

T: Yes, yes. So at least it is not a “risk factor for the municipality”.

S: Which one sorry?

T: So the mask risk is not really a risk factor for that kind of application.

S: No, okay. Yes.

T: Yes accuracy is very high nowadays. Like we have one false positive in a million comparisons. So that means if we do one million comparisons, there is “a chance that one of” them “will be inaccurate”. So it “is becoming very high”, accuracy.

S: Yes. Wauw.

T: Yes plastic surgery it is also one eh corner case we are... “It is possible that the system is deceived because of the plastic surgery”.

S: Yes that it would maybe make a mistake, because then yes.

T: Yes. The speed is also very high so it is almost real time nowadays.

S: Okay.

T: People can just walk in and they can recognize. The accuracy, cost of the system, reliability. Yes so reliability is depending on the accuracy.

S: Yes.

T: The accuracy is high. It is, “there can be multiple checks as well, so instead of one photo. The camera can capture three”, five, six, ten photos and then it can make sure that it can do a second, third, fourth check before giving a decision. So that will make it “a bit more reliable”.

S: Yes.

T: Yes so these are challenges like “lighting conditions, or exposure, under exposure” of the camera eh “distance from the camera, different angle of the face”, eh “partly excluded faces”.

S: And that is maybe also eh has this also to do with accuracy again? Can you say it is under the umbrella of?

T: Yes. Eh “people wearing sunglasses” or scar. All of them are under accuracy.

S: Yes.

T: Yes when “light is projected from behind”. That is very bad lighting condition. That is also under the umbrella of accuracy.

S: Yes.

T: Technical issue angle, yes angle is also the pose. The “quality of the camera”.

S: Yes.

T: If it is very. Sometimes there is “motion blur when we want to detect and track people when they are walking and they walk very fast”. Then with the camera there is not good quality, there is some motion blur in the photo.

S: Yes.

T: “But that can also be removed”.

S: And also maybe in the applications you do now? Is it an issue if sometimes the picture is not from the good angle because if the person has to say you can do it on me, then you can make another picture for example before going in? Or?

T: Mostly it's angle 45, 40 degrees of angle is no problem, but if it is a completely profile photo like 90 degrees, that makes an issue. But still a small angle is not making any issue.

S: Okay.

T: Our software can recognize people from a small part so eh like if the face is visible 40 percent that is also enough. Eh the moment we are doing a project recognizing people while they are wearing Corona masks. We can still recognize people if they are wearing masks so they mouth and nose is covered. Eh only with eyebrows and forehead we can recognize people.

S: Okay. Yes this is also the last one already I think, yes.

T: Yes so ethical issues, they are also related to the privacy and GDPR.

S: Yes. It was also hard for me to find these risks really from literature base because I think there are a lot of sources more from the practical side and where is talked about, but that is not really ehm an overview yet or an yes.

T: Yes, yes. It is still, there is still this debate going on how it can be well addressed. Eh there should be some well regulated guidelines.

S: Yes.

T: “GDPR is a good step” and that is already making it clearer how data should be handled. “But now there should be more guidelines” (2.18).

S: Yes. And then I will stop sharing now. And do you think eh more guidelines then, because GDPR is more on law, should there be more guidelines on the ethical side or the how do you think that would, what kind of form would that have?

T: Yes I think “with time there will be standard applications appearing”(2.1). Eh like using it at the gemeente and using it at supermarkets and using it at for example for payments, online payments. So there will be like 3, 4, 5, 10 standard applications.

S: Yes.

T: And should be possibly “developed guidelines for each of those applications” (2.1) so any country, any supermarket wants to deploy it, then they have available a guidelines “from government organizations”(2.1).

S: Yes.

T: I think something like that might appear in the future.

S: So probably it is more we have those, these applications for facial recognition and then you already know what kind of risks are around that so that is not an issue anymore and only when you want to create a new application field, then it should first be tested again, something like that?

T: Yes, yes, yes.

S: Okay, yes. Really interesting to hear your view also about the, yes, this topic.
Is there something you can recommend to me or you want to add or?

T: Eh no it is very useful what you are doing eh so there was a professor at Leiden University, I think.

S: Yes.

T: She also did some work for facial recognition acceptance and guidelines and she submitted the report to tweede kamer.

S: Ah okay.

T: She was doing it for the government.

S: Yes.

T: Eh and I had an interview with her as well.

S: Okay.

T: And then she submitted the report to national assembly or.

S: Was it around the end of 2019, can that be?

T: Eh let me check.

S: Yes I saw something towards the government about mainly about privacy I think indeed that there was a report about that.

T: I can send you the report. I think it is somewhere. So I will email it to you.

S: Yes thank you that would be nice.

T: Because she did some work on it so maybe it is useful that you also eh if you want you can have a chat with her and.

S: Yes. That would be really nice.

T: Because I think she was doing very similar to what you are doing.

S: Okay.

T: But she was doing it for the government and she gets some assignment from the government, a funded project to research on this topic and give recommendation to the government and she did that and she has interviewed us, 20Face.

S: Okay. Nice I would really like to...

T: So I will forward it to you.

S: Yes thank you that would be really nice. And eh yes also at last it will be good to talk about the anonymity of the, of this interview. Can I mention your name in my thesis or how, what can we arrange about that?

T: Yes. Yes you can mention yes.

S: Yes and I will also eh send my thesis to you so you can check what is in there, what you said and eh before it goes online or something. I think that is good.

T: Okay that is good.

S: Yes okay.
Then yes, this were my questions for now. I really want to thank you for your nice insides and eh.

T: Thanks.

S: Yes I hope that if I...

T: If you come with any other questions you can also email me. So I will.

S: Yes that is what I wanted to ask if there comes something up then I maybe can ask something again.

T: Yes. Sure.

S: Yes then I wish you have a nice day.

T: Thanks you too. Bye bye.

S: Thank you, bye.

T: Bye.

Appendix III Description of the coding process

Unstructured coding
The coding process started with unstructured coding. This resulted in the ‘usage of facial recognition’, ‘privacy’, ‘data protection, ‘accuracy’, ‘legal’, ‘reluctance’, ‘transparency’, ‘trust’, ‘permission’, ‘goal’, ‘scope’, ‘decision making’, ‘risk identification’ and ‘vision’.

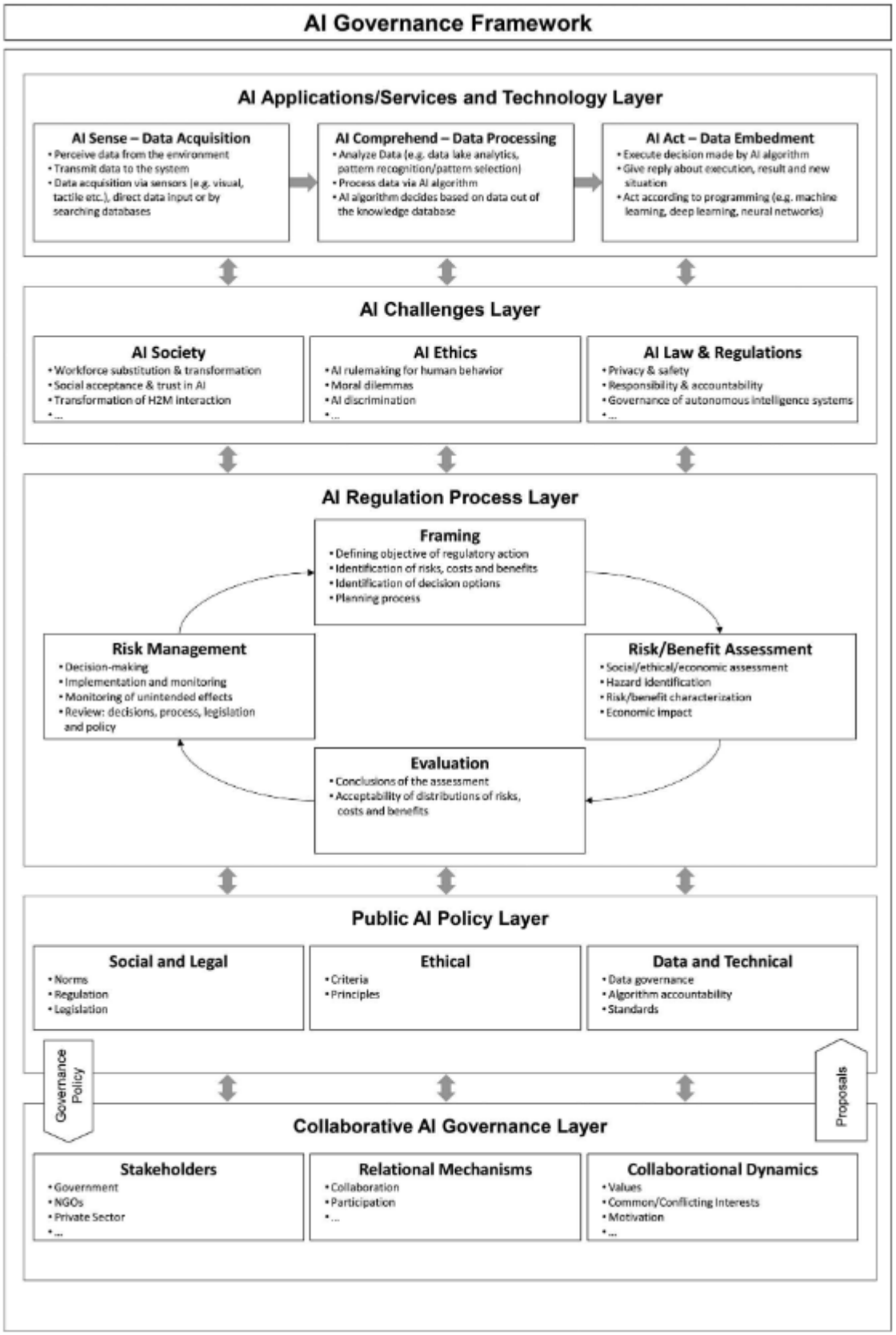
Categorising
There is decided to describe the codes ‘transparency’ and ‘trust’ together in one paragraph because the effect of being transparent might create trust (J. Visser, T. Ali & F. Versleijen).

Then, ‘goal’ and ‘scope’ are joined as one code ‘applicability’. This has been done because of the respondents talking about this goal, purpose and scope as something which should be present to make facial recognition in some case applicable.

Next, ‘decision making’ and ‘risk identification’ are addressed together in one paragraph. The reason for that is that risk identification seems to be a part of decision making and therefore the two overlap each other.

Structured coding
In the following coding process, the results from literature and the results displayed in chapter 4 are further categorized based on the phases from Madzou and Louradour (2020), ‘define’, ‘design’, ‘assess’ and ‘validate’. For the important information left there are added two extra paragraphs, the ‘pre-implementation’ and ‘transparency, integration and communication’.

Appendix IV The AI Governance Framework



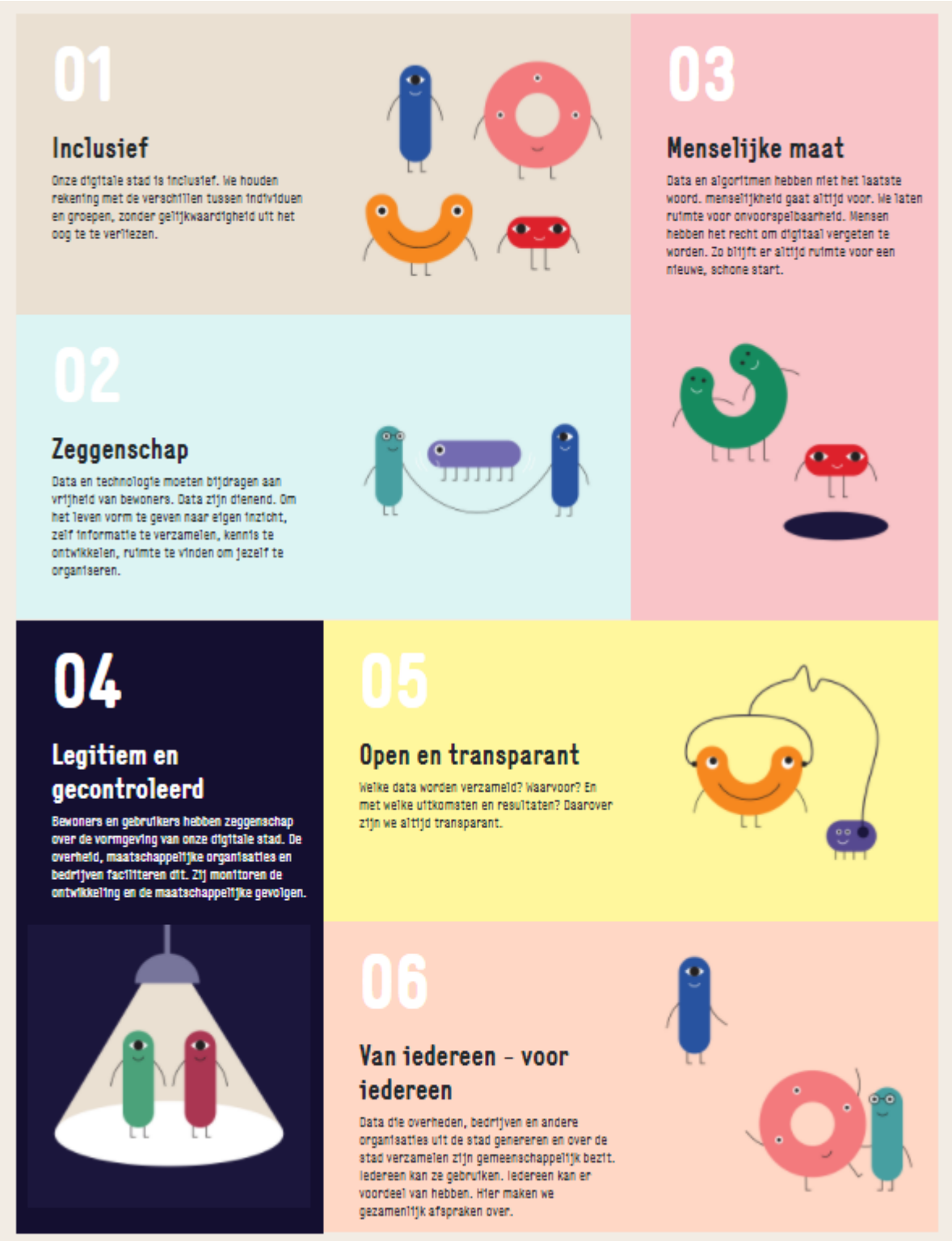
(Wirtz, et al., 2020)

Appendix V Literature output risk governance

Risk Governance aspect	**Citation literature**
Define	FR.1: The concern of disproportional usage (Varley-Winter, 2020)
	FR. 2: Secondly, there is the level of trust in biometric technologies of which the importance is often misunderstood. Varley-Winter (2020) state that ethical regulators and practitioners from industry should reflect on inspiring trust and ensuring trustworthy governance processes.
	AI.1: Formulation of a common understanding of the problem and objectives for regulatory action (Wirtz, et al., 2020).
	FR.3: Define a set of principles for responsible usage of facial recognition containing risks like privacy, bias mitigation, the proportional use of the technology, accountability, consent, right to accessibility, children's rights and alternative options (Madzou, & Louradour, 2020).
	RG.1: the aim of capturing the variety of issues that the stakeholders involved associate with as a risk (Renn & Graham, 2006)
	RG.2: stakeholders, such as experts, policy-makers, the organization itself, stakeholders and the general public (Van Asselt & Renn, 2011)
	FR. 4: The stakeholders involved in this process are industry actors, policy makers, civil society representatives and academics.
	AI.2: A consensus-driven approach and collaboration, within the risk governance process, are subjects that recur frequently in literature (Butcher & Beridze, 2019; Wirtz, et al., 2020; European Union Agency for Fundamental Rights, 2020). There seems to be a high amount of agreement within literature about these subjects. Butcher and Beridze (2019) conclude that the required effective governance contains different stakeholders having critical roles on different levels of governance. Therefore, a combination of consensus-driven standards and technical tools is needed. This conclusion is supported by the statement of the European Union Agency for Fundamental Rights (2020) "working with new AI-driven technologies, which are not yet fully understood and where not much experience has yet been gathered, requires the involvement of all relevant stakeholders and experts from different disciplines" (p. 33), which also seems to indicate a consensus-driven approach. Following, this consensus-driven approach has also been addressed in the AI Governance framework from Wirtz, et al. (2020) in which collaboration between stakeholders is an important aspect through the whole AI Governance framework. The consensus-driven approach is important for creating belief, trust and commitment about the idea in order to boost acceptance and positive effects in society (Wirtz, et al., 2020).
Design	FR.5: Then the 'design' step contains a set best-practices to support a responsible design.
	AI.3: There needs to be a focus on AI governance for specific application areas before a broader global and comprehensive framework would appear (Butcher & Beridze, 2019).
	FR.6: costs of the system (Schaffer, Kincses & Pletl, 2017)
	FR.7: Considering guidelines GDPR (Barnoviciu, Ghenescu, Carata, Ghenescu, Mihaescu & Chindea, 2019)
	FR.8: Individual rights are not strictly shielded by laws.

Assess	FR.9: ‘assess’ is the assessment of the responsible design complied with the principles for action from the define step.
	FR.10: This process, described by Madzou and Louradour (2020), of developing the framework involves a multi-stakeholder approach for ensuring trustworthy and safe usage of facial recognition.
	RG.3: The inclusion part of this principle refers to the multi-actor process, facilitating it and inclusion of actors as a key role in framing the risk, “supposed to support the co-production of risk knowledge, the coordination of risk evaluation, and the design of risk management” (Van Asselt & Renn, 2011, p. 441). Within this principle, consensus-building is an important aspect together with the critical evaluation of it for learning how communication and inclusion can be adequately organized in different cases (Van Asselt & Renn, 2011).
	AI.4: Given the great impact of regulation on society and its potentially negative effects, the affected stakeholders and representatives of public and private interest groups should support the entire regulatory process (Collaborative AI governance layer)” (Wirtz, et al., 2020, p. 6).
	RG.4: the integration principle, assigned by Van Asselt and Renn (2011) contains “the need to collect and synthesize all relevant knowledge and experience from various disciplines and various sources including uncertainty information and articulations of risk perceptions and values” (p. 441-442). Lastly, all actors involved should reflect on what they are doing, according to the reflection principle (Van Asselt & Renn, 2011). This principle emphasizes the importance of repeated consideration during the process from all stakeholders in case of significant and difficult cases.
	RG. 5: ‘stakeholder engagement’ with the importance for assessing and managing risks (IRGC, 2019).
Validate	FR.11: The last step is ‘validate’ in which the goal is to get a certification, for proving the ability to deploy a system following the principles for responsible usage, provided after an audit from a trusted third party.
Transparency, integration and communication	RG.6: A crucial point, indicated by Renn and Graham (2006), for the successful outcome of the risk process, and overall risk governance, is the transparency of the implications and challenges throughout all elements. In addition, the three cross-cutting aspects are important throughout the whole process (IRGC, 2019). The IRGC (2019) describes the aspects as ‘communication’ with the crucial role of being open, transparent and inclusive, ‘stakeholder engagement’ with the importance for assessing and managing risks, and ‘context’ with the “need to deal with the risk in a way that fully accounts for the societal context of both the risk and the decision that will be taken”.
	RG.7: Van Asselt and Renn (2011) mention some principles for the governance of systemic risks: “the communication and inclusion principle, the integration principle, and the reflection principle” (p. 431).

Appendix VI The Tada Manifest



(Tada, 2020)

Appendix VII Table 4 Codes from analysis

Risk Governance aspect	Code	Citation respondents	Citation literature
1. Define	1.1	The organization should figure out how to "demonstrate to" its "citizens", "society or to the supervisor that" they do not store the data or only store it for a specific purpose" and that they remove the data after a certain time (F. Versleijen). Monitoring by using facial recognition seems to be something hardly applicable when considered by F. Versleijen. The reason for this is that in that situation it is unclear "what is being done with the data and there is no clear goal for using it" and "if there is a certain generic goal in which the citizen does not directly see the benefits", it might not be possible to apply the facial recognition. (F. Versleijen).	FR.1: The concern of disproportional usage (Varley-Winter, 2020)
			FR. 2: Secondly, there is the level of trust in biometric technologies of which the importance is often misunderstood. Varley-Winter (2020) state that ethical regulators and practitioners from industry should reflect on inspiring trust and ensuring trustworthy governance processes.
	1.2	Facial recognition might be more applicable when "there is a very good reason for using" it, what "would make it possible to better justify" the decision (F. Versleijen). "Get a very clear idea of the purpose for which they would like to use this software". This purpose determines "what risks are involved" (F. Versleijen).	AI.1: Formulation of a common understanding of the problem and objectives for regulatory action (Wirtz, et al., 2020).
	1.3	When placing camera's in a city you "need to have purpose limitation" (M. Sukel).	FR.3: Define a set of principles for responsible usage of facial recognition containing risks like privacy, bias mitigation, the proportional use of the technology, accountability, consent, right to accessibility, children's rights and alternative options (Madzou, & Louradour, 2020).
	1.4	It is important to "reflect objectively" on the application and verify if there is "applied goal reasoning" (J. Visser).	RG.1: the aim of capturing the variety of issues that the stakeholders involved associate with as a risk (Renn & Graham, 2006)

			RG.2: stakeholders, such as experts, policy-makers, the organization itself, stakeholders and the general public (Van Asselt & Renn, 2011)
	1.5	J. Visser thinks this is application is better applicable because the "goal is more clear".	FR. 4: The stakeholders involved in this process are industry actors, policy makers, civil society representatives and academics.
	1.6	An important aspect for applicability of the facial recognition software is the scope. The case of implementing the software in "a very limited physical environment", which will be secured with "very specific emphasis on every person who walks in", creates "a better story for that limited environment" than applying the software into a broader environment (J. Visser).	AI.2: A consensus-driven approach and collaboration, within the risk governance process, are subjects that recur frequently in literature (Butcher & Beridze, 2019; Wirtz, et al., 2020; European Union Agency for Fundamental Rights, 2020). There seems to be a high amount of agreement within literature about these subjects. Butcher and Beridze (2019) conclude that the required effective governance contains different stakeholders having critical roles on different levels of governance. Therefore, a combination of consensus-driven standards and technical tools is needed. This conclusion is supported by the statement of the European Union Agency for Fundamental Rights (2020) "working with new AI-driven technologies, which are not yet fully understood and where not
	1.7	"Start reasoning from the objectives" of using facial recognition from the perspective of "the various stakeholders that are involved, including the data subjects" (J. Visser). The different stakeholders might have different objectives for using facial recognition or in the situation of facial recognition being used. Make clear what the objectives are "which they wish to achieve through the application of facial recognition, and what are the risks which stand in the way of that objective" (J. Visser).	

	1.8	In case of the municipality of Amsterdam, the decisions around the topic of facial recognition "are being made by the municipal council", the "CTO" and "CIO" (M. Sukel). The facial recognition supplier, T. Ali, mentions that the decision making process contains a group of decision "the CTO and the project manager, they are the key people who working closely with the municipality".	much experience has yet been gathered, requires the involvement of all relevant stakeholders and experts from different disciplines" (p. 33), which also seems to indicate a consensus-driven approach. Following, this consensus-driven approach has also been addressed in the AI Governance framework from Wirtz, et al. (2020) in which collaboration between stakeholders is an important aspect through the whole AI Governance framework. The consensus-driven approach is important for creating belief, trust and commitment about the idea in order to boost acceptance and positive effects in society (Wirtz, et al., 2020).
2. Design	2.1	"with time there will be standard applications appearing". Next to these standard applications, there should be "developed guidelines for each of those applications" "from government organizations", for any country or any supermarket who wants to deploy it (T. Ali).	FR.5: Then the 'design' step contains a set best-practices to support a responsible design.
	2.2	In the current situation "it is almost impossible to avoid sharing more and more information". This raises the question for F. Versleijen "how can I now partly determine myself what happens to my data, but also what remains registered and what not, and for what purpose?" (F. Versleijen).	AI.3: There needs to be a focus on AI governance for specific application areas before a broader global and comprehensive framework would appear (Butcher & Beridze, 2019).
	2.3	T. Ali points out the permission aspect several times during the interview and specifically mentions that "nobody should be recognized without their consent".	
	2.4	One way of doing this is mentioned by T. Ali, they have a platform in which people give permission for using their data. "Only if a person enrols himself or herself by a phone, then we recognize them" (T. Ali). In this way the supplier of the facial recognition software can ensure privacy of the consumers in which "the end user is given complete consent on" the "data and on the photo" and "nobody else can enrol someone else" (T. Ali)	

	2.5	This permission aspect is also in line with the case of the application of facial recognition at the Amsterdam Area, where there was a permission of the employees to be scanned, as mentioned by M. Sukel	
	2.6	From the municipal perspective, M. Sukel points out that they only want to apply technologies when they are “scalable and not too expensive”. It needs to be an application with which they can really “make a difference in the city” (M. Sukel).	
	2.7	“One of the strict criteria’s” that M. Sukel mentions is” that they do not use personal data because the added value does not outweigh the costs. “The juridical costs would be more expensive than our own development costs” (M. Sukel).	FR.6: costs of the system (Schaffer, Kincses & Pletl, 2017)
	2.8	Also, the “internal risks” like costs, “does it deliver the right” results and what is “the perspective of the citizen/ society is important” (F. Versleijen).	
	2.9	“When using facial recognition, you are working with personal data” (M. Sukel). The expert municipal image recognition points out that the use of personal data “is within the privacy regulations” and creates a risk of doing something illegal as a governmental organization.	FR.7: Considering guidelines GDPR (Barnoviciu, Ghenescu, Carata, Ghenescu, Mihaescu & Chindea, 2019)
	2.10	“Everything should be according to the GDPR and plus some more privacy concerns from end user” (T. Ali).	FR.8: Individual rights are not strictly shielded by laws.
	2.11	F. Versleijen points out that “the law is decisive for the municipality and they must comply with the GDPR” also J. Visser mentions that the DPIA is an obligation.	
	2.12	For a municipality it is “mandatory to execute an analysis on privacy risks” (J. Visser) whenever processing is likely to result in a high risk to the rights and freedoms of individuals.	
	2.13	An instrument which is already being used, is the risk assessment for privacy impact called “DPIA”. “The DPIA is an important instrument to start ”measure whether the new development complies with the “legal framework of the GDPR (AVG)” (F. Versleijen).	
	2.14	Additionally, “a municipality has to comply with the baseline information security government (BIO)”. Municipalities base their	

		information security policy and their justification towards the municipal council and the regulators from the kingdom on this BIO which is focused on risk management (VNG, 2020). The baseline describes “the rules of the game, which we have agreed on with each other around information security” (F. Versleijen).	
	2.15	The expert privacy and security, F. Versleijen, points out that “you may expect that” the ethical, privacy and law aspects will be considered correctly.	
	2.16	“On the other hand, you see that legislation is not always clear about what is permitted and what is not” (F. Versleijen).	
	2.17	Additionally, J. Visser mentions that “the fact that something is juridically allowed, by privacy legislation, does not make it a wise idea”.	
	2.18	“GDPR is a good step” in making clearer how data should be handled, “but now there should be more guidelines” (T. Ali).	
	2.19	A risk is the level of qualification of “the person who executes the analysis” (J. Visser).	
3. Assess	3.1	There should be a “really thorough analysis” to be able to “cover the risks as broadly as possible in order to ensure that data is not misused” (F. Versleijen).	FR.9: ‘assess’ is the assessment of the responsible design complied with the principles for action from the define step.
	3.2	For risk identification in case of facial recognition for municipalities, M. Sukel would “look for someone” with a Master’s program in Business Administration and “make it an assignment to sort” out the risks and applicability.	FR.10: This process, described by Madzou and Louradour (2020), of developing the framework involves a multi-stakeholder approach for ensuring trustworthy and safe usage of facial recognition.
	3.3	F. Versleijen suggests a way of mapping out the risks for applying facial recognition could be done by a “discussion in a kind of focus group or an survey to figure out how people think about” the application.	RG.3: The inclusion part of this principle refers to the multi-actor process, facilitating it and inclusion of actors as a key role in framing the risk, “supposed to support the co-production of risk knowledge, the coordination of risk evaluation, and the design of risk

	3.4	Additionally, there will always be the "political position" and "the elections" which has an influence on the risk identification and decision making (M. Sukel).	management" (Van Asselt & Renn, 2011, p. 441). Within this principle, consensus-building is an important aspect together with the critical evaluation of it for learning how communication and inclusion can be adequately organized in different cases (Van Asselt & Renn, 2011).
	3.5	J. Visser agrees on this by mentioning that the case should also be reviewed by the municipal council "before the municipality decides to implement it".	AI.4: Given the great impact of regulation on society and its potentially negative effects, the affected stakeholders and representatives of public and private interest groups should support the entire regulatory process (Collaborative AI governance layer)" (Wirtz, et al., 2020, p. 6).
	3.6	This perspective of the citizen is something which F. Versleijen would want to see "reflected very specifically, because it is also community money that is spent". In this reflection it is most important to focus on the data protection part since the "technical requirements are not so important to society" (F. Versleijen).	RG.4: the integration principle, assigned by Van Asselt and Renn (2011) contains "the need to collect and synthesize all relevant knowledge and experience from various disciplines and various sources including uncertainty information and articulations of risk perceptions and values" (p. 441-442). Lastly, all actors involved should reflect on what they are doing, according to the reflection principle (Van Asselt & Renn, 2011). This principle emphasizes the importance of repeated consideration during the process from all stakeholders in case of significant and difficult cases.
	3.7	The municipality of Amsterdam conducted a research in order to find out the opinion from the citizen of Amsterdam about facial recognition in public areas. They gave presentations in order to see the reactions of citizens and from the internal organization. "Being transparent about facial recognition, where does it happen, organize meetings about it, and see the reactions of people", also "internally within the organisation" (M. Sukel).	
			RG. 5: 'stakeholder engagement' with the importance for assessing and managing risks (IRGC, 2019).
4. Validate	4.1	To be able to objectify this case it is important to analyse "the independent view out of the direct field of those involved and the importance". A way of doing this is to let some independent person look at it (J. Visser).	FR.11: The last step is 'validate' in which the goal is to get a certification, for proving the ability to deploy a system following the principles for responsible usage, provided after an audit from a trusted third party.

	4.2	As a solution for this trust question, F. Versleijen mentions a "certificate". The doubtfull side of a certificate is the saving of data and its level of "transparency" and whether it can be "measurable".	
5. Pre-implementation	5.1	Before implementation of an application like facial recognition, it is important "to ensure the that entire security of that entire environment is in order" which has to do with the security of the data (J. Visser).	
	5.2	"There is quite a lot of reluctance" around (F. Versleijen) the topic facial recognition among municipalities and many people "are still afraid of using facial recognition" (T. Ali).	
	5.3	The usage of facial recognition rises question like "how is it for me as citizen in my municipality, how do I know what the municipality does with the information they gather and how is my privacy guaranteed, but also how to prevent that me form being falsely accused" (F. Versleijen). "Surely, here in the Netherlands, we are quite fond of our freedom and also of our privacy" (F. Versleijen). The understanding why such applications would be needed is complicated and "the fact that there is a great deal of uncertainty about facial recognition" which creates reluctance (F. Versleijen).	
	5.4	It becomes a "balancing act for municipalities" between possibilities and reluctance. "Politically no one dares to say something" about the topic and most of the time the application of facial recognition is called "a pilot" (F. Versleijen) or "facial comparison" (J. Visser). Furthermore, F. Versleijen points out that it is an unclear point about "who is going to be decisive when there are no clear guidelines from the national government". In this case, the Netherlands, "municipalities have a lot of autonomy as long as they follow the guidelines of the law" (F. Versleijen). On the other hand, according to M. Sukel, it seems hard to find a politician who "wants to give a clear opinion or wants to speak out".	
	5.5	"If there is a meaningful application, then as a municipality, you have to communicate this very well in terms of stakeholders' expectations,	

		otherwise it" evolves in a discussion in "terms of public opinion and politics" (J. Visser).	
	5.6	J. Visser mentions that besides the areas of law, regulations and privacy, "management of society's expectations" is really important. As municipality "you can come up with something juridically valid", but if "society feels surprised" by the implementation and "did not realise sufficiently what the consequesnces would be or the municipality did not communicate sufficiently" about their intentions, then this results in a lot of reactions (J. Visser).	
6. Transparency, integration and communication	6.1	M. Sukel would deal with trust and transparency by "being transparent about image recognition, where does it happen, organize meetings about it, and see the reactions of" the citizen before implementing it.	RG.6: A crucial point, indicated by Renn and Graham (2006), for the successful outcome of the risk process, and overall risk governance, is the transparency of the implications and challenges throughout all elements. In addition, the three cross-cutting aspects are important throughout the whole process (IRGC, 2019). The IRGC (2019) describes the aspects as 'communication' with the crucial role of being open, transparent and inclusive, 'stakeholder engagement' with the importance for assessing and managing risks, and 'context' with the "need to deal with the risk in a way that fully accounts for the societal context of both the risk and the decision that will be taken".
	6.2	Also the supplier of facial recognition takes part in the creation of transparency. Their project manager "looks at all the data flows in the system of the client and he also looks at our data flow and our cloud based environment. And he tries to manage that everything is very transparent to the end user and only the person who is authorized can get access to the data" (T. Ali).	RG.7: Van Asselt and Renn (2011) mention some principles for the governance of systemic risks: "the communication and inclusion principle, the integration principle, and the reflection principle" (p. 431).

Appendix VIII Table 5 Risk overview

Risk / ***Author***	*Privacy*	*Security*	*Technical* *(+accuracy, speed)*	*Legal* *(+GDPR)*	*Data protection*	*Ethical* *(+discrimination, social, trust)*	*Resources* *(+Cost, storage)*
Hu (2017)						X	
Savastano (2017)	X		X	X	X	X	
Barnoviciu, Ghenescu, Carata, Ghenescu, Mihaescu & Chindea (2019)				X			
Han, Jeong & Won (2011)	X	X					
Kapatamoyo, Ramos-Gil & Dominiquez (2019)	X	X		X	X	X	
Sharif, Bhagavatula, Bauer & Reiter (2016)			X				
Spektor (2020)					X		
Awais, Iqbal, Ahmad, Alassafi, Alghamdi, Basheri & Waqas (2019)			X				
Medapati, Tejo Murthy & Sridhar (2019)			X				

Van der Haar (2019)			X				
Schaffer, Kincses & Pletl (2017)			X				X
Betta, Capriglione, Crenna, Rossi, Gasparetto, Zappa, Liguori & Paolillo (2011)			X				
Maeng, Chois, Park, Lee & Jain (2011)			X				
Gorodnichy & Granger (2015)			X				
Li, Liu, Lin & Wang (2017)			X				X
Karishma, Krishnan, Kiran, Dalin & Shivaji (2018)			X				
Jurevicius, Goranin, Janulevicius, Nugaras, Suzdalev & Lapusinskij (2019)			X				
Shareef (2016)			X				
Chun & Papanikolopoulos (2016)			X			X	
Kim & Park (2019)	X		X				
Praveen & Dakala (2020)	X		X			X	
R1			X	X	X	X	
R2	X		X	X	X	X	
R3	X			X	X	X	X
R4	X		X	X	X	X	