



**Universiteit
Leiden**

Governance and Global Affairs

**The Risks of Predictive Policing: A case study of the
Netherlands.**

Student:	Bram J. Marisael
Student number:	1224859
Supervisor:	Dr. Niculescu-Dinca
Second reader:	Dr. Matthys
University:	Leiden
Concerning:	Master Thesis Crisis and Security Management
Date:	13 January 2018
Word count:	23.043 (Excl. Annexes)

First of all, I would like to show my appreciation for the people of the Dutch police. They made it possible for me to conduct my research. Therefore, I would like to express my sincere appreciation to all of the people that I have interviewed for making time for me on such a short notice.

Special gratitude goes out to my supervisor, Dr. Niculescu-Dinca. Thank you for accepting me as a student next to your capstone, giving me the initial contacts for my research and providing me with feedback during the whole writing process

Abstract

A fairly new phenomenon is the use of predictive policing methods. This type of policing tries to predict and prevent crime before it has even taken place. In the United States a lot of literature and theories are developed on its use, benefits and pitfalls. These kind of studies are lacking in the Netherlands, where predictive policing has only just started with the use of a predictive policing system called CAS. This gap in the literature is why it is interesting to research how predictive policing is taking shape in the Netherlands. Examining predictive policing in the Netherlands is also relevant on a societal level. Predictive policing methods are often thought of to produce discriminatory or biased outputs for civilians. The thesis aims to assess the risk perception of the Dutch police on the risks of predictive policing. This is done by constructing a framework of five risks that are mentioned extensively in existing literature. This framework is utilized to interview six predictive policing experts of the Dutch police. The purpose of these in-depth interviews is to see whether experts of the Dutch police perceive the same risks. Do they think some risks are probable and are they concerned with the consequences of risks? In the analysis the data that is gathered from the open-end elite interviews is colour coded and then linked to each risk that the literature discussed. Furthermore, new risks that are mentioned by the experts are also analysed. All risks that are mentioned in the literature on predictive policing are perceived by the Dutch police. Some risks such as privacy risks are seen as more serious than others such as classification risks. Most of this difference in risk perceptions has to do with the design of CAS, which tackles some risks. Other risks are minimized by the use of safeguards such as the information officer. New risks that are mentioned in the interviews are mainly internal organizational risks for the Dutch police on the implementation and use of CAS. All in all the risk perception of the Dutch police on their predictive policing system is serious and extensive.

List of Contents

1. Introduction & Research Question.....	7
1.1 Research Problem.....	7
1.2 Research Question & Objective.....	9
1.3 Societal relevance.....	10
1.4 Academic relevance.....	11
2. Theoretical framework.....	12
2.1 Introduction.....	12
2.2 Big Data.....	12
2.3 Algorithmic Governance.....	13
2.4 Intelligence-led Policing.....	14
2.5 Predictive Policing.....	16
2.6 Risk.....	18
2.7 The Risks of Predictive Policing.....	19
2.7.1 Classification Issues and Human Bias.....	20
2.7.2 Profiling Risks.....	21
2.7.3 Algorithmic Risks.....	22
2.7.4 Less Exposed Risks of Predictive Policing.....	24
3. Methodology.....	26
3.1 Research Design.....	26
3.2 Case Selection.....	27
3.3 Conceptual Framework & Operationalization.....	28
3.4 Data.....	30
3.5 Limitations.....	33
4. Analysis.....	34
4.1 Profiling Risk.....	35
4.2 Algorithmic Risk.....	38
4.3 Privacy Risk.....	42
4.4 Classification Risk.....	44
4.5 Risk of Losing Traditional Policing Skills.....	47
4.6. New Risks.....	49
4.7 Combining the Perceptions of the Dutch Police.....	52
5. Conclusion.....	55
6. References.....	58

List of Tables & Figures

Figure	1. Case Study.....	22
	2. Conceptual Framework.....	24
Table	1. Risks of Predictive Policing	25
	2. Color-Coding Scheme	29

1. Introduction & Research Question

1.1 Research Problem

A fairly recent phenomenon is the so called Smart City. A Smart City is a city in which advanced systems manage energy, water, transportation, traffic, healthcare and education (Popescul & Radu, 2016, p. 29). These systems collect and manage a huge amount of information and data in their respective sector. Likewise, in the field of policing practices there is a visible increase in reliance on the information infrastructures that we encounter in smart cities (Niculescu-Dinca, 2016, p. 455). This reliance on information structures in policing can be observed in predictive policing. Predictive policing is a policing model that uses information and advanced analysis to prevent crimes. This policing model relies heavily on predictive algorithms, information technology and the use of data. In the most basic sense it tries to predict on which location a crime will happen, or which specific location has the highest chance of a crime being committed (Ferguson, 2012, p. 265).

There are several benefits that predictive policing creates and facilitates. First of all the search for patterns is simplified. A computer can identify patterns more easily than a human being, simply because it can process much more data. If crime patterns are predicted more effectively this has the advantage of a better resource allocation. Most police forces have to make strategic choices in where to deploy their cars, officers etc. The use of a predictive policing system helps in making these strategic choices (Fyfe et al., 2018, p. 5). On top of that predictive policing is also very cost-effective. If police officers can be directed towards 'crime hotspots' this results in them being able to arrest more criminals and prevent more crime than they usually would have done if they were patrolling on intuition. In this sense they are being more effective at their job (Ferguson, 2012, p. 269-270). Another economic advantage of predictive policing is that if the police can patrol pre-emptive, this can lower possible costs related to vandalism, property damage and costs due to theft. The effectiveness of predictive policing models is also the result of its sophisticated analysis. This analysis incorporates factors such as demographic trends, parole populations and economic conditions to predict crime patterns. Previously it was too hard for the police to take all these factors into account when predicting crime. Finally the most obvious advantage of predictive policing is social economic, it reduces the risk for citizens to become victims of crime. Furthermore it can pre-emptively stop offenders from making life changing mistakes (FICCI Studies & Surveys, 2018).

However, there are also some signs to be careful with the use of data and algorithms in policing practices. As indicated by Ferguson (2012) predictive policing makes a lot of use of

algorithms and big data. Rosenzweig, Smith and Treveskes argue that the rule of algorithms must not be mistaken, as often happens, to be an objective and more rational rule of law (Rosenzweig, Smith & Treveskes 2017). Algorithms could incorporate prejudice in some cases. The reason for this incorporated prejudice could, for example, be the result of algorithms that use some type of machine learning or because of human bias (Barocas et al. 2017, p. 680).

Barocas et al. (2017) argue that even if algorithms are free of malice they can produce similarly discriminatory effects. They use the example of an algorithm that instructs police to search pedestrians. They state that if this algorithm has been trained on a dataset that over represents crime among certain groups, the algorithm may direct police to detain members of these groups at a disproportionately high rate (Barocas et al. 2017, p. 681). This could eventually lead to a situation in which information infrastructures directly affect the trust between the police and certain social groups or communities (Niculescu-Dinca, 2016 p. 465).

The features of predictive policing through big data, as mentioned above, pose a problem. On one hand predictive policing might make it easier for police to allocate resources in a correct way, provides a cost-effective solution to crime and has social economic advantages for citizens. On the other hand it might pose the problem that the police loses its original skillset or becomes too reliant on algorithms and predictive policing and therefore underestimates the risks, some of which are mentioned above, that come with it. There is a lot of literature and theory on predictive policing, its benefits and its risk, but not that much is known about how the people who actually work with predictive policing systems view this policing model. A gap in the literature can be identified by looking at the perception of police themselves about predictive policing methods and systems. This thesis will address this gap in the literature by delving deeper into the perception that the police has of the risks of predictive policing.

1.2 Research Question & Objective

The central research question that is used to target the research problem described above is the following one: *‘How does the Dutch police perceive the risks associated with predictive policing?’*

This will be assessed with a case study of the Crime Anticipation System (CAS), the most relevant and important predictive policing system of the Netherlands which has been implemented in 2017. The research will focus on how the police themselves perceive the risks of predictive policing. In the literature multiple authors have indicated that predictive policing can lead to different issues. Classification risks, profiling, subconscious discrimination of minorities and non-reporting issues are mentioned as important challenges for predictive policing methods. However, what seems to be lacking is a stance that does not come from the academic world, but from the people who actually work with these predictive systems. This stance will help with either identifying some of the risks that the literature mentions, identifying risks that the literature does not address or possibly debunking certain risks. If the police’s own perception of risks is examined and linked to the existing literature and ideas surrounding predictive policing, this will create a better understanding of how valid and relevant different types of risks are. This research will be explorative because it will try to construct an overview of the risk perception of the police, something that has not been done in the existing literature. In this sense there will be no testing of hypotheses, instead this research will try to investigate certain expectations or assumptions on the risks of predictive policing by the Dutch police. These expectations are constructed through the existing literature on the risks of predictive policing. In the second chapter of this thesis the different concepts that are important in understanding predictive policing and its risks are highlighted and explained. In the third chapter the methodology of this research will be explained. The fourth chapter consists of an in-depth analysis and the thesis is wrapped up with a conclusion.

1.3 Societal relevance

This research question is relevant to answer, both on a societal and academic level. On the societal level, many sectors are becoming increasingly reliant on big data and algorithms to help with certain problems that the sector faces. This is, as mentioned above, also the case for policing methods. It is seen as a viable solution because of its cost-effectiveness, efficiency in allocating resources, and help in making strategic decisions and identification of crime-patterns on a big scale. This way of policing is seen as one of the most influential models of policing in this current time, mainly because it uses a lot of technological innovations and thus is seen as a model that is up to date with the latest technologies. More countries and police forces are starting to use algorithms and big data of predictive policing systems as their main policing practices. The trust in predictive policing as the policing model of the future seems partly justified. It certainly has a lot of advantages, but there seems to be some risk and possible pitfalls involved in it as well. Therefore the topic of predictive policing carries a lot of societal relevance. If this is the policing model of the future it is important that citizens and practitioners of these systems are aware of the risks that surround this policing model. It can help in preventing unwanted outcomes due to unaddressed or overlooked risks in predictive policing. Furthermore, this specific case of the Dutch predictive policing system, the CAS, has not been around for a long time. The pilot started in 2014 and the rollout of the system started in 2017. This makes it even more relevant on a societal level to examine what kind of risks the Dutch police perceives in this system.

1.4 Academic relevance

Regarding the academic relevance, if looked at the existing body of knowledge surrounding predictive policing, there are a lot of theories and focus points regarding methods, benefits and risks. There is extensive literature, focusing on both technical and ethical aspects of predictive policing. However, what seems to be missing is an in depth analysis of what the police themselves think of predictive policing. Certainly regarding the risk-factor of predictive policing a lot of assumptions are made in the literature about what kind of risks are the most urgent and important ones. These assumptions on risks have not been verified by the police themselves in a lot of cases. This is why it is interesting to try and understand the risk perception that the police themselves have of risks that are associated with predictive policing. It might give an insight as to which risks, of the ones that are identified in the literature, are or are not present in these predictive models or if there are even some risks that have been overlooked by academics. Another important part of the academic relevance is the fact that this research will focus on the Netherlands and the CAS. A lot of predictive policing articles and theories are derived from American predictive policing systems. This means that a lot of case studies on predictive policing systems are focusing on either the United States (U.S.) or the United Kingdom (U.K). Systems such as PredPol have been examined quite extensively. The CAS however is a different system in many ways. This is why this research, because of its focus on the Netherlands has more academic relevance than just for the fact that it is an in-depth analysis.

2. Theoretical framework

2.1 Introduction

The theoretical framework of this thesis will use a funnel that starts with big data and algorithms. This is done in order to get a better grip on how big data and algorithms are working together to create information structures and in what ways they can shape predictive policing models. This is done since predictive policing is a unique form of policing that relies on big data and algorithms in particular. After the origins and benefits of predictive policing models are clear, the risks that are associated with predictive policing will be examined. This will happen in two parts. First of all, since this research concerns the risk perception of the Dutch police, the concept of risk will be further explored. In the second part both academic literature and police insights will be used to identify the risks of predictive policing and see which ones are the most important. This will result in a theoretical framework that first discusses the basis on which predictive policing is designed: algorithms and big data. After that the origins of the policing model will become clear and the concepts of risk and risk perception will be elaborated upon. All of this is concluded by providing a clear overview of the current literature, both from academics and the Dutch police, on the specific risks of predictive policing.

2.2 Big Data

As mentioned above, big data is a big part of predictive policing. Many authors have tried to define the concept of big data, one of them is Batty (2013). He stresses that the importance of a focus on information technology and the concerns it raises about issues that are related to the use of big data. First of all he argues that the best definition of big data is a really simple one, but therefore one that is easily understandable as well, namely: *'any data that cannot fit into an Excel spreadsheet'* (Batty, 2013, p. 274). The concerns that Batty specifically points to when discussing big data are plenty. Issues of privacy and confidentiality are obvious ones (Batty, 2013, p. 277). The definition of big data as described by Batty is a simple one, but a more elaborate definition is necessary. There are many definitions and none of them seem academically agreed upon. However, Kitchin indicates that most definitions include the 3Vs: volume, velocity and variety. Big data are high in volume, high in velocity and diverse in variety. This means big data is perceived to be terabytes or petabytes of data which is being created in or near real time and has both a structured and unstructured nature (Kitchin, 2014, p. 67-68). Next to these three 3Vs the literature on big data also describes some other key characteristics of big data. The main ones are that big data is exhaustive in scope, fine-grained

in resolution, relational in nature and flexible (Kitchin, 2014, p. 68). Kitchin states that many branches of governments have changed over time and by changing have adopted new management practices and technologies. As a result of this information systems and big data have become essential to support infrastructures of organizations by helping them to make decisions about present and future operations. In this way, big data allows organizations to be run more intelligently (Kitchin, 2014, p. 118-119). According to Kitchin big data provides the possibility to develop, run and regulate and live in a city on a foundation of strong and rational evidence. This results in a city that, due to big data, is more efficient, sustainable, competitive, productive and open. On the contrary, Kitchin also notes that this kind of governance is prone to a 'big brother' feeling due to its technocratic nature (Kitchin, 2014, p. 125). He adds that normative conversations on the future of big data and questions about the kind of big data world we would want to live in, are currently underdeveloped. Furthermore he stresses that these conversations and questions are needed, seeing how big data is increasingly shaping our governance, organizational management and economy (Kitchin, 2014, p. 127).

2.3 Algorithmic Governance

This shaping of our governance by big data goes hand in hand with the topic of algorithmic governance. Big data often uses algorithms to create the instructions mentioned above. Algorithms can be seen as a computer procedure that guides your computer step by step to solve a problem or reach a goal. In this way an algorithm can be viewed upon as a list of tasks for your computer, which is the input. The output of the algorithm is the completion of these tasks. Završnik sees an algorithm as a computer guided replacement of proper reasoning (Završnik, 2017, p. 3). Over the last decade more and more software is used to provide government services and even government decision-making. Algorithms have become an essential part of bureaucracies and civil services (Searle, 2016, p. 172). This increase in governmental use of algorithms to govern has not gone unnoticed. Many have raised questions about the consequences of this form of governance. An extreme example of algorithmic governance is China where algorithms are used to engineer an entire society. An economic and political rating system, constructed by algorithms, is being implemented in the country. The goal is the spreading of integrity throughout China by providing the trustworthy with benefits and discipline the untrustworthy (Brehm & Loubere, 2018, p. 38-39). Of course this is just one case, which is China, but more and more governments are becoming entangled within the web

of big data and the use of algorithms to construct societies. In this thesis the focus will be on the use of algorithms in one specific governmental branch, the criminal and justice department.

Završnik explains that an algorithm can be used to predict certain events, given the correct input, and prevent them before they are set in motion. This kind of use of algorithms is not applicable to all branches of government, but it is, like Kitchin (2014) indicated, present in a lot of them. One of the branches of governance in which it is used is the criminal system. Especially the decision-making process within the crime system is becoming more and more automated. All of this is the result of big data and its underlying promise of security. The way in which this promise is met, is by using algorithms that can take on large amounts of data at an increasingly faster processing rate algorithms. Završnik goes a step further by saying that power in this sense is being transferred from the democratic polis to a digital entity (Završnik, 2017, p. 7-8). In the book 'Big data, crime and social control' Završnik states that a challenge of big data is to accumulate large amounts of data and extract useful instructions out of this data. But he wonders for whom and at what cost (Završnik, 2017, p. 3). Within the criminal system the ability of algorithms to predict certain events leads to the use of algorithms in policing. There is a visible increase in reliance on information structures such as big data and algorithms in policing (Niculescu-Dinca, 2016, p. 455).

2.4 Intelligence-led Policing

This increased reliance on information structures within policing is a fairly recent trend. However, it is important to note and understand that there are other popular policing models that are still being used and have been used prior to predictive policing such as community policing and problem-oriented policing. Predictive policing however, is a part of intelligence-led policing (ILP).

This is why ILP is the most important policing model for this research. ILP originated in England in the 1980s, where it was seen as a means to battle crime through better intelligence (Treverton et al., 2011, p. 32). Carter describes ILP as a philosophy. He argues that it is a manner in which intelligence fits into the operations of a law enforcement organization (Carter, 2004, p. 4). ILP has no universally accepted definition, but a lot of definitions do touch upon the same parts. One definition of ILP is: '*a collaborative law enforcement approach combining problem-solving policing, information sharing and police accountability, with enhanced intelligence operations.*' The focus, as this definition indicates, lies on intelligence. This is the collection of raw information that can be used in an analysis. This analysis and the focus of it

is often determined by a data analyst. They define intelligence requirements and make a selection in data that is used in the final analysis of the raw data. The shift towards ILP has, by many, been described as the result of an increased focus on homeland security (Carter & Carter, 2009, p. 317-318).

To be specific, this model of policing focuses on the use of covert methods to deal with crime. The clear advantages of the model are flexibility in choices of tactics, higher likelihood of multiple arrests, removal of interview-based evidence and encouraging cooperation between police officers and members of other agencies (Maguire, 2000, p. 319-320). Furthermore, as Treverton et al. indicate, ILP reduces the need for police presence on the street. ILP was invented to improve policing through practices of analysing empirical evidence with better and faster technologies. This is combined with integrating research results into policing practice. As a result data collection, data analysts and measures driven by data analysis are at the core of ILP (Treverton et al., 2011, p. 32-33). Sanders et al. add that ILP integrates old knowledge of policing like criminal informants and suspect interviews, with new knowledge of policing. By this new knowledge they mean possibilities such as crime analysis and the surveillance of national databases (Sanders et al., 2015, p. 713).

Maguire argues that this role of the police as: *'communicators of risk knowledge'* by which he means that the police consists of: *'collectors, analysts and disseminators of data which feed a never-ending process of risk classification and profiling'* (Maguire, 2000, p. 318-319). In order to keep this sequence running routine and special surveillance is carried out by the police in different areas on different activities and individuals. This increased surveillance is transferred to local level law enforcement as well, whereas previously these technologies were mainly used to investigate and battle major organized crime (Maguire, 2000, p. 318-319). Another key factor of ILP is that it means that reactive policing is changed into proactive policing. Supporters of ILP argue that it is the perfect policing strategy in terms of efficiency and facing the emerging new challenges within battling crime (Fyfe et al., 2018, p. 2-3). The ultimate goal that ILP sets, is predictive policing. Predictive policing can be seen as the final and most developed part of ILP. A lot of police departments are currently switching, or already have switched, to transition to ILP in the name of predictive policing (Treverton et al., 2011, p. 33).

2.5 Predictive Policing

Predictive policing sounds like something you would see in sci-fi movies about futuristic forms of policing. However, the use of predictive policing has already spread across police services around the world rapidly. Predictive policing, put simple, is a policing method that focuses on stopping crimes before they are even committed. By using advanced analytics and data the police tries to act pre-emptively against crimes by focusing on high-risk crime areas and individuals. The advanced systems being used in predictive policing are being applied to zoom in on potential criminal activities. The way in which this is achieved is by giving input into a predictive model, often consisting of datasets guided by algorithms, which then produces an output that police officers can use to patrol certain neighbourhoods that are being considered prone to criminality by the predictive model (FICCI Studies & Surveys, 2018). Karppi defines predictive policing as a policing model that: *'uses algorithmic analysis of "criminal behavior patterns" together with three data points, "past type, place and time of crime" to provide "law enforcement agency with customized crime predictions for the places and times that crimes are most likely to occur'* (Karppi, 2018, p. 1).

This type of policing offers many new options to the police. In the United States research concluded that in some cities criminal activity was highly over represented in some areas. In Seattle half of the crimes were committed on 4.5 % of the city streets. Similarly in Minneapolis 3.3 % of the streets attributed to 50.4 % of all dispatched police. It is important to note that this research was done after all these crimes had been committed. Predictive policing offers the police the opportunity to map and patrol these 'high-risk' city streets pre-emptively and therefore preventing crime from happening (Ferguson, 2012, p. 273-274). Other studies have also indicated that criminals are used to habits, which leads them to commit the same types of crime, but also returning to areas where they have successfully committed crimes in the past. Predictive policing systems allow the police to use an incredibly sophisticated system to reveal these types of crime patterns, instead of simply placing pushpins on paper maps (Koss, 2015, p. 302-303).

There are two types of models in predictive policing technology. The first model is the near repeat model. This model assumes that crime spreads through local environments like a disease. One of the conclusions that is derived from this assumption is that when crimes occur in a certain location, this will tend to happen again in the same location. Koss argues that crime hotspots are very hard, almost impossible, to predict as an individual. Mainly because they appear and disappear in extremely complicated ways. The near repeat model requires regular input by agencies to remain up-to-date. Studies have shown that this type of model has a high

success rate for predicting burglaries, but lacks in predicting gun violence or crimes of passion. One study also showed that the near repeat model can predict the location of violent gang related activities (Koss, 2015, p. 309). This results in near repeat models being validated for some types of crime, but certainly not for all types (Ferguson, 2012, p. 281).

The second model is risk terrain modelling (RTM). This model uses geographical information to identify features or certain locations that might contribute to an elevated crime risk. The presence of bars, liquor stores and strip clubs are some of the factors that the RTM identifies as crime elevating (Koss, 2015, p. 310). After this identification the RTM then looks for similar geographical features in other areas and predicts the risk of crime. This is based on how close these areas are to the above-mentioned features. The main difference with the near repeat model is that the RTM predicts crimes based on behavioural, social, physical, and environmental factors instead of only relying on information about locations where criminal activity occurred in the past (Koss, 2015, p. 310). Research on the effectivity of the RTM has shown that it in fact seems to be able to predict 'random' shootings based on these features (Ferguson, 2012, p. 283).

Predictive policing in general seems to offer several benefits, which is the main reason that it is currently becoming more popular in different police forces to use these kind of systems and models. The first advantage of predictive policing is that computer guided algorithms can analyse and recognize patterns a lot faster than humans. Furthermore, these systems can incorporate multiple factors within their pattern analysis such as demographic trends, parole populations and economic conditions (FICCI Studies & Surveys, 2018). This results in an analysis that is more complete and sophisticated than one a human being could develop. This analysis and especially the recognition of crime patterns on a larger basis leads to a second benefit. Predictive policing systems help for a great deal when police departments are making strategic choices about where to deploy their officers. You want to put your police officers at the places where they can be the most effective. This is where the predictive policing systems offer a helping hand. As Koss (2015) indicates these systems are based on identifying so called crime-hotspots where crime is most likely to occur (Koss, 2015, p. 302-310). If this is known the police can spread their forces in a much more efficient way, thus leading to a better allocation of their often limited resources. If police officers would patrol the streets based on intuition it is to be expected that they would not be as effective in targeting crime (Ferguson, 2012, p. 269-270). This advantage deals with cost-efficiency as well. Nowadays a lot of pressure is put on police departments to perform. After all it is often presumed that it is the taxpayer's money that is spent on the tackling of crime by the police. If police officers are

deployed more effectively during their shift this means that they are more cost effective than if they would have nothing to do most of their shift (FICCI Studies & Surveys, 2018).

2.6 Risk

As indicated above there are good arguments as to why a police department should use predictive policing methods. However, there are also several risks involved in predictive policing. The given that my research question focusses on the risk perception of the Dutch police means that a clear and important factor within my research question is the concept of risk. Before the actual risks of predictive policing will be discussed, it is necessary to apply a focus on the concept of risk perception theories that are associated with it. This will help to indicate what exactly risk perception is and how to eventually recognize it within the Dutch police.

Before risk perception or the phenomenon of risk inside institutions is observed, the concept of risk will be touched upon. Risk is often seen as the likelihood of someone experiencing danger (Short Jr, 1984). Frame defines it a bit different, he argues that risk is the chance or likelihood of events with negative consequences (2003). This definition of risks in a negative way is carried over to institutional or organizational risk. Ericson and Haggerty (1997) examine the way in which risk discourse is socially organized through the institutional defining of dangers. First of all they argue that this focus on danger by institutions as something that should be countered inherently means that risk is characterized by a negative logic. This results in a situation in which the institution is concerned with preventing the worst-case scenario, instead of thinking about something good to come from risks (Ericson & Haggerty, 1997, p. 85-87). According to Ericson and Haggerty police organizations are institutions that have traditionally been concerned with different types of risks and have a strong sense of organizational risks (Ericson and Haggerty, 1997, p. 295). Another important factor that they attribute to police organizations is that they are seen as leaders in technological development and adaption (Ericson and Haggerty, 1997, p. 389). Following the literature one could argue that this indicates that the Dutch police should have a strong sense of organizational risk. The fact that they are working with predictive policing systems also confirms that it is an organization that leads in the field of technology. But how to translate this organizational risk into organizational risk perception? First of all it is important to note that the research question obligates a definition of risk perception that should be applicable to an institution. Secondly, it

must be stressed that the risks that are examined in this research are both risks to the organization as well as risks that the organization might cause to others.

But what exactly is risk perception? One of the main theories surrounding risk perception is the psychometric paradigm, which has its roots in psychology. This theory states that risk is subjective and is not something that can be measured objectively. Instead, it is dependent on things like experiences and cultures (Slovic, 1992). Akintoye & MacLoad (1997) agree with this notion. They state that risk perceptions are built on beliefs, attitudes, judgments and feelings. This leads to risk perception that can be defined in different ways. Moen et al. define risk as the subjective assessment of the probability of a specified event and the way we are concerned with its consequences (Moen et al., 2004). Another definition comes from Wachinger and Renn, who see risk perception as a process of multiple events such as collecting, selecting and interpreting signals from uncertain impacts of events, activities or technologies. This is followed by a final judgement that finishes the process and concludes it by taking a decision (Renn & Wachinger, 2010). A final definition is provided by Spencer (2016), who defines it as a brain process where previously assimilated risks are reconstructed through a subjective judgement. The definition provided by Moen et al. (2004) seems to be the one that is most applicable to institutions, which is why it is the one that will be used in this thesis. In this regard this thesis will focus on how the Dutch police assesses the probability of certain risks of predictive policing and in what ways they are concerned with their consequences.

2.7 The Risks of Predictive Policing

Now that the concept of risk has been examined it is interesting to look at the actual risks of predictive policing. The discussion of predictive policing risks will consist of content from both academic literature and literature that originates from the Dutch police. This will ensure that a clear image of predictive policing risks is constructed from both the academic world and the police themselves. These risks are not only risks, such as privacy issues, that are focussed on society and its citizens. There are also risks that are only applicable to the police, an example of this is the loss of traditional policing skills. This means that this thesis is about risks that the organization of the Dutch police might inflict upon others through predictive policing and risks that predictive policing causes for the organization themselves. Following the definition of risk (Moen et al., 2004), which was specified on the Dutch police as: *'The probability of certain risks of predictive policing and in what ways the Dutch police are concerned with their consequences,'* this thesis will focus on the ways in which they are

concerned with the consequences of both of these risk-types. The risk on the loss of traditional police skills is one that clearly is a risk for the Dutch police. But a risk such as algorithmic risk is not as obvious. It is a risk for citizens if the algorithm is biased, but also for the police because it affects their legitimacy and effectiveness. This overview will not split up the risks in risks 'to' or 'because of' the organization. The first reason behind this is that sometimes risks can be interpreted in both ways, the second reason is that it is not the goal of this thesis to create such an overview. The goal is to create an overview of all the risks surrounding predictive policing and apply them to the Dutch case. Therefore, the literature on the risks of predictive policing will be examined to create an overview of the most relevant risks that authors identify and describe. After this image is constructed it will either be validated or debunked. This will happen by comparing the risks that are mentioned in the literature with the risks that are observed by predictive policing experts of the Dutch police.

2.7.1 Classification Issues and Human Bias

Within the literature on predictive policing several important risks are identified. As Maguire argues, predictive policing, for a big part, deals with risk classification and profiling (Maguire, 2000, p. 318-319). Fyfe et al. sharpen this notion by stating that predictive policing and its use of big data analysis and algorithms are taking classification and categorization to a whole new level (Fyfe et al., 2018, p. 158). This is where the first concerns regarding predictive policing are emerging. Bowker and Star (1999) were one of the first ones to express their concerns about big data analysis in relation to classification. It is important to grasp that classifications are not to be underestimated, they are a powerful technology. Furthermore, classifications are all around us in the information landscape that is being created this very moment. One of their issues regarding classification, which seems closely linked to classifications used in predictive policing, is the black boxing of classifications. As information structures are more and more reliant on classifications, they argue that there is a risk of making classifications both potent and invisible, thus black-boxing them. This could lead to the exclusion of the public from policy participation because they have no insight in these classifications (Bowker and Star, 1999, p. 319-324).

A point that follows up on these classification risks, is the risk of seemingly objectivity or neutrality in algorithms. Karppi argues that techniques and technologies are never neutral. In his eyes they always establish and maintain boundaries across race, gender and class. This implies that technologies such as predictive policing have different outcomes and consequences for different people, and thus are not a one size fits all solution to the tackling of crime (Karppi,

2018, p. 4). This lack of objectivity in algorithms is mainly a cause of human bias. Koss is another author who discusses the risks of predictive policing. She highlights that within algorithms and especially their creation humans are still the ones who select what information they incorporate into certain systems. Individuals make choices about what data to collect and what method is best suited to collect this data. She agrees with Karppi by stating that outputs from predictive policing algorithms should not be mistaken for facts. In this regard she concludes that *'the data is only as good as the people using it* (Koss, 2015, p. 311-312).'

2.7.2 Profiling Risks

Next to the classification issues other authors indicate other risks of predictive policing. One of them is that predictive policing systems are inherently biased because they rely on reported crime data. This crime data is often extracted from areas that are heavily policed. By this type of predictive policing, based on historical data input, the risk is that poor or minority communities are overrepresented because they often live in the areas that are policed the most (Kirkpatrick, 2017, p. 23). Karppi also identifies this risk of human bias that might lead to overrepresentation of certain minorities. He goes even further by stating that predictive models carry an inherent risk of racial profiling. His main argument for this statement is that, even though predictive policing only maps locations and not individuals, it still directly affects those who live in or pass through these mapped locations (Karppi, 2018, p. 4). Karppi is not the only one who observes this tendency towards discriminatory outputs from predictive policing systems.

Koss, who looks at predictive policing methods in the United States, mentions that the high-crime label is often attached to low-income minority neighbourhoods across the U.S.. This has led to an uneven distribution in the number of people of colour that have been stopped-and-searched. She warns for the incorporation of, as she calls it, structural racism into criminal justice systems through predictive policing. Many young black men in the U.S. have indicated that they have an expectation of being stopped, interrogated and searched a number of times in a single week (Koss, 2015, p. 321). She also indicates that low-income minority neighbourhoods often lack the power and money to combat the increased policing in their area on the basis of predictive policing, whereas wealthier neighbourhoods could possibly use their power to make a case for less heavy policing (Koss, 2015, p. 322).

There is very little written information in which the police addresses the risks of predictive of policing, but there is one specific work that is the most relevant and important one for Dutch policing. This is a book written by Rutger Rienks in 2015, Rienks was the head of

the department for business intelligence at the Dutch police from 2013 until 2015. In this function he dealt with predictive policing in the Netherlands extensively, which is why he is considered to be an expert on this topic. His book therefore can be considered authoritative when it comes to predictive policing in the Netherlands (De Correspondent, 2015).

In his book Rienks also identifies the risk of profiling. He states that if an individual is selected to be controlled on a basis that is above average this can give a rise to feelings of inequality or even discrimination. Rienks therefore indicates that the police should be careful with predictive policing measures. Selecting and treating people based on personal characteristics such as race, skin-color or heritage is forbidden. In this sense heavy patrolling in poor neighbourhoods, often occupied by certain minorities, could also be seen as a selection and treatment on personal characteristics. As a measure to counter this possibility of discrimination he stresses the importance of selection of the basis of behavioural characteristics instead of personal ones (Rienks, 2015, p. 142).

2.7.3 Algorithmic Risks

The third risk that can be distilled from the literature is the algorithmic risk. Barocas et al (2017) pay attention to the technical aspects of predictive policing risks. They mainly touch upon the risks of the reliance on algorithms in predictive policing. They argue that most algorithmic problems are present because of machine learning, something that is used in predictive policing as well. Machine learning is an algorithm where the machine or system '*has been "trained" through exposure to a large quantity of data and infers a rule from the patterns it observes*' (Barocas et al., 2017, p. 679). Within machine learning several risks can be identified. Since it are these kinds of automated decision systems that are used in predictive policing, they are vulnerable to both faulty and biased outputs. Decision rules of machines that produce the outputs of predictive policing systems might be constructed mathematically, but the lessons they might have been 'trained with' could have been faulty, biased or unfair (Barocas et al., 2017, p. 680).

Barocas et al describe three ways in which decisions that are made by algorithms may produce discriminatory effects. The first example is focused on cases where algorithms are 'trained' to learn from historical examples. If these historical examples, that the machine uses to train itself, are statistically incorrect this creates a problem. A good example would be a situation in which an algorithm, like in predictive policing, would instruct officers to stop and search people in certain neighbourhoods. However, if this algorithm has been trained with a dataset that over represents crime rates within certain neighbourhoods this might lead to an

algorithm which directs police officers to certain areas at a disproportional high rate. In this way the algorithms are subconsciously creating a discriminatory output (Barocas et al., 2017, p. 680-681).

A second algorithmic risk is that models that use algorithms can be constructed in a wrong way and therefore might create faulty results. Barocas et al indicate that most of these construction errors are present because of wrong selection choices by individuals who instruct and create algorithms. They call these choices ‘feature selection.’ If selection criteria within an algorithm are badly constructed this can have severe implications for the model. The three most common mistakes are firstly incorporating decisions that take membership of a certain group into account, an example of this could be that the algorithm takes in gender or race into account when making decisions. The second mistake is assessing members and non-members, for example males and females, with a wrong dataset. For example, if the historical examples that are entered into an algorithm contain the data on 100 men and 50 women, the data and its conclusions on women might be less reliable because of the lower N used in the dataset (Barocas et al., 2017, p. 681).

Where the risk mentioned above deals with the unintentional construction of discriminatory features within the algorithm, the third algorithmic risk is intentional discrimination. A data scientist that has his own, prejudiced motives, could intentionally alter the data that is used for machine learning through historical examples by picking examples that suit his agenda. This could then create intentional discriminatory outputs. The process in which a data scientist incorporates his own prejudice into an algorithm is called masking. Since machine learning is a process that is very reliant on human input this means that machine learning is very vulnerable to masking issues. This risk is closely linked to human bias risks which are mentioned above (Barocas et al., 2017, p. 682). A final risk regarding the historical data that predictive policing systems use is that it could be a misrepresentation. For example, many incidents of vehicle thefts or sexual assault and rape are not reported. These crimes could also occur in certain areas where the algorithm does not see any incentive to increase policing. In this sense the system could miss what is really happening out there (Kirkpatrick, 2017, p. 23).

Rienks highlights the algorithmic risks as well. He gives examples of decisions that are being made in a black box and thus have no transparency or algorithms that are no longer understood by data scientists themselves (Rienks, 2015, p. 135). Another point of attention in algorithmic risk that is identified by Rienks is the fact that an algorithm can never be 100% right. The goal is to create an output with the highest possible score, but sometimes you will

encounter false-positives when you are working with algorithms. He argues that this power of output, score wise, is very dependent on the input variables, the way in which the algorithm is constructed and sufficient testing and training of an algorithm (Rienks, 2015, p. 136). False-positives are a risk when working with systems that are conducting automatized analysis. For example, a young driver in a very expensive car is not necessarily a criminal, but can also be a successful celebrity or entrepreneur (Rienks, 2015, p. 47).

2.7.4 Less Exposed Risks of Predictive Policing

In this final part on risks of predictive in academic literature the focus will be on risks that are not as big and elaborated upon as the ones that are listed above. This is not about how often they are named, instead it is about how extensively they are examined. For example, some risks are covered in entire articles or are addressed in multiple paragraphs in several articles. This does not go for the following risks. They are only mentioned shortly in most cases, or they are not named at all. However, it is still important to take them into account as well. Especially since this theoretical framework aims to provide an extensive overview of all risks of predictive policing, instead of just highlighting the most important ones. A risk that has not yet been mentioned is the loss of traditional policing skills. A situation in which the police can point at people and arrest them with the sole argument: ‘the algorithm said so’ is problematic. Of course this example is exaggerated, but the focus on algorithms does pose a potential risk of police officers losing their knowledge and skillset. Even when working with algorithms it is important that a police officer can still judge individual incidents according to his own intuition and insights (Smit & de Vries, 2016, p. 16).

Rienks quickly touches upon the risk of the disappearance of traditional policing skills and increased reliance on algorithms. He wonders if algorithms could one day replace the police officers as we know them (Rienks, 2015, p. 139). This raises a control concern. Rienks argues that algorithms and predictive policing methods certainly create new possibilities for police department, but that a clear distinction about who is in control should be made. If algorithms can rewrite themselves and learn from mistakes, and the police officers follow algorithms ‘blindly’, who is in control in the end? In this sense Rienks stresses the importance of policing as a human job in which the algorithm can guide in a way. But eventually an algorithm should not be the final decision maker, but the police officer (Rienks, 2015, p. 137-140).

Another risk that is not mentioned often in the literature, but still is important to take into account, is the risk of privacy breaches. Predictive policing can certainly impact the personal life of individuals by affecting their direct living area. One extreme example is the city

of Chicago, where predictive warrants were used to search houses of frequent offenders. Another part of this privacy related risk is what kind of data a data scientist want to include in his algorithm. Some data might be very useful to predict crime, but it might just as well be data that is too personal to use (Smit & de Vries, 2016, p. 18).

Rienks also observes these privacy concerns related to predictive policing. He indicates that it is clear that when actions, such as searches and patrolling, are being linked to the prediction of crime in a specific area this means that individuals are being targeted because of their presence in a certain location. He admits that this targeting can be a big intrusion into the privacy of citizens (Rienks, 2015, p. 140). Furthermore the risk of creating some sort of ‘big-brother’ is highlighted in the context of privacy. It is possible to add in all kinds of personal characteristics into predictive policing algorithms to make them more effective. However, this does carry an inherent risk of too much digitalization of personal information which could then lead to privacy breaches (Rienks, 2015, p. 146).

3. Methodology

3.1 Research Design

The research method that I will use is a qualitative design that makes use of in-depth interviews containing open-ended questions. I will use a holistic single case study, namely the case of the Dutch Crime Anticipation System (CAS). This case will be discussed further in the case selection. I will conduct this case study by sticking to outlines provided by Robert K. Yin (2018) in his book ‘Case Study and Applications.’ To answer my research question: ‘*How does the Dutch police perceive the risks associated with predictive policing?*’ Following this research question a unit of observation and a unit of analysis can be appointed. My unit of analysis will be the Dutch police, while my unit of observation will be the risks of predictive policing that are perceived by the Dutch police (see figure 1).

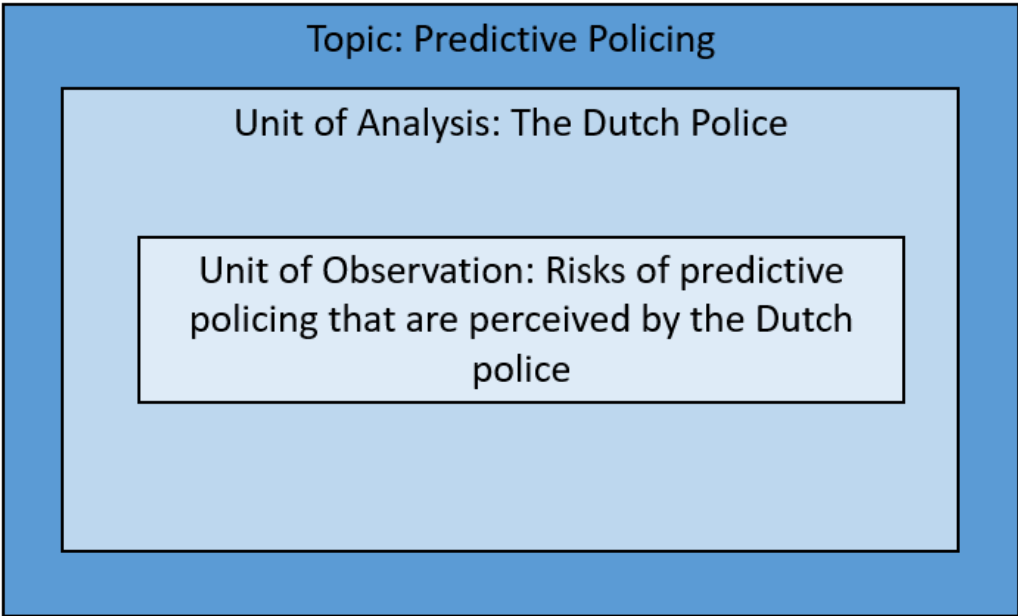


Figure 1, Single Case Study.

I will conduct interviews with Dutch experts in the area of predictive policing. My design will therefore consist of elite interviewing. My research will revolve around the ways in which the Dutch police perceive the risks of predictive policing. This will be done by making a comparison between the risks that are highlighted in both academic literature and police literature on the one side, and risks that are mentioned in the interviews. In the literature several important risks are highlighted. I will operationalize these risks in paragraph 3.3.. Following my research, these operationalized risks can be either validated or diffused by the results of the interviews. It will be interesting to analyse the data from interviews in relation to the existing theories on the risks of predictive policing.

3.2 Case Selection

In order to carry out my research I will use a holistic single case study. This is due to the fact that my research question tries to explain how the Dutch police perceives risks of predictive policing. This is a ‘how’ question, which means that my research will be an in-depth research that will try to identify the risks that the police perceives. Questions that focus on how something occurs are more explanatory, a case study is best suited for this kind of research (Yin, 2018, p. 3-5).

To be specific I have chosen for a holistic single case study. This entails that my research will only focus on one case with one unit of analysis. My case will be the Crime Anticipation System (CAS), a predictive policing system that is used by the Dutch police which is my unit of analysis. This choice for a single case has two main reasons. First of all there only is one relevant predictive policing system that is in use in the Netherlands, this is the CAS. I think that my research has more value if I solely focus on this case and do not try to compare to other cases. This is because there has not been much research into this particular case, since it has only been implemented in the Netherlands in 2017. Therefore it is better suited to first explore this case instead of comparing it to, for example, predictive policing systems in the United Kingdom or United States. The second reason is a practical one. Due to the timeframe in which this thesis has to be conducted it is not feasible to go in-depth into more predictive policing cases. This is why I have chosen the most important and relevant one to answer my research question.

I want to examine and assess the perception of the Dutch police on the risks of predictive policing. The CAS had developed from 2014 onwards and it is currently being used in more and more cities after a successful pilot. My choice for the CAS is because it is the best and most relevant example of predictive policing practices in the Netherlands. Furthermore it is the only one that is being implemented at this very moment, which makes it a logical and interesting case to study.

3.3 Conceptual Framework & Operationalization

Within my research question: *'How does the Dutch police perceive the risks associated with predictive policing?'* concepts have to be defined and indicators for measuring risk must be made clear. I will use Karppi's definition of predictive policing, mainly because it is the one that covers every aspect of predictive policing while the definition remains understandable: *'predictive policing is a policing model that uses algorithmic analysis of "criminal behaviour patterns" together with three data points, "past type, place and time of crime" to provide "law enforcement agency with customized crime predictions for the places and times that crimes are most likely to occur'* (Karppi, 2018, p. 1). Next to a definition of predictive policing it is important to define the concept of risk perception. This has to be done before indicators can be established on how to assess the risk perception of the Dutch police. I will use the definition of risk perception by Moen et al: *'Risk perception is the subjective assessment of the probability of a specified type of accident happening and how concerned we are with the consequences'* (Moen et al., 2004, p. 8). The main reason for using this definition is because it is clear and applicable to organizations as well next to individuals. Since I want to assess the risk perception of the Dutch police this is an important factor to take into account. The conceptual framework of this thesis is visualized in Figure 2.

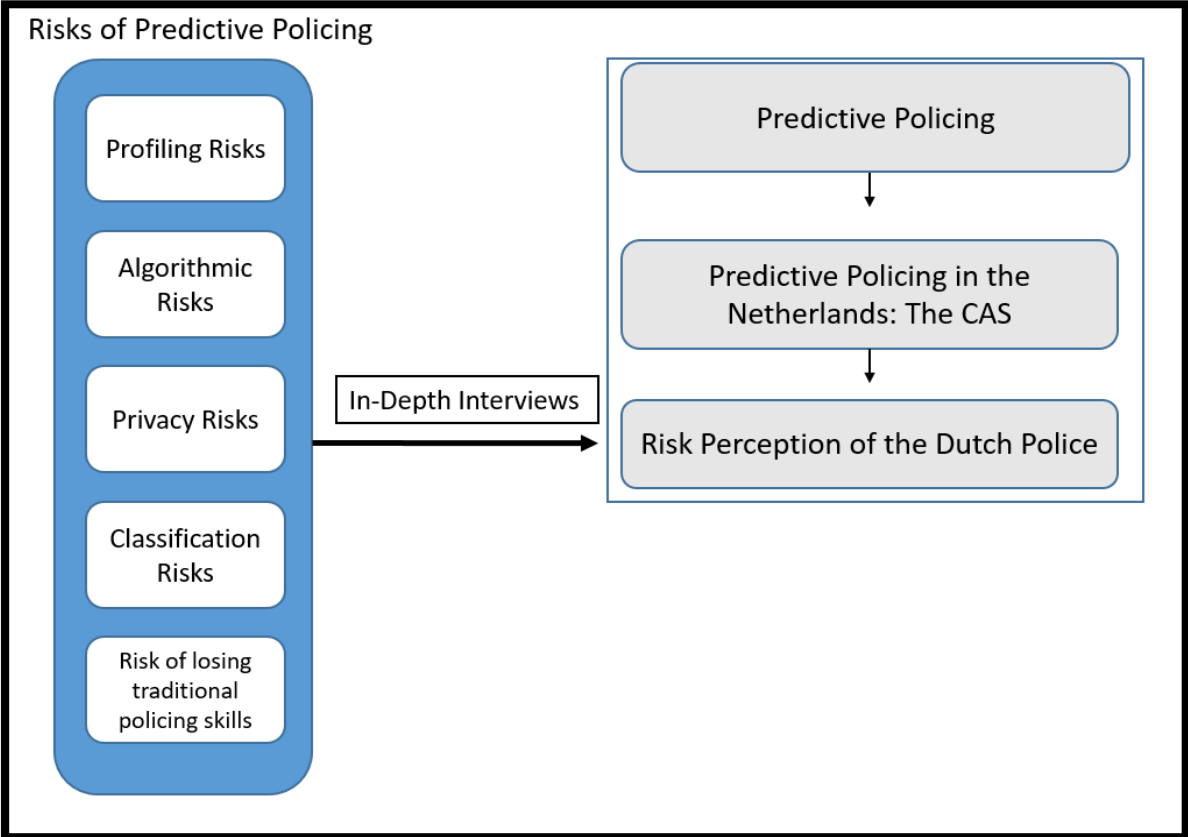


Figure 2, Conceptual Framework.

So how will this risk perception be determined? From the theoretical framework several potential risks of predictive policing can be identified. The most relevant and studied risks of predictive policing, as they are explained and mentioned in the literature, will be my indicators to assess the perception of risk. The risks that are mentioned in the literature are: profiling risks (Karppi, 2018) (Koss, 2015) (Kirkpatrick, 2017), algorithmic risks (Barocas et al., 2017) (Kirkpatrick, 2017) (Rienks, 2015), privacy risks (Smit & de Vries, 2016) (Rienks, 2015), classification risks (Fyfe et al., 2018) (Bowker & Star, 1999) (Koss, 2015) and the risk of losing traditional policing skills (Smit & de Vries, 2016) (Rienks, 2015). These risks are explained extensively in the theoretical framework. A definition for each of these risks is given in Table 1. Table 1 provides a deeper insight as to what is meant with each risk and with what indicators these risks can eventually be identified in the in-depth interviews. The indicators, words that are closely linked to the definition of the risks, will be used specifically in the analysis of the interview transcripts. They can indicate in which part of the transcript something is being said about a specific risk. In this sense indicators will help to quickly identify paragraphs in the transcripts that are tied to a certain risk.

Risks	Definition	Indicators
Profiling Risk	The risk on selecting and treating people based on personal characteristics such as race, skin-color or heritage (Rienks, 2015, p. 142).	<ul style="list-style-type: none"> • Profiling • Discrimination • Minorities • Ethnicity • Race
Algorithmic Risk	The risk on the production of discriminatory or faulty outputs from algorithms due to machine learning, construction errors and/or wrong datasets (Barocas et al., 2017).	<ul style="list-style-type: none"> • Machine learning • Bias • False Positives • Feature selection • Incorrect data(sets)
Privacy Risk	The risk of impacting the personal life of individuals by affecting their direct living area through predictive policing systems (Smit & de Vries, 2016, p. 18).	<ul style="list-style-type: none"> • Privacy • Transparency • Societal concerns • Personal life
Classification Risk	The risk of black boxing classifications which makes classifications both potent and invisible. This could lead to the exclusion of the public from	<ul style="list-style-type: none"> • Black boxing • Classification • Categorization

	policy participation because they have no insight in these classifications (Bowker & Starr, 1999).	
Risk of Losing Traditional Policing Skills	The risk of losing traditional policing skills, such as judging individual incidents according to own intuition, because of too much reliance on guidance by algorithms (Smit & de Vries, 2016, p. 16).	<ul style="list-style-type: none"> • Reliance on algorithms • Losing of skills(set) • Intuition • Final decision maker

Table 1, Risks of Predictive Policing.

This research aims to assess how the Dutch police perceives these risks. This perception will be assessed by analysing which risks are mentioned in the interviews with experts of the Dutch police and in what kind of context. Through asking open-end questions about these risks the answers of these experts can be linked to each potential risk of predictive policing. The experts might stress the importance of some risks, but on the other hand might not be overly concerned by other potential risks. Another interesting factor that could come forward out of this research, is that the police might indicate completely different risks that have not been mentioned in the theoretical framework. This could prove that, on a practical level, there are different risks than the ones that the literature deems to be the important ones. The word importance implies that some are more or less important than other. That is not the case, in the theoretical framework it has already been argued that it is not about how often risks are named, instead it is about how they are examined in the literature. With ‘deems to be important ones,’ all the risks that are mentioned in the literature are meant. The fact that the literature mentions and elaborates upon them means that they are important, to the authors of the literature on predictive policing at least. The real life situation, on a practical level, could expose other risks that have not been mentioned in the literature.

3.4 Data

My main method of gathering data has been in-depth elite interviews. This data on the risk perception of the Dutch police is gathered through elite, semi-structured interviews. The fact that they are semi-structured means that there is no set list of questions that are asked to each interviewee in the same way. There were some standard questions, but that the idea was to ask specific follow-up questions to try and stimulate the interviewees to provide additional information. This is done in order to minimize the danger of me bringing up risks that the interviewee did not even think about before they heard my questions. A possible limitation of this method is that the interview questions might still have contained hints and could have been

too much of a guidance towards a certain answer. This will be more extensively in the limitations of the research.

I have conducted six interviews in total, some of them have been established through snowballing. My thesis supervisor, Dr. Niculescu-Dinca, established the initial contact with Rutger Rienks, an expert of the Dutch police. By asking him for more contacts I have managed to get more connections into the pool of data experts of the Dutch police. Next to this line of investigation I have also contacted certain experts myself. In this sense I had two lines of investigation that I explored next to each other. This provided me with enough options to gather my data. My aim was to have six in-depth interviews and in total I was able to conduct all six of these in-depth interviews. It was important that each interviewee had clear knowledge about Dutch predictive policing methods. Knowledge of the CAS would be even more valuable, since it is the most important predictive policing system at the moment. Each of my six interviewees can be considered an expert on the topic of predictive policing and all of them can be considered authoritative representatives of the Dutch police as well. This last part is important because the conclusions of the research will be drawn on an organizational level. This means that the interviewees need to provide an authoritative and correct representation of the police as a whole. It is difficult to do this with six interviewees, but it can be done. Mainly because the CAS and predictive policing within the Dutch police are surrounded by a small group of experts. In my selection I tried to mix in interviewees from the 'higher' level of predictive policing, such as the designer of the system, the national coordinator of the system and the individuals behind the national evaluation of the CAS. Besides that I also, for example, looked at interviewees on a regional level. The reason behind this is to add in as much diversification as possible in the knowledge and background of my interviewees. This ensures that the pool of interviewees, as a whole, can be considered a correct representation of the thoughts of the Dutch police as a whole on predictive policing. My initial group of people to approach within the police, that had enough knowledge and understanding of predictive policing, was a small one. Therefore I think that six out of this pool can be considered an authoritative sample for the entire Dutch police when it comes to predictive policing. Especially because it includes the most important people behind the most significant predictive policing system.

The first interview took place with Rutger Rienks, he is the former Head of the Business Intelligence and Quality department of the National Police. In this function he was closely involved in the shaping of the CAS and the first steps of the system. Next to that he also wrote an important piece on predictive policing in the Netherlands: '*Predictive Policing; kansen voor een veiligere toekomst.*' My second interviewee is the designer of the CAS, Dick Willems. As

a data scientist working for the National Police he developed the system single handed, which is why he has some unique insights into the system. My third interview was with Bas Mali, a researcher for the Police Academy. He is a very relevant source as well because he was co-responsible for writing the evaluation of the national pilot of the CAS, called: '*Predictive Policing: lessen voor de toekomst; Een evaluatie van de landelijke pilot.*' I also managed to interview his partner, with whom he wrote this evaluation, Mariëlle den Hengst. Next to being responsible for the evaluation, she is the head of the Real-Time Intelligence lab of the National Police. My fifth interviewee was Hans Grübe. He is a policy officer of the biggest police region of the Netherlands, Oost-Nederland. He was the head of the implementation of the CAS in this region, which accounts for 27 police teams. In this function he dealt and still deals a lot with predictive policing and the CAS. My final interview was with René Melchers, he is the current head of the Businesses Intelligence & Quality department. However, he is responsible for the nation-wide rollout of the CAS. This means he is a key stakeholder in the national implementation of the system. This overview of the interviewees shows that they have all worked with the CAS in different manners, but can be considered experts in this field. For this reason the selection of interviewees is a good representation of the Dutch police, which is why it can be used as a source to assess the risk perception of the Dutch police.

The goal was to conduct enough interviews to have a sample of interviews in which information is started to repeat itself, which indicates a pattern. After this saturation I analysed the interviews by transcribing the voice-recordings of the interviews. These transcripts will be unfocused ones by nature. This means that they will contain solely what has been said, it does not contain the tone or way in which things have been said. Afterwards I will develop a coding scheme to analyse in detail what the experts mention on the potential risks of predictive policing. The coding scheme is theory driven, which means that it has emerged from the existing body of knowledge and theories. In this particular case the risks that have been mentioned in the literature. A coding scheme will help in distilling relevant information from the interviews. I will colour code the different risks and highlight these in my transcripts. In this way I can link different parts of each interview to a certain risk. This will indicate which risks are perceived in what manner.

3.5 Limitations

My research focuses around elite interviews. One of the paths that I am exploring is through snowballing. This might lead to bias within the group of interviewees, since they all know each other and are from the same ‘circle.’ I have minimized this by following a second line of investigation that I conducted on my own account. However, it is still possible that, because of the lack of people that have expert knowledge about the CAS, I will still encounter people from the same circle of experts of the Dutch police. Next to this problem another problem concerning the reliability of my research could be bias. With interviews you are never certain of a certain bias within the interviewee. They might have their own reasons to participate in interviews, such as pushing a certain agenda. Which is why not everything they say should be considered to be their honest opinion for the full hundred percent. In this specific case I am talking to experts from the Dutch police about risks. This means that they could be biased in the sense that they will not be as critical as they could be on their own predictive policing system. In my interviews I have not encountered clearly biased answers, which leads me to believe that the interviewees have answered the questions as honest as possible but this should not be taken for granted. On top of that problems could occur from the fact I have not added in enough triangulation within my interviews. This means that I should interview experts with different characteristics, age and gender could be some of those characteristics. Out of my six interviews only one is with a female interviewee, this could lead to a certain bias. I do think the age of all interviewees is equally distributed.

I have conducted semi-structured interviews. This means that I did have some standard questions to spark a discussion with the interviewees, one of them being a question such as: *‘What do you see, as an expert, as the most important risks in predictive policing systems such as CAS?’* While I asked some standard questions to each interviewee, the idea was to ask follow-up questions to stimulate the interviewees until they provide sufficient information. The goal was to get the interviewee to mention certain existing or new risks without me bringing them up. This would ensure that they perceived the risks themselves, instead of being led to a certain risk by my question. Although this was necessary sometimes, for example with a sensitive risk such as profiling, most risks have come directly from the interviewees themselves without me giving them a hint. A problem that does come with this method, is that no interview really is exactly the same. The order of topics, the number and nature of questions differs each interview. Finally, since I am using a single case study, this means that my external validity will not be as high as it would be with a multiple case study.

4. Analysis

As mentioned in the methodology, I will use a coding scheme (Table 1) to link each risk that is observed in the literature to data that is gathered from interviews. The most convenient way to do this, is via a color-coding. Each risk gets its own colour, after which parts of the text in each interview are highlighted with that specific colour if the risks are mentioned. A factor that must not be overlooked is the fact that the interviews might contain new risks that have not been mentioned in the literature and therefore have not been included in the coding scheme.

Risks	Definition	Indicators
Profiling Risk	The risk on selecting and treating people based on personal characteristics such as race, skin-colour or heritage (Rienks, 2015, p. 142).	<ul style="list-style-type: none"> • Profiling • Discrimination • Minorities • Ethnicity • Race
Algorithmic Risk	The risk on the production of discriminatory or faulty outputs from algorithms due to machine learning, construction errors and/or wrong datasets (Barocas et al., 2017).	<ul style="list-style-type: none"> • Machine learning • Bias • False Positives • Feature selection • Incorrect data(sets)
Privacy Risk	The risk of impacting the personal life of individuals by affecting their direct living area through predictive policing systems (Smit & de Vries, 2016, p. 18).	<ul style="list-style-type: none"> • Privacy • Transparency • Societal concerns • Personal life
Classification Risk	The risk of black boxing classifications which makes classifications both potent and invisible. This could lead to the exclusion of the public from policy participation because they have no insight in these classifications (Bowker & Starr, 1999).	<ul style="list-style-type: none"> • Black boxing • Classification • Categorization
Risk of Losing Traditional Policing Skills	The risk of losing traditional policing skills, such as judging individual incidents according to own intuition, because of too much reliance on guidance by algorithms (Smit & de Vries, 2016, p. 16).	<ul style="list-style-type: none"> • Reliance on algorithms • Losing of skills(set) • Intuition • Final decision maker
New Risks	Risks that have not been mentioned in the Literature	<ul style="list-style-type: none"> • N/A

Table 2, Colour-coding Scheme of each Risk

Now that each risk can be linked to the interview transcripts, the results can be observed. This will not happen with colour-counting. Since I have conducted in-depth interviews, I will be focusing on the actual contents of the interviews, instead of simply counting how many times a certain word has been said. I will examine each paragraph in the interview transcripts that is linked to either an existing risk or new risk and see how much emphasis is placed on the risk. The identification of these paragraphs mainly happens through using the indicators. If an indicator is present in a piece of text, this part of the text will be examined to see if there indeed is data on the specific risk that is tied to the indicator. Of course, there are no indicators for new risks, which is why it could be a problem to identify these. I will try to identify them by, after I have linked all existing risks to certain parts in the transcripts, examining the transcript as a whole and observe the parts that have not been assigned to an ‘existing risk.’

Firstly it is important to see whether the interviewee observes the risk as one that is present within the Dutch predictive policing system. If the risk is present, it is necessary to examine in what way it is present and how the police deals with the existence of the risk. The most logical and transparent way to conduct the analysis is by elaborating on the results for each risk. This will happen in the order in which they are noted down in the colour-coding scheme. This means that the first risk that will be examined is the profiling risk, the concluding risk will be the new risks that are possibly mentioned by interviewees. I will handle the analysis of each individual risk in the same way. I will give a brief introduction of the risk, contextualize it and then the risk will be analysed with findings from the interviews. This will mainly happen through quotes, which can be linked to specific risks.

4.1 Profiling Risk

The profiling risk is one that is defined as the risk on selecting and treating people based on personal characteristics such as race, skin-colour or heritage (Rienks, 2015, p. 142). In the literature on predictive policing systems in relation to profiling risks, it became clear that there were a lot of arguments that could be made for this specific risk. In the interviews questions have been asked as well to the police experts to examine how they look at this risk. Is it a clear one that they pay attention too? Or is it a non-existent risk in the Dutch case because of certain built in safeguards? The interviews were analysed by looking for indicators such as profiling, discrimination, minorities and race. Whenever an indicator was found this, the paragraph in the transcript that accompanied it was examined.

In every single one of the interviews, at some point, the debate on profiling and discrimination came up. This is why certain quotes can be linked to this issue of which some directly address the profiling issue. Bas Mali, when asked if he had noticed anything in relation to profiling in the CAS pilot, answered: *‘No. It does use selection. Discrimination is selection on the basis of improper grounds. In this case the system does make a selection, but it is based on proper criteria. If more crime happens in a certain area it is logical to expect more crime there’* (Mali, 11th December 2018). This is supported by Den Hengst, she argues that *‘Police officers know for example that there are certain areas where there are more crimes than in another area. When the system indicates that area they will say: ‘there is more crime so it is logical we are directed to that region’’* (Den Hengst, 6th December 2018). In contrast to what one might expect, Bas Mali indicates that predictive policing systems might even cause less profiling. This is because he states that officers often take action based on their instinct, which might contain some form of bias. With the CAS you might have less human bias because it selects on certain variables instead of instinct (Mali, 11th December 2018). Dick Willems agrees on the fact that there do not seem any ethical risks within his system, he argues that *‘Usually people have these questions it’s about ethics, I don’t really think there’s an ethical problem in what we’re doing. Sometimes people ask me “what if the patrols are going to neighbourhoods with a high number of Moroccan people?” Then they’re probably going to go there because crime is pretty high there, so you’re going to go there for the same reason that you would go to any other area in Amsterdam’* (Willems, 11th November 2018). This illustrates that Willems does see the risk of profiling, but he does not see it as something that could occur within the CAS. An important factor in this, is that he states that: *‘CAS is location-based, it’s not person-based, so it’s kind of different from the high-risks that are usually in the news. You know, there you see that you have some kind of inter-mediating available which basically means that you are ethnically profiling. Because we use locations I don’t think that’s really going to be a big issue’* (Willems, 11th November 2018). The quote clearly indicates the reason Willems does not see ethical issues as a big problem in his system.

Kirkpatrick stated that, based on historical data input, the risk is that poor or minority communities are overrepresented in predictive policing systems because they often live in the areas that are policed the most (Kirkpatrick, 2017, p. 23). This seems to be countered by the argument that police has always been in those areas. But, Kirkpatrick does seem to have a point. Hans Grübe indicates some variables that the system takes into account, some of these are the types of buildings in a neighbourhood, the income of people, and rental property versus owner

occupied homes (Grübe, 14th December 2018). This does show that some variables do correspond with income. However, Grübe does state that: *'The system does not see if a suspect is white, yellow, black or red. It only shows the risk profile of certain areas and does not take nationality into account'* (Grübe, 14th December 2018). One could state however, that income as a variable could lead to discriminatory effects in poor areas, thus leading to discriminatory effects based on lower incomes. Koss (2015), for example, argued that predictive policing methods in the U.S. often attach the high-crime label to low-income minority neighbourhoods. Melchers agrees that if burglary correlates with low-income minorities the system would show this relationship: *'If low-income neighbourhoods would have a relation to burglary, then the system would indeed show this relation. Data science is a very difficult job because these kinds of issues'* (Melchers, 9th January, 2019). In this sense Koss' statement on low-income minorities that could be discriminated does seem correct in the case of the CAS. However, Information officers also look at the maps that the CAS provides them with to assess if these are correct. If a low-income area would not have a lot of crime, but would pop-up on the CAS maps, the information officers could correct it. This is what Melchers stresses as well: *'Information officers always have to indicate why we are patrolling a certain area'* (Melchers, 9th January, 2019). He states that it is not enough if they just say, they CAS maps indicated it, and they have to develop their own analysis as well, outside of the CAS maps.

In this regard, a big part of the reason why the CAS is not perceived to be discriminatory, is because it focusses on locations, instead of persons. This means that it, fact wise, shows the location with the highest risk of a burglary for example. As Rienks indicates: *'We don't have predictive solutions yet that go out to people, they look after places. Of course you want as little features related to people as possible, you don't want any predictions dealing with people I would say'* (Rienks, 9th October 2018). Dick Willems, the man behind the CAS feels the same way about it. He argues: *'I don't think people realize how much work it is to use lists on certain kinds of individuals in an ethical way. That cannot be done I would say'* (Willems, 11th November 2018). It is good that people behind the CAS are thinking about these types of issues, Den Hengst also indicates that certain arguments on profiling are based on evidence. She states that: *'In the CAS, they were looking at all sorts of factors which might predict crime and one aspect that was a great predictor was ethnicity of persons. Well we don't want that in the system, but it correlates very highly with a certain geographic area. So if an area is an input in your system, then you're very much profiling, as if you would use ethnicity in the system'* (Den Hengst, 6th December 2018). This quote illustrates that there is a thin line between predicting locations and predicting on the basis of ethnicity. However, it must be said that it is clear that

this certainly is not meant to be a factor of the system, which is why areas are not an input but an output. The quotes of Rienks and Willems also indicate that it certainly is not the intention or idea that personal characteristics are included in the CAS. Melchers concludes that there will always be a debate about variables in relation to profiling: *'It does not matter long you make your list of variables, you will always have a discussion with citizens and police officers about which ones you have used and if they are correct'* (Melchers, 9th January, 2019).

The paragraphs above indicate that all interviewees do perceive the problem of profiling as a serious one, giving the fact that they have all given explanation on the risk and have clearly thought about it in relation to the CAS. The main arguments against profiling occurring in the CAS are that the system selects on certain specific indicators, and that improper personal characteristics are not included in this assessment. Furthermore the system is only able to predict locations on a map. The interviewees indicate that this does happen based on historical data, but that this is logical. If area X has always had a lot of crime, it makes sense for the police to be in that area. It would be weird if they did not do anything with this historical data. Another point that ties into this is that the police patrolled those areas as well before the use of the CAS, because some areas have been known as high-risk areas for a longer period of time already. One could argue that the use of a variable such as income in the system could produce discriminatory effects, but this is mitigated through the use of information officers who still have to interpret the data that CAS hands them. All in all the Dutch police clearly does perceive this risk, but not as the most serious one. Especially because of the nature of the CAS, it selects on locations, not on personal characteristics. The only argument that could be made, is that it also takes variables income and housing into consideration.

4.2 Algorithmic Risk

The algorithmic risk was described as the risk on the production of discriminatory or faulty outputs from algorithms due to machine learning, construction errors and/or wrong datasets (Barocas et al., 2017). This risk is a technical one and deals with issues such as machine learning, bias, false positives and incorrect data (sets), which is why it is important to look at the perception of people such as Dick Willems and Rutger Rienks, mainly since they are the people behind the technical parts of the CAS. Especially Dick Willems will probably be the best informed person in the Netherlands about these risks. Asked on the biggest risks of predictive policing, Rutger Rienks mentions one that is an algorithmic risk: *'What we need to take care of, I think at least how to deal with the false positives. So, if the computer is saying*

something which is not correct, then you should always be aware of the fact that it might be not correct. Even when the module performance can be up to 90% or so, the chances of being 100% correct in this outcome is 0, so there's always a chance that you are wrong. Although that goes for human observation as well' (Rienks, 9th October 2018). This indicates that the police have a clear perception of algorithmic risks. Dick Willems also mentions this risk, but he adds that: *'The actual decision-making is human, it's not by Artificial Intelligence or something'* (Willems, 11th November 2018). This is a clear example that illustrates that the police did consider this a risk, and therefore did not incorporate machine-decisions into the algorithm or their ways of working.

Barocas et al. mentioned the risks of machine learning which produce faulty outputs because the data that they have been 'trained with' could have been faulty, biased or unfair (Barocas et al., 2017, p. 680). The CAS uses supervised machine learning. Dick Willems gives two reasons why he decided to use a certain kind of machine learning: *'You can do supervised learning really complicated, we do not do that for two reasons. One is you can't see what's going on anymore, the other one is that it takes a lot longer to build'* (Willems, 11th November 2018). Although the second reason is a practical one, the first one indicates that algorithmic risks, such as using wrong data sets to train algorithms, have been taken into account in the CAS. Den Hengst does see some risks in this area. She states that: *'Another risk I see is that when you put police officers in a certain area, they will see things in this area. It will enter the system, and these kind of data influences the prediction, so it will enforce itself. Because you get a lot more reports on that area because you are more frequent there in that area, and you will also get the prediction in that area. But it's not really being researched yet whether that's really happening, but it's a risk'* (Den Hengst, 6th December 2018). This relates to the risk that focusses on how the CAS could create certain high-risk areas, simply because it sends out police officers to certain locations more often. The fact that Den Hengst mentions this however, indicates that the Dutch police does not overlook these kinds of factors.

Melchers also mentions this risk: *'With some types of crime we use data that gathered ourselves to make a prediction, for example pickpocketing or fake dope-dealing. If we put that in the system the prediction will be a confirmation of our own patrol.'* When asked how this was prevented in the CAS he indicated that it was done as follows: *'by not telling the system to make predictions on themes that have collected data in this way'* (Melchers, 9th January, 2019). This means that Melchers agrees on the fact that you could get a self-fulfilling prophecy if you do not handle your data carefully. This prophecy can be avoided by not applying the CAS to

certain types of crime that the police observes themselves. For example, if they go hunt on pickpockets, they will find them and put the data on where they arrested pickpockets in themselves. If there is a burglary a civilian comes to the police. In this regard the data is brought to the police, instead of them 'fetching' it. This is the type of data that, according to Melchers, the police use to make prediction. It is also the reason that the construction of high-risk areas is prevented (Melchers, 9th January, 2019).

This was also brought to light by Hans Grube. When responding to the creation and use of algorithms he states that *'A point of the system is that it is a general algorithm that is used for multiple specific crimes. There are themes that do not lend themselves for this general algorithm. You should have a specific one'* (Grube, 14th December 2018). This is an issue that is also recognized by Dick Willems. He adds that for some crime types it is more difficult to use predictive policing systems such as the CAS, than for others. Muggings and robberies are a lot harder to predict than burglaries. Mainly because they only take a very short period of time, you do not have a big window of opportunity to catch criminals. A quote that provides further context is the following one: *'We should avoid using predictive policing for some types of crimes indeed. Or you should make an in depth study of the dynamics of that crime type to make an analysis. CAS as it is right now should not be used for those types of crime'* (Willems, 11th November 2018).

A risk that Kirkpatrick indicated regarding the historical data that predictive policing systems use, is that it could be a misrepresentation. He argued that crimes could occur in certain areas where the algorithm does not see any incentive to increase policing and that in this sense the system could miss what is really happening out there (Kirkpatrick, 2017, p. 23). Dick Willems indeed does see unreported crime as a big problem of the CAS system. When asked if this was a problem he said the following: *'Yes. Especially because we don't know how much unreported crime we have. Muggings are often not reported for example because people know the perpetrator. I also think that the processes that we have in place can alleviate that problem in some way. If you have a good information specialist he doesn't only look at what's registered, but also talks to his officers and the community'* (Willems, 11th November 2018). This indicates how it is difficult to make an accurate prediction, which is why it is good that Willems immediately acknowledged this risk. Hans Grube supports this notion by endorsing that it is difficult that the system does not take unreported crime into account. Mainly because in his area of operations, rural areas, sometimes there is not enough volume for the CAS to make a prediction (Grube, 14th December 2018). Put simply, sometimes there is insufficient historical

data to make a prediction. Unreported crime obviously is a problem in the sense that this is not taken into account in the prediction, or even leads to a situation in which no prediction can be made. It does seem like attempts are made to mitigate this specific algorithmic risk, for example by using information from community officers as well when making sense of predictions.

Barocas et al (2017) also indicate that construction errors could be present because of wrong selection choices by individuals who instruct and create algorithms. They call these choices 'feature selection.' If selection criteria within an algorithm are badly constructed this can have severe implications for the model. Rutger Rienks ties into this by stating that: *'The one who designs the module was the one who actually sort of was responsible for the outcome, right? So, of course it is a huge risk that a data scientist is falling in love with his own module just like painters, they always say. But, well, a process should be in place that looks after that the creation of the module; at least two data scientists need to look at it and it should also be evaluated by a third party before it actually is brought into production'* (Rienks, 9th October 2018). Den Hengst also addresses this specific issue by stating that: *'Understanding what the model does with the data and how the model is trained is very important for the strategic level of the police to decide yes we will implement it, or no we won't'* (Den Hengst, 6th December 2018). These quotes illustrate that the police put thought into the argument, made by Barocas et al., which focusses on the selection choices on which the system is trained. The use of multiple data scientists, as indicated by Rienks, to see whether modules are faulty or not is very important in mitigating construction errors.

All in all the police and the people behind the system have clearly thought about algorithmic risks. Rienks immediately identified false positives, an algorithmic risk, as one of the two risks that are most concerning. Dick Willems also noticed some algorithmic risks such as unreported crime that remains undetected, but was also very quick in mentioning counters to those risks such as supervised machine learning. Hengst and Melchers also mentioned risks such as the self-fulfilling prophecy in creating high-risk areas and even more importantly, how this creation can be avoided. This illustrates that the police has thought about a lot of options regarding algorithmic risks. It indicates that the Dutch police perceives algorithmic risks seriously and target them specifically with counter measures. They do need to pay attention to risks like the possibility of faulty predictions, which is a risk that will probably always be present. Another one is the risk that one algorithm could be used for all sorts of crimes, while sometimes one algorithm should be developed and used for one specific crime. It is important for the Dutch police to keep this in mind. Finally, the Dutch police also observes algorithmic

risks such as construction errors, but anticipates these by using multiple data scientists to double-check whether modules are faulty.

4.3 Privacy Risk

The privacy risks were also mentioned in the literature. Although they were not mentioned that extensively in the literature, a lot of interviewees did voice their opinions in it quite often. Privacy risks have been defined as the risk of impacting the personal life of individuals by affecting their direct living area through predictive policing systems (Smit & de Vries, 2016, p. 18). Factors that are closely related to this risks are transparency of predictive policing systems, societal concerns on these systems, personal data and intrusion on one's personal life.

A part of this privacy related risk is what kind of data a data scientist wants to include in his algorithm. Some data might be very useful to predict crime, but it might just as well be data that is too personal to use (Smit & de Vries, 2016, p. 18). Willems touches on this subject by stating that: *'From the data set that we use alone you can't follow through or drill down to any specific household or any specific persons. We do use some personal data, for example, we know if a square is close to a known offender, but we can't tell from the dataset where that address is located'* (Willems, 11th November 2018). This means that he does perceive and recognizes the risk, but he does not see it as a plausible one in his system. Rienks sees this risk as well, he states that the second big risk of predictive policing is the privacy related: *'Another thing is that you might try to module criminal phenomena that, well, are sort of not socially accepted. So, that's more on the ethical level where, you know, the modules that we have been creating so far are more about the ranking of locations rather than the ranking of persons. When you start developing modules that creates prediction about human beings, do we socially accept it? Probably the answer is no, so I think we should not go that way'* (Rienks, 9th October 2018). This is a very good example of how the police perceives the risk. It is clearly indicated by Rienks that it is not the way to go because the society will not accept it. He also adds that predictive policing is a way to preserve privacy for most and expose those who are meeting some select criteria (Rienks, 9th October 2018). Another way in which the police tried to mitigate privacy related risks is by using privacy by design. Den Hengst elaborates: *'Since 2012 the police have embraced privacy by design, it should be from the beginning part of your focus when you look at the problems of the system. The policy is that there is privacy by design.'* However, it is also important to note that she adds a side-note: *'although it is a policy, it is not*

always followed by everyone from the start' (Den Hengst, 6th December 2018). This all does indicate that then police take it up very highly, but there does seem some room for improvement. Regarding this improvement Melchers mentions that he likes it that the system is bringing up privacy related questions. He indicates that: *'If we invest in CAS, as the Dutch police, we should be able to explain where taxpayer's money is going. So the added value of this discussion is that we also have to explain what CAS is. This means that we have started a discussion within society on the use of algorithms and their possible flaws. Is there discrimination or bias in it?'* (Melchers, 9th January, 2019). This illustrates that the Dutch police does care about transparency a lot. Melchers also mentions that the police has reached out to the media a lot themselves to explain CAS. That implies that they care about being open to the public about the use and benefits of CAS.

One could still argue that privacy does not have to be person-related, but it can also happen location-wise. The privacy of people can still be affected because a direct living area is targeted. In the interviews a point that was put forward, regarding privacy, was how the interviewees thought that predictive methods might lead to a change in the trust that citizens have in the police. One might expect that the fact that the police is using certain computer guided algorithms in order to patrol more efficiently, could lead to some questions regarding the big-brother effect. This creation of the 'big-brother is watching you' is highlighted often in relation to privacy. Rienks argues, in his book, that adding all kinds of personal characteristics into predictive policing algorithms to make them more effective, carries an inherent risk of too much digitalization of personal information (Rienks, 2015, p. 146). When asked about how predictive policing could affect the general trust of citizens in the police, the answers were contrary to what one might expect. Rienks argued that predictive policing might even increase the trust in the police, because *'You can at least explain why some action took place. Sometimes people think something looks suspicious. But this creates a slippery slope, what is suspicious? I think you can objectify this by putting algorithms in place'* (Rienks, 9th October 2018). Dick Willems agrees on the stance that it will not be that big of a problem, as long as predictive policing is done in a neutral way. Another addition is made by Hans Grube, he thinks that *'If you tell society, their response will be positive. People think: 'I want less burglaries in my neighbourhood, I do not really care that much about how the police targets it.' 'I even think that it will add value for the citizen if you tell them that you are doing it based on clear information'* (Grube, 14th December 2018). This is in line with Rienks, both argue that instead of being negative, privacy-wise, it can be seen as a positive too for citizens. By clearly stating

that you are doing things based on a certain system you can also create trust in the police. Bas Mali argues that the risk of selecting on improper grounds might even be greater if a human does it, simply because they often work on the basis of routine actions or gut feeling. Therefore he thinks that systems such as the CAS might actually help regular police officers in explaining the reasons to the citizens behind police patrols in a certain area (Mali, 11th December 2018).

One of the main takeaways from the points that the interviewees made regarding privacy related risks, is that sometimes they even see it as a bigger risk than the literature. In the literature it was mentioned, but less than for example the profiling risk. In the interviews on the contrary side, it became clear that the police does see this as an important factor when developing and working with systems such as the CAS. Their risk perception is bigger in this sense. Therefore they target this risk by using measures such as privacy by design and using data that is not connected to specific persons. Interviewees also indicated that personal related data is not the way to go. Furthermore, the algorithms were seen as a reason to create transparency for people on the street instead of hiding it. Because police officers could indicate that they were in a neighbourhood based on an analysis. Additionally, like Melchers mentioned, the police actively went to the media to show the CAS. This illustrates that they want to be as transparent as possible about the system. All of the factors mentioned above show that privacy is a key issue for the police.

4.4 Classification Risk

This risk has been operationalized as the risk of black boxing classifications which makes classifications both potent and invisible. This could lead to the exclusion of the public from policy participation because they have no insight in these classifications (Bowker & Starr, 1999). It is interesting to see if this risk is recognized by the interviewees. They have insights into how the system is built up and can indicate if the CAS is or is not an example of a black box. Indicators of this specific risk are black-boxing, classification and categorization.

Rienks indicates that the Dutch police has developed the CAS themselves, without a third party. He mentions the contrast with the CAS and PredPol, since that is a third party policing system which stores data on servers in the United States. He argues that: *'Police Forces want to design the algorithms themselves with a clear explanation and understanding of how it works. They need to explain their way of working with predictive policing practices to the politicians and the people as well'* (Rienks, 9th October 2018). He sees this as a reason why the

Dutch police was very much in favour of developing their own system, built on their own models and data. Den Hengst confirms this by stating that clear benefits of the systems are that data is not being transferred to third companies, on top of that she argues that it is also a key benefit that the police knows what the algorithm can and cannot do (Den Hengst, 6th December 2018).

It is very interesting as well to see how Dick Willems views these issues. He perceives the advantage of building the system within the Dutch police. Next to his argument that they can fine-tune the policing system according to their own need, he argues that the system is transparent, but only for those who understand analytics: *'You have to be a data scientist or statistician to understand what I'm saying.'* Next to this quote, another one that illustrates this opinion is that he indicates: *'I can't make it transparent to the average guy on the street because they don't know anything about predictive Analytics'* (Willems, 11th November 2018). It is quite logical that he mentions this. In the literature however, it does not seem that sufficient thought has been put into this risk. Often there is an idea that systems such as CAS should be more transparent, but the question is whether regular people can understand these kind of systems. Of course, that is partly what different authors mean, the systems are so advanced that they are difficult to grasp. Dick Willems elaborated on the actual need for regular people to understand systems such as the CAS. He indicated that people from the ministry of Safety and Justice sometimes ask him about his algorithms: *'But usually they don't so either they understand what I'm saying, which is transparent to me I guess, or they lost the will to understand this issue, which is on them then'* (Willems, 11th November 2018). This illustrates that although there are voices to be heard on transparency, this also requires people to dive deeper into analytics and data usage. You need to understand these systems in order to make it transparent for yourself. One cannot ask for transparency and at the same time ignore learning about the technical parts behind the system. Willems clearly wants to explain how his system works, but you have to understand his technical explanation.

Even though there is some feeling that the factors mentioned above make sure that the CAS is not a black box, there are some indications that it has some black boxing elements. However, these are not as obvious as it seems. Hans Grube adds new points to the debate on black-boxing by mentioning that information officers, who provide the agents on the streets with their CAS-guided information and high-risk areas, do not know all the variables. Grube states that: *'it would be nice to click on a high-risk square and see what exactly the prediction is based on.'* When asked about what information officers do and do not know, he adds that:

'you know the algorithm, what indicators it uses and you have an estimation on their weight, but you do not know which one carries the most weight in the prediction' (Grübe, 14th December 2018). However, when speaking to Melchers, it seems that that this is done on purpose. Melchers argues that: *'We did not provide the information officers with that information on purpose, we want them to enrich the CAS data with their own instincts, experiences and gut feeling'* (Melchers, 9th January, 2019). This illustrates that the reason behind not opening up the variables and their weight to everyone is a clear choice. It is done so that people still think for themselves whether the output from the CAS is correct.

Den Hengst does stress a very important factor within black-boxing issues. She indicates that: *'The data scientists working on the algorithms know how it would work, but they still create a black box for the rest of the organization'* (Den Hengst, 6th December 2018). This is interesting. At first it seemed as if it only was a black-box to the world outside the police, because the police would obviously understand the algorithms. But, if we observe what Den Hengst states, it is clear that the algorithm could be seen as a black-box to the rest of the policing organization as well. Melchers describes it a bit different. He states the following: *It is a bit of a black box, but a black box that we can open up if we need to in case of an emergency or a court case'* (Melchers, 9th January, 2019).

All of the above does indicate that a lot of thought that has been put into the black-boxing risk of the CAS. Due to the development of the system by the police themselves, most of these black boxing issues are non-existent. The only part that could cause some concerns, is the one that was mentioned by Grübe and Den Hengst. When information officers do not know how the systems weighs certain factors, this could be seen as a system that is not transparent and a black-box to some parts of the organization outside of the data scientists. Still, Melchers indicated that this was done on purpose, the reason being that information officers should not only follow maps, but instead are stimulated to use other information outside of predictive policing systems as well. Furthermore, I do think that if an information officers would want to know this weight of certain indicators, he could ask Willems. He indicated in the interview, as his quotes show, that he is more than willing to help people understand the algorithm. The main ingredient that is necessary for people to understand the algorithm is a sufficient amount of knowledge on things like machine learning. Melchers also added that in when necessary in a court case they could check exactly how the predictions are built up by the CAS. In this sense I think that the CAS certainly is not a black-box, but it has some elements that could be seen as black-boxing, although these are largely mitigated because you can 'open up the box.'

4.5 Risk of Losing Traditional Policing Skills

The final risk from the literature is focused on the loss of traditional policing skills. This is what will happen when police officers will just blindly follow computers, without thinking for themselves. A system such as the CAS would become leading in that regard, and no longer guiding. The risk has been defined as the risk of losing traditional policing skills, such as judging individual incidents according to own intuition, because of too much reliance on guidance by algorithms (Smit & de Vries, 2016, p. 16). The main indicators for this risk were the reliance on algorithms, losing of skills (set), intuition and final decision maker issues.

In his book, Rienks wonders if algorithms could one day replace the police officer as we know it (Rienks, 2015, p. 139). Who is in control in the end? When asked about elaboration on this paragraph in his book and if traditional policing skills can be lost he answers: *'It might happen. Luckily in the Netherlands, the officers are quite highly educated so they always need to think for themselves. The human factor is important in the Dutch police, so it won't happen'* (Rienks, 9th October 2018). Of course, this seems like the logical thing for a (former) police officer to say. But Rienks also indicates that it indeed could be seen as a potential risk. Dick Willems adds some more credibility to the argument on the human factor within the Dutch police. He states that police officers are selected on two things, both the possession of an aura of authority and making split-second decisions. He indicates that these two things combined usually lead to stubbornness. It is because of this stubbornness that he does not see a future image in which police officers will blindly follow the system. A quote that illustrates this is the following: *'I don't think they will ever blindly follow systems, I think it will always be in support of what they normally do'* (Willems, 11th November 2018). These answers of both Rienks and Willems shows that they think the loss of traditional policing skills is not likely to happen.

Bas Mali, when asked about the possibility on police officers who blindly follow a system, indicates exactly the same. He states that: *'Knowing the police officers, it will never happen. They are stubborn enough. Dutch agents will not let themselves be purely be guided by a system'* (Mali, 11th December 2018). It is striking that he immediately also mentions the stubbornness of the general police officers. This does seem to indicate that there is truth to this claim that Dutch police officers have general qualities in their nature which help them to counter this risk. A second reason, next to stubbornness, might be capacity related. Grube argues that officers will not follow the system blindly simply because they cannot do it. Sometimes the system might indicate that officers should go to a certain neighbourhood, but the officers are required at an emergency situation or somewhere else. Furthermore, he indicates that the system

is not necessarily prescribed to officers (Grübe, 14th December 2018). They are allowed to structure their own patrol, following the system is not required, but it is encouraged. I would say that this certainly is a reason why the CAS will probably not lead to a loss of traditional policing skills. Grübe illustrates this by stating the following: *'You should see this system as pretty low profile. It is a tool to create some more guidance, but we are not strictly telling police officers to use it'* (Grübe, 14th December 2018). He argues that in fact, the risk of going all in on a system like the CAS might be the biggest risk. He states that *'You should never just look at the system, you should apply your own logic next to it. It is just a 'stupid' system, so to speak, that makes a prediction based on algorithms. You should not blindly follow it'* (Grübe, 14th December 2018).

In the eyes of Melchers, the biggest risk is that people will see CAS as some kind of miracle tool. He indicates the following: *'The biggest risk that I see is that CAS is seen as some sort of magical tool. So that if you read CAS maps you will know exactly where all the crime will happen. That these maps become some sort of truth for colleagues on the street or whoever is looking at the maps'* (Melchers, 9th January, 2019). The fact that the national project leader of the CAS sees this as the biggest risk does illustrate that the police think about the use of CAS very thoroughly. That is why Melchers stresses that the CAS is not some miracle tool and will still require police officers to use their own instincts (Melchers, 9th January, 2019).

Den Hengst also sees the loss of traditional policing skills as a risk. She mentions that in some situations police officers are not sure about what action they should take if they do not get the appropriate information (Den Hengst, 6th December 2018). In that regard it could be a danger that if the CAS does not give any instructions, or the information officer does not, the police officer might get lost and does not know what to do. This might also be a factor because the officer on the street has no clue what the CAS does. Willems mentions, when asked if police officers on the street know about what the CAS does, the following: *'Not at all. No, because, you know, the information specialist has to have some knowledge, right? They at least need to know how to interpret the maps and the graphs, what they do afterwards is basically gather new information and form their own hypothesis'* (Willems, 11th November 2018). This places a lot of emphasis on the role of the information officer, but the officers on the street are somewhat left out of sight in this approach. It might be an issue if they do not understand the system that, together with an information officer, feeds them their information. One other important factor that does seem positive, with regards to the human touch, is that Willems indicated that the decision will always be human. So the information that is being sent to the

officers on the street will always come from a human information officer. In that regard the final decision maker issues will not exist, because it will always be a human who decides.

So why exactly this risk is perceived so clearly, and why are the interviewees consistent in their answers? A part of this answer might boil down to training. The police officers who work with the CAS have received training on the system. This might also influence their ability to work with the system and knowing when to follow instructions from the systems or not. Rienks indicates that the police officers receive training before they are sent out to work with it (Rienks, 9th October 2018). Willems elaborates on this. When asked if regular police officers know about the use of the system, he states that: *'For the information officers there is a training, for police officers there isn't.'* The reason for this difference is that for police officers on the street it is still the same job. Willems describes it as follows: *'It's basically the same job as before. Maybe with different targeting but what they do on a day to day basis is the same'* (Willems, 11th November 2018). Den Hengst also indicates that training is role specific for analysts, police officers get general information on the system, but are not necessarily instructed about the risks.

When this risk is examined, the perception of it is very clear, but it is not as serious as the perception on other risks such as profiling, privacy and algorithmic risks. This is mainly due to the given that a lot of faith is placed in the characteristics of most Dutch police officers. As indicated by most interviewees, the police officers are having their own ideas and are clear in voicing these ideas. This stubbornness is believed to prevent them from blindly following the system, but we can consider their training and the lack of top-down emphasis, from police leadership, on the system as important factors as well. All of these factors combined give an idea of why this risk is not perceived to be a very big one by the Dutch police. The only point of concern could be that street-level police officers do not know much about the CAS. The question in this sense is if they should know how the system works, or if this perhaps is unnecessary.

4.6. New Risks

An interesting option that the interviews provided me with, is the discovery of new risks. The literature mentions all sorts of risks, one more relevant than others, but it does certainly not touch upon all the risks that are attached to the CAS. In the interviews some other risks also popped up. A possible question following the discovery of these new risks is if they are the

result of a lacking theoretical framework that might have overlooked certain risks. This will be addressed in the conclusion. It is interesting to observe the most relevant and most named ones as well, next to the ones that have been analysed above. The new risks can be split up into two parts. One of them is risks regarding the effectiveness of the system, the second type of risk is the risk for the police department. This second risk is more or less one that is forth flowing out of the first risk, but this will be made clear later on.

The first problem is unreported crime. Dick Willems was the first of my interviewees to mention this problem. It came up when we discussed how effective the CAS is at preventing crime and how this could be measured. Willems indicated, when asked if unreported crime was a big problem: *‘Yes. Especially because we don’t know how much unreported crime we have. Muggings are often not reported for example because people know the perpetrator. In certain neighbourhoods that might be a problem. I also think that we processes that we have in place can alleviate that problem in some way. If you have a good information specialist he doesn’t only look at what’s registered, but also talks to his officers and the community’* (Willems, 11th November 2018). This illustrates that unreported crime indeed affects the effectiveness measurement. But, as Willems responds, there are some procedures in place that could help to alleviate the problem. When you talk to a community you can engage in a conversation on crime with citizens. That way you can check if your input into the system is correct. If, in these conversations, you notice there are a lot more burglaries or muggings than the ones that you are reporting into the system, this means that crime is not being reported (Willems, 11th November 2018).

Unreported crime is just one factor of something bigger, effectiveness. When you introduce a system like the CAS, it is important to have some idea of how effective it is or is going to be. A lot of time, effort and resources are invested into these systems, therefore it is useful to know its impact. Dick Willems agreed that it was hard to estimate the impact of the system: *‘I have a sense of its predictive power, but you’re asking about the effect of crime. That’s pretty hard to determine. We could try to do some analysis to see if it’s effective. But we do not have GPS data to trace our colleagues so we do not know if they follow the CAS plan on their patrol.’* Furthermore, if there would be a decline in burglaries, the following is important to keep in mind: *‘We’ve seen a decline in burglary, but we cannot all account that success to the CAS system, it is one big mix of police and community activities. So it’s hard to tell in practice and assign a decline in crime to one police activity’* (Willems, 11th November 2018). This all illustrates how hard it is to actually say something regarding the effectiveness of the

system. Bas Mali's opinion is also an interesting one to take into account. Since he did the evaluation of the CAS he will have some input into the effectiveness of the system. He argues that: *'You can't influence a real life situation. You are looking for a causal relation, but you can't isolate this phenomenon like you could in an experimental design'* (Mali, 11th December 2018). This effectiveness can certainly be seen as a risk, but there is another problem that is the result of this lack in effectiveness.

Since the police finds it hard to assess the effectiveness of the system, it is hard to bring across the benefits of the CAS to police officers. The culture of the Dutch police has been mentioned above, it is one of intelligent police officers with a healthy amount of stubbornness. It can be difficult to implement a system such as the CAS in such a force. Den Hengst strengthens this idea by mentioning that it is difficult to show police officers that the system works (Den Hengst, 6th December 2018). This is something Willems knows as well: *'Younger police officers like this police technology being used, but the older guys say look I've been doing this job for 30 years'* (Willems, 11th November 2018). Bas Mali goes further, he explains it as follows: *'This is one of the problems, we are dealing with officers who are very conservative and who can be stubborn. They will not change that easy'* (Mali, 11th December 2018). If the system was objectively successful in preventing crime, something that is really hard to measure, every single police officer would use it. But right now that does not happen like it should, Grube adds: *'Look, if you would catch people red-handed every time, we would use it all the time. That is not the case however, so people do not use it all the time'* (Grube, 14th December 2018).

The culture has been mentioned a couple of times now. This seems to indicate that the CAS is not received the same everywhere by every single police unit. A risk that comes from this observation is the way in which different police forces have different strategies in implementing the CAS. Rienks confirms that teams use the system in different ways: *'When they introduce the model to a new CAS team, a new area where there is one team in charge, they always tune the model specifically to the geographic location because the data is from years ago so they can train the model specifically to that situation and they know the performance in that region'* (Rienks, 9th October 2018). If you do not implement it the same way in every region however, or attach the same value to the system, it becomes vague. Which team uses it, which team does not? Things such as the impact of the system are even harder to grasp when you do not know these factors. Den Hengst agrees that it is difficult, she states that it is also difficult because: *'You predict burglaries will happen in certain areas and if nothing happened, and police officers will go there and nothing happened, saying: 'I worked an entire*

time shift and nothing happened and that CAS doesn't work.' It's very difficult to help them understand that nothing happened because they are there and the system really worked well' (Den Hengst, 6th December 2018). This is followed up by an argument made by Grube, who indicates that leadership and the culture are very important for teams who might use the CAS. If teams do not have a feeling for the system and do not use it, the knowledge of and enthusiasm about the CAS could be gone just as quick as it came (Grube, 14th December 2018). Melchers does not really view a disruption within the Dutch police, because of the different way that's CAS is used, as a risk. He argues that: *'Not every area needs the same approach. The system is available for everyone, but that does not mean that everyone should use it in the same way'* (Melchers, 9th January, 2019).

All in all the measurement of the CAS does pose a problem. You cannot measure how effective your predictive policing system is in preventing crime. This is a problem when you want to assess the impact of resources that you put into such a system. A risk that evolves out of this problem is the risk for the system within the police, mainly in how it is taken up by the police officers. If outputs from predicting policing systems do not grasp the attention of police officers who go out on the street to work with it, it could create a disruption within the police force. One where data scientists and elements of leadership are pushing hard on a system, while street-level officers do not see the outcomes and benefits of the system. This risk is somewhat different in nature than the other ones mentioned earlier on, mainly in the sense that it is a risk purely for the police themselves.

4.7 Combining the Perceptions of the Dutch Police

In this final part of the analysis the perception that the Dutch police has of each risk will be reflected upon. The goal is to create a clear overview of the perception of each risk. The Dutch police perceives the problem of profiling as a serious one. The main arguments against profiling occurring in the CAS are that the system selects on certain specific indicators, personal characteristics are not included in this assessment. However, income was mentioned to be a variable. An argument could be made that the CAS could possibly discriminate against lower-income areas. But this is certainly not the goal or a wanted effect of the system. There are several measures in place to prevent profiling, as Willems indicated. Another factor against the occurrence of profiling is that the system is only able to predict locations on a map. The interviewees indicate that if an area has always had a lot of crime, it makes sense for the police

to be in that area. The profiling risk is clearly observed by the Dutch police, but because of the way the system is built it they do not see it as one of the most stressing ones.

A risk that is perceived to be more important is the algorithmic risk. False positives were mentioned as one of the biggest risks by Rienks. Another one was mentioned by Hengst, she argued how the CAS could create certain high-risk areas. The fact that Den Hengst mentions this however, indicates that the Dutch police does not overlook these kinds of factors. Another important algorithmic risk, unreported crime, was also immediately recognized by Dick Willems. This again shows that the Dutch police is busy with the risks they perceive to be serious. An example of this is the fact that they try to avoid construction errors by letting multiple data scientists have a look at a system before they put it in place. Thus, the Dutch police perceives algorithmic risks in particular to be important risks that require a lot of attention.

Another risk that received a lot of attention of the interviewees is the privacy risk. In fact, this risk was a lot more important to the police than it was in the literature on predictive policing risks. In the literature it was mentioned, but less than for example the profiling risk. In the interviews on the contrary side, it became clear that the police does see this as an important factor when developing and working with systems such as the CAS. They target the risk within the CAS by using measures such as privacy by design and using data that is not connected to specific persons. They also target it by telling their story about CAS in the media to create transparency. By making use of these measures, Interviewees even indicated that algorithms could create transparency for people on the street, instead of hiding it. These factors show that privacy is a key issue for the police and that the perception of this risk, importance-wise, is up there along with algorithmic risks. I think this is a key issue because the police always relies heavily on the support and especially the trust of the general public, which is why issues like privacy receive a lot of attention.

In the literature, a lot of thought was put into the classification risks of the CAS. However, due to the development of the system by the police themselves, most of these black boxing issues are non-existent. This ensures them to be fully aware of what they put into the system and create the system exactly in the way they want it to work. A risk that could give rise to some concerns, is that information officers do not know how the system weighs certain factors. Because of this the system could be seen as a black-box to some parts of the organization outside of the data scientists who create the algorithms. One important factor in this is that the black box can be opened. If necessary it can be checked what exactly lead to a

certain prediction. This immediately takes away a lot of black boxing issues. Willems also indicated that he is more than willing to help people understand the algorithm. I think this means that the CAS could be a black-box for some people, but that if you want to understand it you can. The risk perception on classification risks is less than the three mentioned before. The reason for this is the same as with profiling risks, the system is not built in a way that makes classification risks very plausible. This means that the risk perception of this risks is less than it is on other ones.

When the risk on the loss of traditional policing skills is examined, the perception of it is not as serious as the perception on other risks such as privacy and algorithmic risks. This is mainly due to the given that a lot of faith is placed in the characteristics of most Dutch police officers. Police officers are having their own ideas and are clear in voicing these ideas. This stubbornness is believed to prevent them from blindly following the system, but we can consider their training and the lack of top-down emphasis on the system as important factors as well. All of these factors combined give an idea of why this risk is not perceived to be a very big one by the Dutch police.

The interviewees also gave rise to some new risks such as the measurement of the CAS. This mainly goes for the measuring of effectiveness of the system. Since this is very hard to do, you cannot assess how good the system is working and if the resources are worth the final result of the CAS. Furthermore it is also difficult to show your police officers the use and importance of the system. As said before, if outputs from predicting policing systems do not grasp the attention of police officers who go out on the street to work with it, it could create a disruption within the police force. One where data scientists and elements of leadership are pushing hard on a system, while street-level officers do not see the outcomes and benefits of the system. On the other hand, it must be said that this different use of the CAS is not seen as something that is necessarily negative. Every location needs its own approach.

5. Conclusion

This thesis started with the introduction of a research problem. Out of this problem a research question was posed: *'How does the Dutch police perceive the risks associated with predictive policing?'* Through semi elite interviews this research question has been examined. Several risks were apparent in the literature surrounding predictive policing methods. These were used to create an overview of all the risks in predictive policing.

In the interviews each of these risks was touched upon. Some were perceived by the Dutch police to be bigger risks than others. Not only in relation to each other but also in relation to the amount of attention certain risks received in the literature. For example, the literature did not make a very big case out of the privacy risks in predictive policing. However, in the interviews this risk was perceived as a very important one. In general, all the risks that the literature mentioned were perceived as well by the Dutch police. The algorithmic risks, privacy risks and profiling risks were seen as the most important ones. Especially the algorithmic and privacy related risks were taken up very serious by the Dutch police. Because of the design of the system, certain risks that were given a lot of emphasis in the literature did not lead to the same risk perception within the Dutch police. Classification risks in particular were not perceived to be very serious due to the design of the CAS. Profiling issues were also seen as less serious than privacy and algorithmic risks due to the nature of the CAS. The risk of losing traditional policing skills was also not indicated to be apparent within the Dutch police. The police did admit it was a possibility, but due to the characteristics of the Dutch police they did not see it as a very plausible risk. Next to perceiving every single risk from the literature, the police also perceived some new risks such as the risks surrounding the effectiveness of the system and the possibility of disruption in the police force. One important question is if this is caused by a theoretical framework that is not broad enough. I would argue that this is not the case. These new risks are risks on a practical level and more importantly, they are risks within the organization. As an outsider you do not have much insight into risks such as the effectiveness of the CAS or how this might cause a disruption within the police force. Therefore I think that these new risks are not the result of a theoretical framework that lacks depth.

Concluding, it is very interesting that each risk from the literature was perceived by the Dutch police and that they even indicated new risks. In the theoretical framework risk perception was defined as: *'The probability of certain risks of predictive policing and in what ways the Dutch police are concerned with their consequences.'* Following this definition leads it can be concluded that the Dutch police perceives the risks associated with predictive policing

to be very serious. The Dutch police has assessed the probability of the risks in predictive policing and has looked at which risks could be present in the CAS and the consequences they could have. The fact that they implemented a lot of safeguards such as information officers for some risks and designed their system in a way that minimalizes other risks shows that they are concerned with the consequences. This leads to the belief that their risk perception is apparent and very thorough. They do not overlook any risk and pay attention to measures that contribute in avoiding and minimizing them. It must be mentioned that, although they perceive every risk, they need to maintain this level of attention. Algorithmic risks, for example false positives, cannot really be avoided. This means that some risks require the constant attention of the Dutch police, while other ones such as classification risks are dealt with more comfortably due to the design of the Dutch predictive policing systems.

One could argue that this research did have some limitations. The first one, as was mentioned in the methodology, is a limitation that deals with the interviewing method. By conducting semi-structured interviews no interview was the same. This did provide for interesting data, but something could be said to have used a standard set of questions for each interviewee. I did not do this because my interviewees all have different background. For example, I chose to ask the designer of the system more technical questions than I asked the regional coordinator. This has been done in order to create a complete overview of every risk as they were perceived by the Dutch police. In order to do this I had to ask different people within the Dutch police that all have their own expertise and experience with predictive policing. This is the main reason that questions have differed between interviewees. Another possible limitation of my conclusion could be that the Dutch police indeed does perceive every single risk that was mentioned in the literature, but that my questions stimulated this. An argument could be made that in some cases I did ask on comments regarding a specific risk. Having that said, in all interviews combined every single risk was mentioned ‘out of the blue’ at least once by different interviewees. In a lot of interviews the interviewees were the ones bringing up certain risks, after which I could stimulate them to elaborate them on this particular risk once it was mentioned.

Another limitation could be that some of the interviewees know each other and come from the same small group of predictive policing experts. I did use a second line of investigations to try and avoid this. However, there are only a few people within the Dutch police force with extensive knowledge on predictive policing risks. Furthermore, ones could argue that they possibly did not always express their true feelings and opinions. I would like to indicate that I did not have this impression at all, which leads me to believe that every interview

was genuine. However, it is important to keep in mind that it is the Dutch police who is asked about risk perceptions on predictive policing in the Netherlands. Since it is something new they have started working with recently one could imagine that they will not be too harsh in their judgement of the system. Especially people who, for example, developed it.

On top of that a limitation of the research is the time period. More interviewees could have been included in the research, but due to a limited amount of time to finish the thesis this was not possible. It mainly boils down to the fact that I really tried to target experts. Their agendas are often filled a couple of months beforehand. Future research could perhaps deal with the option to include more interviewees. Another limitation is that the amount of data from the interviews is somewhat difficult to analyse sometimes. This is because certain risks, such as algorithmic risks and classification risks, which first appeared to be very different, do have similarities such as the focus on the use of data sets. Because of these similarities, sometimes, certain interview results could be assigned to both risks, instead of just one. In future research this could be dealt with by making the distinctions between risks even more clear.

A very interesting option for future research could be to investigate the new risks that this research has identified. One could do a deep study into these risks to gather more information on them and on how the Dutch police plans to deal with them. On top of that future research could link these findings to other police forces around the world. As mentioned before the data in this research is only concerned with Dutch predictive policing. These results could be aligned with research into other countries that use predictive policing methods. An interesting outcome of this future research could be that it can examine which police forces could be considered to be more responsible and aware of the risks in predictive policing systems. That way it could become an option to give police forces certain templates or recommendations on how to deal with specific risks.

All in all this research has clearly identified the risk perception of the Dutch police on the risks associated with predictive policing. It has also shown how these risks relate to the current literature on predictive policing risks. The findings indicate that the explorative nature of this research has been met. On a final note I would like to explicitly thank all of the people who gave me the opportunity to interview them. Without them this research could not have been conducted, the outcomes would have been impossible to reach on my own.

6. References

- Akintoye, A.S. & M.J. MacLeod (1997). Risk analysis and management in construction. *International Journal of Project Management*, 15, 31–38.
- Alderson, J. (1979). *Policing Freedom: A Commentary on the Dilemmas of Policing in Western Democracies*. Plymouth: MacDonald and Evans.
- Barocas, S., Felten, E., Huey, J., Kroll, J., Reidenberg, J., Robinson, D. G. & Yu, H. L. (2017). Accountable Algorithms. *University Of Pennsylvania Law Review*, 165(3), 633-705.
- Batty, M. (2013). Big data, smart cities and city planning. *Dialogues in Human Geography*, 3(3), 274-279.
- Bowker, G. & Star, S.L. (1999). *Sorting things out: Classification and its consequences*. Cambridge: The MIT Press.
- Brehm, S. & Loubere, N. (2018). The Global Age of Algorithm : Social Credit and the Financialisation of Governance in China. *Made in China: A Quarterly on Chinese Labour, Civil Society, and Rights*, 3(1), 38-43.
- Carter, D. L. (2004). *Law enforcement intelligence: A guide for state, local and tribal law enforcement agencies*. Washington, DC: U.S. Department of Justice.
- Carter, D. L., & Carter, J. G. (2009). Intelligence-led policing: Conceptual considerations for public policy. *Criminal Justice Policy Review*, 20(3), 310–325.
- De Correspondent. (2015). *De politie van de toekomst houdt iedere burger non-stop in de gaten*. Visited on 12 October 2018, from: <https://decorrespondent.nl/3044/de-politie-van-de-toekomst-houdt-iedere-burger-non-stop-in-de-gaten/279163005704-5df91b90>.
- De Standaard. (2018). *Agenten aansturen met algoritmes? 'Oppassen voor ethnic profiling.'* Visited on 4 September 2018, from: http://www.standaard.be/cnt/dmf20180830_03691319
- Ericson, R.V. & Haggerty, K.D. (1997). *Policing the Risk Society*. Toronto: University of Toronto Press.
- Ferguson, A.G. (2012). Predictive Policing and Reasonable Suspicion. *Emory Law Journal*, 62(2), 259-325.

- FICCI Studies and Surveys. (2018). *Predictive Policing and Way Forward: Prediction led policing processes and practices*. Visited on 14 September, from: https://global-factiva-com.ezproxy.leidenuniv.nl:2443/ha/default.aspx#!?&_suid=153734994542208964603372144533.
- Frame, J.D. (2003). *Managing Risk in Organizations: A Guide for Managers*. Hoboken: John Wiley & Sons.
- Fyfe, N.R., Gundhus, H.O.I., & Rønn, K.V. (2018). *Moral Issues in Intelligence-led Policing*. New York: Routledge.
- Jiao, A.Y. (1998). Matching police-community expectations: A method of determining policing models. *Journal of Criminal Justice*, 26(4), 291-306.
- Karppi, T. (2018). The Computer Said So”: On the Ethics, Effectiveness, and Cultural Techniques of Predictive Policing. *Social Media + Society*, 4(2), 1-9.
- Kirkpatrick, K. (2017). It's not the algorithm, it's the data. *Communications of the ACM*, 60(2), 21-23.
- Kitchin, R. (2014). *The data revolution: big data, open data, data infrastructures and their consequences*. Los Angeles: SAGE.
- Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, 79(1), 1-14.
- Koss, K. K. (2015). Leveraging predictive policing algorithms to restore fourth amendment protections in high-crime areas in a post-Wardlow world. *Chicago-Kent Law Review*, 90(1), 301-334.
- Maguire, M. (2000). Policing by risks and targets: Some dimensions and implications of intelligence-led crime control. *Policing and Society*, 9(4), 315-336.
- Moen, B., Sjöberg, L. & Rundmo, T. (2004). Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research. *C Rotunde publikasjoner 84*.
- Niculescu-Dinca, V. (2016). *Policing Matter(s): towards a sedimentology of suspicion in technologically mediated surveillance*. Maastricht: Datawyse / Universitaire Pers Maastricht.
- NRC. (2017). *Misdaad voorspellen, het kan echt*. Visited on 4 September 2018, from: <https://www.nrc.nl/nieuws/2017/05/16/misdaad-voorspellen-het-kan-echt-9100898-a1558837>.

- Rathenau Instituut. (2017). *Nederlandse Politie: Technologie noodzakelijk voor aanpassing aan snel veranderende samenleving*. Visited on 5 September 2018, from: <https://www.rathenau.nl/nl/digitale-samenleving/nederlandse-politie-technologie-noodzakelijk-voor-aanpassing-aan-snel>.
- Reisig, M.D. (2010) Community and Problem-Oriented Policing. *Crime & Justice*, 39(1), 1-53.
- Reisig, M.D., Kane, R.J., Cordner, G. (2014). *The Oxford Handbook of Police and Policing* Oxford: Oxford University Press.
- Rienks, R. (2015). *Predictive Policing: kansen voor een veiligere toekomst*. Apeldoorn: Politieacademie.
- Rosenzweig, J., Smith, E., & Treveskes, S. (2017). *Forum: Interpreting the Rule of Law in Xi Jinping's China.* In: *Made in China Yearbook 2016: Disturbances in Heaven*. Canberra: ANU Press.
- Sanders, C.B., Weston, C. & Schott, N. (2015). Police Innovations, 'Secret Squirrels' and Accountability: Empirically Studying Intelligence led Policing in Canada. *British Journal Of Criminology*, 55(4), 711-729.
- Searle, R. (2016). The Promise and Pitfalls of Algorithmic Governance for Developing Societies. *Postmodern Openings*, 6(1),171-176.
- Short Jr, J. F. (1984). The social fabric of risk: towards the social transformation of risk analysis. *American Sociological Review*, 49(6), 711-725.
- Slovic, P. (1992). *Perception of risk: reflections on the psychometric paradigm*. In: *Social theories of risk*. Westport: Praeger.
- Smit, S. & Vries, A. de. (2016). Predictive policing: politiewerk aan de hand van voorspellingen. *Justitiële verkenningen*, 42(3), 9-22.
- Spencer, T. (2016). *Risk perception: theories and approaches*. New York: Nova Publishers.
- Tilley, N. (2008). *Modern approaches to policing: community, problem-oriented and intelligence-led*. In: *Handbook of Policing*. Cullompton: Willan Publishing.
- Treverton, G.F., Wollman, M., Wilke, E. & Lai, D. (2011). *Moving Toward the Future of Policing*. Pittsburg: RAND Corporation.
- Wachinger, G. & Renn, O. (2010). *Risk Perception and Natural Hazards*. Non-Profit Institute for Communication and Cooperative Research.

Yin, R.K. (2018). *Case Study Research and Applications: Design and Methods*. Los Angeles: SAGE.

Završnik, A. (2017). *Big data, crime and social control*. London: Taylor and Francis.