University of Twente

Enschede, Netherlands

NAVIGATING INDIVIDUAL PRIVACY AND PUBLIC SAFETY

An Analysis on the Dutch Policy Discourse on Social Media Surveillance

Katja Lindenaar (S2486687)

Programme: Management, Society and Technology

Supervisors: Dr. M.R.R. Ossewaarde & Dr. V. Junjan

Date: 3rd of July 2024

Word count: 11.239

ABSTRACT

This thesis explores the complex relation between privacy and safety within the context of social media surveillance and AI, focusing on the Dutch government's policy discourse. AI surveillance is not just happening in authoritarian regimes but also in democracies and policy makers are faced with challenges that arise when balancing public safety and individual privacy. The study looks into the Dutch government's conceptual understanding of privacy and safety and how the tension between these two values is navigated. The main research question is: "How does the Dutch government, in its policy discourses, envision the relationship between privacy and public safety in its social media surveillance via AI?", this question is supplemented by sub-questions focusing on gaining a deeper understanding. The study concludes that the Dutch government strives to use AI ethically and responsibly, aligning its use with democratic values, while also addressing the challenges posed by digital surveillance. They adopt a cautious approach to AI implementation, emphasising the need for a legal framework and transparency to minimise risks to individual privacy. This research provides valuable insights into the Dutch government's approach, potentially informing future policies, but nevertheless, future studies are suggested to enhance the understanding of AI.

TABLE OF CONTENT

1. INTRODUCTION

1.1. Background and state of the art

Social media surveillance is a topic that is gaining more attention, and more governments are starting to use social media surveillance. Not only authoritarian countries are using it now, but democratic countries are also making this shift. (Freedom House, n.d.) Surveillance done by governments gained massive attention during the Snowden affair, when Edward Snowden leaked documents of the National Security Agency about global mass surveillance. It came as a surprise to people that surveillance was happening in the most high-tech ways possible, that people could not even imagine this happening. (Lyon, 2015) And this is and was not the only time something similar to this happened. The Dutch government is also surveilling social media networks according to Buro Jansen & Janssen (2017), hey revealed in 2017 after their Wet Openbaarheid Bestuur (WOB). (Buro Jansen & Janssen, 2017). While one might expect such a revelation would disturb the Dutch population, there is nothing to find about it in the news. In an era characterised by rapid development of artificial intelligence (AI) technology, and the presence of social media platforms, our lives have become deeply intertwined with technology like never before. The delicate balance between ensuring public safety and the guarantee of individual privacy rights by the government, begins to conflict as AI-driven systems are used more and more by governments. How do governments navigate this balance in their policy discourse, is a question that lies at heart of contemporary debates around the use of advanced technologies, for maintaining societal order and monitoring safety. In their policy discourses, governments all over the world struggle with the challenges posed by the rapid evolution of artificial intelligence, but also seek possibilities to use these technologies to their own advantage.

The growth of social media platforms has changed the landscape of public discourse tremendously, giving new opportunities to connect with each other and express oneself. While these platforms offer all these opportunities, they also pose significant challenges in terms of privacy infringements and possible threats to public safety. The increase of misinformation, commonly referred to as fake news, hate speech and radicalisation has prompted governments to explore strategies for monitoring and regulating digital spaces. With this development also evolved the public discourse on surveillance. The perception on safety and privacy in the context of AI and these policy discourses have changed over the course of time. Where privacy started as a right to be let alone in your personal space (Lukács, n.d.), a new personal space was added called the internet, stirring up new debate on the concept of privacy. While online surveillance sounds like something very futuristic, or something that fits in an authoritarian state like China, where a social credit system is in place, there are risks this type of surveillance can have. In the past social media has also proven its power, for example during the Arab Spring where many people were influenced. Although there is no clear evidence that social media breaks authoritarianism down, many authoritarian governments have gone great lengths to limit its power.(Zeng & Wong, 2022)

1.2. Knowledge gap

While there is extensive research on privacy issues related to major companies like Meta and Alphabet (Google), and the possibilities of social media surveillance and AI surveillance (Trottier & Lyon, 2012), there is a significant gap in understanding the perspective of the Dutch government on these issues. Existing studies have looked into the American public discourse on surveillance (Simone, 2009), and there is evidence that social media surveillance is happening (Feldstein, 2022), also in the Netherlands (Buro Jansen & Janssen, 2017). However, no research has been conducted on how the Dutch government perceives social media surveillance, particularly in conjunction with AI. The research aims to fill this gap by investigating the Dutch government's discourse on social media surveillance and AI. This will involve analysing official documents, public statements, and policies to understand the government's stance and approach towards these issues. The research will provide valuable insights into how the Dutch government navigates the complex landscape of privacy, social media, and AI surveillance. This could potentially inform future policies and practices, contributing to a more comprehensive understanding of the global discourse on these critical issues. This gap in knowledge formed the basis of this research question.

1.3. Research questions

Given the identified knowledge gap, this research aims to understand how the Dutch government, in its policy discourses, envisions the relationship between privacy and public safety in its social media surveillance. The research question directly addresses the identified knowledge gap by focusing on the Dutch government's perspective, which has been largely unexplored in existing research. This research will focus on the following question:

RQ: "How does the Dutch government, in its policy discourses, envision the relationship between privacy and public safety in its social media surveillance via AI"

The sub-questions are designed to provide an answer to the main research question:

SQ$_1$: "How does the Dutch government envision the role of AI in its own social media surveillance?" This question explores the government's use of AI in surveillance, a key aspect of the knowledge gap. It is aimed to gain an understanding of how digital surveillance is happening at this moment, which can address the ethical aspect of the main research question, answering the value aspect of it.

SQ$_2$: "How are privacy and safety understood in the context of surveillance by the Dutch government?" This question delves into the government's conceptual understanding of privacy and safety, central themes in the knowledge gap. In order to conclude how the concepts relate to each other, it is key to understand the concepts on their own, and how they are understood by the government, and in comparison to scientific literature.

SQ$_3$: "How does the Dutch government view the tensions between privacy and surveillance?" This question investigates the government's stance on the balance between privacy and surveillance, a critical issue identified in the knowledge gap. This is also the last puzzle piece to answer the main research question.

By addressing these sub-questions, the research will fill the identified knowledge gap, providing valuable insights into the Dutch government's stance and approach towards privacy, social media, and AI surveillance. This could potentially inform future policies and practices, contributing to a more comprehensive understanding of the global discourse on these critical issues.

1.4. Research approach

This research adopts a discourse analysis to examine the Dutch government's policy discourses on social media surveillance. Discourse analysis is a qualitative research method that investigates the use of language. It allows for an in-depth exploration of how language, both written and spoken, are used in the context of certain topics and the context of society. In the contact of this research, discourse analysis will be used to analyse the language used in policy documents, speeches, and other official communications from the Dutch government. The aim is to understand the underlying assumptions and ideologies that shape the policy discourses on social media surveillance. And while it could be possible to look into existing laws and policy's they merely reflect what is actually done by the government in regard to the issue. By looking into policy papers and such, it is possible to discover not only actions but also intentions, motives and reason why certain things are deemed important. It gives an insight into why certain choices are being made or might not be made by the government. To achieve this, this paper is structures in the following way. First there will be an outline of relevant core concepts in the theory chapter, then the chosen method, the discourse analysis will be explained more in the methods chapter. After this, the results of the analysis will be described and set out in the contact of the sub-questions. The last chapter will provide with an overall conclusion.

2. THEORY

2.1. Introduction

Now that the research question is clear, in this next chapter concepts will be set out and explained that are relevant to the topic of this research, social media surveillance. This chapter will further look into the concept of privacy and of safety and what they mean on their own, in relation to each other and in relation to the topic of social media surveillance. These two concepts are of great important to the understanding of the Dutch policy discourses and are widely used in the discussions on the topic of social media surveillance. It is important to understand the concepts at hand, since they support the analysis that is done later in this thesis. In this chapter the justification for all the concepts can be found. The core concept of this thesis, social media surveillance will first be looked into. What is social media surveillance and how is it described in the current research that is available. In addition to this, as mentioned before, the concept of privacy will be set out. What is privacy and what does it mean in the rapidly changing world of AI and social media surveillance. After this, safety as a concept will be discussed. What does safety mean and how does it relate to the topic of social media surveillance. Lastly the relation between tension field between safety and privacy in the context of social media will be theorised and examined. This chapter will end with a short conclusion on what these concepts will all mean for the rest of the thesis and what can be expected from the research based on the concepts. All these concepts and relations will be supported using academic literature, which will also lay the foundation to the analysis that will be done in this thesis. It offers a theoretical base which can be used to address the main research question.

2.2. Theoretical concepts

2.2.1. Social media surveillance

There are several features to social media surveillance, Trottier and Lyon (2012) argue that there are 5 key features of it that can be summarised in one sentence being: monitoring the individuals social networks in a changing online environment by using its activities and social ties, where users contribute to the identity construction of others. (Trottier & Lyon, 2012) This means that there is a profile build about an individual using information and data on the internet. Digital surveillance is something that has been a topic of policy discourses for a long time, especially since the rise of internet. As mentioned before, the topic gained popularity after the revelations of Edward Snowden, who in 2013 revealed a huge surveillance network of the National Security Agency of the USA. (Fuchs & Trottier, 2017) The rapid development of technologies is one of the big factors that enable social media surveillance, these technologies are able to configure enormous records of personal activities using the digital footprint every person leaves while using the internet. (Brown, 2014).

One of the tricky things of social media surveillance is that data is not solely collected based on the digital movements of the individual. The ties of this individual are something that majorly contribute to the data set of this one individual. It means that it is very hard to protect privacy online, if the connections of an individual are not concerned as much about the privacy as the individual. (Trottier, 2012) Most digital surveillance is tied up in the daily lives of individuals, tracking searches on the internet, engagements with friends on social media and posting content. (Jones, 2020) Social media surveillance is both seen in scientific literature as something that people are contributing to themselves, as Trottier & Lyon argue, but this contribution is also done by their network according to Brown. It is hard to say who is right in this instance, On the one hand, if the network of the individual plays a major role in building the database of one other individual, one might argue that this individual is helpless and cannot do anything about this. It is out of their power and influence. On the other hand, as Trottier & Lyon argue, shed light on the fact that while ones ties are building the others' databases it also mentions the activity of the individual, making the individual one with a choice in having these ties or not. Even though there are a lot of different ways of surveilling the internet, the discourse of social media surveillance will be the main focus for this research.

2.2.2. Privacy

Privacy is a term that has been used for a long time, but what is considered as private differs according to the time period and context, the society, and the people. The modern notion of privacy first appeared in "The Right to Privacy" written by Louis Brandeis and Samuel Warren, published in 1890. They defined privacy as "the right to be let alone", which has developed further over the course of time (Lukács, n.d.) Privacy as a value has not been popular before as it is right now, in the digital time. Through the use of social media networks and internet, the meaning of privacy has changed, for example wanting to share little information with people one is known with compared to more information with organisations, platforms and people we are not familiar with. And while people often think they are very privacy conscious, what is not realised is the digital footprint people are leaving. Where in the past to find something out about an individual one had to watch the person and actively collect the information, nowadays the profile is already existing on the internet and even created by the individual himself. (Gross & Acquisti, 2005) This not only changed the debate around privacy but also the interpretation and understanding of it. It makes the discussion around privacy even more complex, the first intention with privacy was to be let alone as was defined by Brandeis and Warren, but how should this be understood if one is let alone, their information was just public. Is the right to be let alone still sufficient when one is not disturbed but is still being watched using the profile one has created online for themselves, not being aware of the possible consequences.

The paper by Carmody et al. (2021) concludes that current legislation often is not sufficient enough yet when it comes to protecting the privacy of individuals. This also means that the current legislation is not adequate in the current situation of rapid development of artificial intelligence and poses a big challenge for legislators to fill this hole. (Carmody et al., 2021) And while this challenge is discussed by others too, research also shows that Dutch citizens show a greater trust in their government which results in a lower expression of privacy concerns. Cause for this is the belief that EU regulations would be able to protect citizens from huge privacy violations. (Hartog et al., 1999) While people often feel like they are protecting their privacy well enough, another sentiment can be found when looking at the discourse around social media. Research found that people can be indifferent about their privacy, especially when things like efficiency, safety and free services and products are in play. Individuals know that parties are collecting their private information, but they do not seem to mind that as much as one would expect. Another reason for an indifferent attitude towards privacy loss, can be the invisibility of the collection of the data that is happening. (Van Nieuwenhoven, 2019) All these different aspects show that privacy is not a one sided concept, it has many angles to be looked at and paid attention to, from having the right to be let alone, to be let alone but still be watched and followed via the profile one is making for themselves on the internet.

2.2.3. Safety

Safety is the result of risk existing or not, making it a variable that is hard to measure. This is why risk is often used as an antonym for safety. Risk is for example “an unwanted event which may or may not occur” (Roeser et al., 2012) making safety and how safe something is the result or outcome of the risk or lack thereof. Safety is discussed to be one of the most important things in the discourse of electronic surveillance, in which safety is the main reason and argument for the use of electronic surveillance. Safety on its own also changed over time, it was always seen as something physical for example not being attacked or hurt. Now the digitalisation of the environment made that the concept of safety was redefined and has gained new factors to be taken into account. On the one hand as something that can contribute to the physical safety and on the other hand adding new risks to safety of people, just not anymore on the street but on their phone or other digital aspects of their life. (Ronchi, 2019)

Safety is often used as a justification and an argument in favour of the implementation of AI making it an important concept in the context of social media surveillance. (Tiainen, 2017) The relevance of this justification can be found in literature. An example: in the police world a shift can be seen to intelligence-led policing dominated by the new technologies, the police started using, amongst other, enhanced predictive analytic technologies. With these strategies the police are able to analyse data, recognise patterns and predict possible risks more and faster than ever. (Fuchs, n.d.)In some discourses, for example in the US policy discourse on surveillance, a strong connection can be found between liberty or national identity, stating that without surveillance, the freedom of a country could be endangered, adding another argument for the use of surveillance. It can be argued that without surveillance the nation’s freedom could be at greater risk compared to the risks surveillance brings, making the debate complex. (Simone, 2009) And in defining safety, there seems to be no right or wrong, the various scientific publications highlight a different aspect on safety and how this has changed over time. The perception of being safe is therefore a difficult one to generalise, since this might differ from individual to individual. Most people preferer to be safe but might not understand the impact of what being safe means.

2.2.4. Tension between safety and privacy in the context of social media surveillance

Now that the concepts of safety and privacy have been explained, the next layer of the discussion is the complex relationship between safety and privacy in the context of AI and social media surveillance. Safety and privacy being in conflict with each other is not something new in this world, but the rise and rapid development of AI technologies has intensified the tensions between the two. AI introduced a new level of complexity to the political and ethical discussion of the topic. (Carmody et al., 2021) The use of AI in digital surveillance does not come without controversy, and raises complex questions about privacy, the ethical aspects of it and maybe the most important aspect, the delicate balance between individual rights and collective safety. A balance many policy makers have struggled with in the past. (Simone, 2009)

The development of AI offers opportunities to better safety of individuals and of society, for example through predictive policing, since it is able to analyse big batches of data faster than was possible before and is able to anticipate on criminal activities and with this increasing safety. (Fuchs, n.d.) Similarly, AI can make the digital environment a safer place with its ability to detect online threats and harmful content. (Jones, 2020) And while it might sound wonderful to life in a crime free world, where there is no threat, these safety benefits often come at the cost of the privacy of the individual. These AI systems rely on extensive data collection, including personal information that is collected in the digital environment, and not limited to the data individuals produce on their own, but also what their connections online produce. (Trottier & Lyon, 2012). Next to this, there is often a lack of transparency data collection online which makes it difficult for individuals to understand how their data can be or is used by whatever actor is in the picture. (Brown, 2014). And on top of that, research show different individual perceptions of safety and privacy, meaning there is no absolute right amount of safety and privacy. (Van Nieuwenhoven, 2019) Throughout publications the discussion on the value of safety versus privacy is an ongoing topic. Not without an exception researchers struggle with balancing these two values themselves in their research.

2.3. Conclusion

This thesis chapter set out the concepts that are relevant to answering the research question of this thesis. Social media surveillance is an evolving topic that will become more relevant over time. It is characterised by monitoring individual's online movements and has been used more and more with the further development of AI. Privacy, the right to be let alone, is now facing new challenges with the rise of AI and social media surveillance and current legislation often fails to protect individuals' privacy. Nevertheless, the Dutch citizens often have high trust in their government and express fewer privacy concerns compared to the American citizens. They believe in the EU and their regulations which will be able to protect them. The reality is unfortunately not always like that. Safety on the other hand is often used as a justification for the implementation of AI and electronic surveillance. Intelligence-led policing is therefore something that is being implemented more often at the police, these prediction technologies are used to analyse data, recognise patterns, and predict possible dangers. This tension between privacy and safety forms the core of the discussion around social media surveillance. And while social media surveillance could be a handy tool to ensure safety, it also poses risks to privacy. This complex relationship between privacy and safety is expected to be seen in the analysis of the Dutch policy discourse that is analysed in this thesis. In conclusion, the tension between safety and privacy is a complex issue with no easy solution. It involves balancing possible safety benefits with the obligation to respect and protect individual privacy. This thesis will provide with more context how the Dutch policy discourse envisions the relation of privacy and safety in the context of social media surveillance.

3. METHODS

The purpose of this thesis is to find the Dutch policy discourse on the relationship between privacy and safety, in the context of social media surveillance. The main research object of this research, and thus the case, is therefore the policy discourse on social media surveillance by the Dutch government. This case will be further explained in the first sub-chapter of the methods chapter. In order to discover the policy discourse of the Dutch government, a qualitative research design will be used for the research, which will focus on textual sources. How these textual sources will be collected can be found in the second sub-chapter. Lastly, the goal is to analyse the way in which the Dutch government voices its policy discourses on social media surveillance. How this analysis has been done through content analysis can be found in the third sub-chapter of this chapter. A coding scheme will also be provided in this chapter in order to show the operationalisation of the theoretical concepts in this analysis. At the end of this chapter there should be a clear overview of how the analysis was done in order to answer the research question.

3.1. Case description

The main research object of this research is the policy discourse of the Dutch government on social media surveillance, in particular how the Dutch government envisions the relationship between privacy and safety, two important arguments in the discussion. Social media surveillance by the Dutch government has been subject to discussions for a while now. Recently the Royal Dutch Marechaussee used pictures from a protest action and matched it to public sources like social media to identify activists. This method did not hold up in court and the cases were suspended, partly due to the inaccuracy of this method. (Van Der Parre, 2024) (Houwing, 2023) This was not the first time the topic of online surveillance got attention. Trouw previously revealed that the government was saving tweets to measure the satisfaction of the citizens (Keukenkamp, 2022), and the Volkskrant wrote an article about the municipalities using social media surveillance to be able to get a view on possible disturbances such as protests and riots. (Von Piekartz, 2021) Throughout this research the focus is on finding the Dutch policy discourse, which is their vision on the topic of social media surveillance, these visions can be found in policy papers and other documents. The same goes for the understanding of the topic, which is essential when making policy, does the Dutch government even understand what they are talking about is at question here. Next to documents, another indicator of vision and understanding could be how often debates are happening on this specific topic. Due to all this public attention, this topic also gained political attention, and after some debates and question this led to the writing of the "*Overheidsbrede visie Generatieve AI*" translated to the Government-wide vision Generative AI. This document sums up the vision of the Dutch government, the risks and opportunities and looks into the question of what legal frameworks are already in place concerning AI. It also proposes policies and actions. (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2024c) To add to this, the authority of personal information. Autoriteit Persoonsgegevens, started in 2023 with the monitoring of algorithms. (Autoriteit Persoonsgegevens, 2023) All these quick developments show the urgency of the topic, as it is also acknowledged by the Dutch government and show the relevance of the question in this thesis.

3.2. Method of data collection

This research will primarily focus on textual sources. These textual sources will primarily include policy documents, legal papers, government reports and official statements, these will be supplemented with academic literature related to social media surveillance and privacy regulations. The documents will be collected in the first place from the available websites of the Dutch government, related organisations, and others where these are published. This analysis will include a systematic examination of the language and narratives within these textual sources. It will be focused on identifying dominant discourses and key themes within these documents. This will also include an examination how concepts such as “safety”, “privacy” and “social media surveillance” are defined and framed within the discourse of the Dutch government, as well as their justifications for social media surveillance practices. These documents are a good resource to gather data from, since they represent the opinion or point of view of the government which make them a relevant source for the research, since policy papers and similar reflect the opinion of the government. The reason to use these kinds of documents for the research is because they are the best source that reflect on the discourse and development of AI and surveillance within the Dutch government. For example, motions that have been filed and discussed within the Dutch house of representatives, the Tweede Kamer, reflect a certain sentiment within the population, and the political mood of that moment.

As mentioned before, the textual sources that will be used will be including but not limited to policy documents, legal papers, reports by the government and others, and official statements. The documents will be collected on different website such as rijksoverheid.nl, overheid.nl, it-academieoverheid.nl and rdi.nl. These websites contain information published by the Dutch government on a variety of themes. Several search terms that can be used to find these documents are “Algoritme”, “AI”, “Privacy”, “Veiligheid” and “Online media”. The dataset contained of 29 documents, over 1100 pages, and were published by the various ministries, the National Police and semi-independent research organisations that wrote advisory reports for the government. It also included letters to the parliament, and motions that were discussed in parliament. All the documents that were used, were published in the past 10 years. These documents were selected because they indicated something on the vision of the Dutch government on the topics of safety and privacy, in relation with AI or social media surveillance, or just about social media surveillance of AI. These documents too say something about the sentiment around privacy and safety in the Dutch policy discourse of social media surveillance. By using documents that are not directly related to the topic of social media surveillance in the analysis, it is possible to somewhat predict certain choices that the Dutch government can make in regard to the topic. These documents also indicate a certain importance and value that is tied to the topic, if there is never any debate on this topic in parliament it indicates a sentiment that is or is not there. The dataset that will be used will be an original dataset, since the selected documents will form a new dataset, which were not yet used in other research. In these documents the different concepts explained in the theory part of the research proposal can be found, such as privacy, and safety, since they form the core of the Dutch discourse around the use of AI.

3.3. Method of data analysis

After all the data is collected the next step is to analyse all the documents. For the purpose of this research, a textual analysis is considered best suited for answering the research question. Textual analysis can add depth of understanding to topics, whereas quantitative research usually focuses on giving one concrete and clear answer to a research question. With textual analysis, an extra layer is added, which is the understanding of the research subject and therefore gives the chance to delve into the underlying reasoning, values, and ideologies within the discourse of social media surveillance and privacy. For this research a discourse analysis will be executed, but what is a discourse analysis and what are the problems with a discourse analysis? As defined by Taylor (2013) a discourse analysis has many ways of implementation. The discourse analysis refers therefore "to a research approach in which language material, such as talk or written texts, and sometimes other material altogether, is examined as evidence of phenomena *beyond the individual person*". In a sense, a discourse is discussion through which beliefs and others are displayed. (Taylor, 2013). It focuses on the investigation of text and seeing it in the context of the society or the societal mood of that time. Something that needs be taken into account, is that discourse analyses can be subject to subjectivity, since it can depend on the researchers interpretation what is deemed important and whatnot. One way to prevent this is to not pick and choose which quotes are deemed relevant for the sake of the research but keep all the quotes with the keywords in the dataset, to prevent data manipulation.

In order to operationalise the discourse analysis, Atlas.ti will be used as the main tool to analyse the dataset. Atlas.ti is a coding tool, which can help to process big batches of textual data into measurable data through the use of a coding scheme and the quantification of the textual data. After loading all the documents and papers that will be used in the analysis into Atlas.ti, the first step in the analysis is to start coding the content of the documents. This involves scanning and reading through them and assigning codes according to the coding scheme which can be found later in this chapter. All these codes say something about the sentiment of the Dutch government in its policy discourse around the topic of social media surveillance and AI. In this first step sentences with words like "veiligheid", "privacy", "publiek doel", "gevaar" and synonyms of these words will be marked and assigned a code when relevant to the topic of the research. These codes indicate something about the discourse that is found in the source. The next step would be to check the data, are there codes which are used significantly more or less compared to others? It is good in that case to look over the documents again to prevent it being a structural mistake of missing a topic that should have been coded. If after the check this indeed is what the data looks like, that is also fine. It could be the case that some topics are reflected less on in these documents in this specific dataset. The third step would be to look into the data and see where patterns can be recognised. In case one code is assigned a lot, this most probably indicated something about the Dutch policy discourse of social media surveillance or AI. Based on this quantification of the textual data the main research question and sub-questions can be answered using the number of mentions of a code and using specific examples from the texts. The coding is a way to quantify the value of privacy and safety in the Dutch policy discourse of social media surveillance. These specific examples form an important basis for the arguments and the support of the answers to the questions in the thesis.

Provided below is the coding scheme used for the analysis. In this coding scheme, there are two concepts that will be coded in the textual data that will be analysed. First of all privacy, the goal was to find the discourse on privacy and the discussion around it, and also with what sentiment privacy is perceived. Is the development negatively or positively related to privacy, is it not particularly clear, or maybe even neutral. How does it affect the aspect of privacy is a question that is central for this concept. The same thing will be done for safety and the same questions apply for this concept. These codes are designed to be able to figure out how the arguments of privacy and safety are used in the specific documents. This coding scheme was composed using keywords that were chosen for the analysis. After highlighting all the quotes that contained said keywords, the coding scheme was applied to the quotes in a deductive way, looking into every quote and what the meaning, load, and sentiment were of the sentence. By applying the coding scheme in such a way, it was possible to look into the meaning of the sentence and what was meant, rather than just applying a code based on a word. More nuance was possible in the coding process.

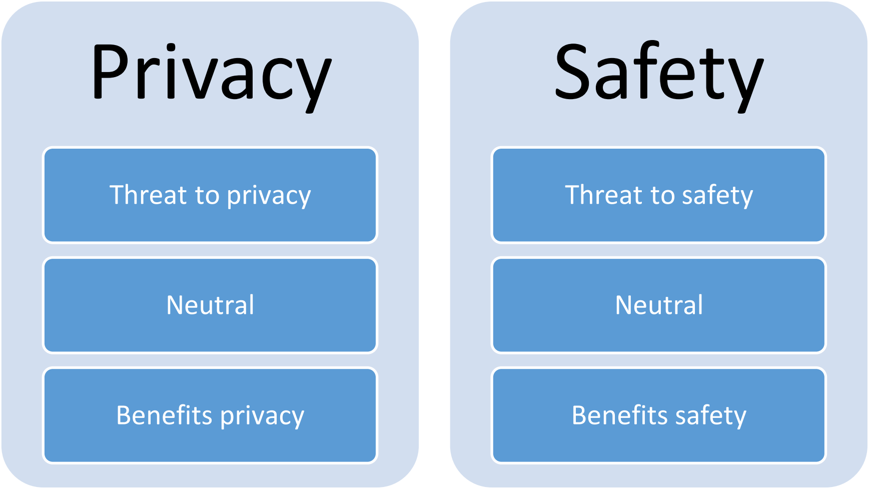

Figure 1: Coding scheme

3.4. Conclusion

This chapter provided with a detailed description of the methods that will be used in order to answer the main and sub research questions of this thesis. It provided with the case for this research, which is how the Dutch government balances safety and privacy in the discussion around social media surveillance and AI. The data that is collected for the sake of this research, are various document that are related to the topic of the research and come from various sources related to the Dutch government and its institutions but are also supported by reports that were addressed to the government. These documents will provide with an insight into the policy discourse of the Dutch government and how the government interprets the questions and dilemma's that come with AI use. This chapter ended with a step by step description of how the data that is collected will be analysed using a discourse analysis approach. The operationalisation of the research method involves the use of Atlas.ti and a coding scheme which were provided in the chapter. The combination of the research method, the operationalisation and the quantification of the textual sources, the chapter shows how the chosen method will provide with the answers to the research questions at hand in the following chapters of this thesis.

4. ANALYSIS

4.1. Introduction

In this next chapter, the results of the textual analysis executed in this research is presented. The chapter starts with an analysis of the discourse on safety as can be found in the various sources of the Dutch government. Next, how privacy is described was analysed based on the various textual sources of the Dutch government. The second and third sub-chapters are focused on the concepts of safety and privacy on their own and how they are portrayed in Dutch policy. The fourth sub-chapter is focused on the Dutch policy discourse of the tension field between safety and privacy and how this is envisioned by the Dutch government according to their discourse. This analysis was done based on the methods described in the methods chapter and contain of an analysis of various policy papers. It is supported by the theory that was collected and set out in the theory chapter above and thus is a combination of analysis and theory, thus integrating both the analysis and theory in order to provide with comprehensive understanding. At the end of this chapter, the firth and last sub-chapter, the sub-questions from the introduction are answered, these answers will form the base for the answer to the main research question. This answer can be found in the conclusion chapter, placed after the current chapter.

4.2. Privacy – a buzz word that is liked by the government

To start off with the positive sentiment towards the concept of privacy. The Dutch policy discourse shows a fast amount of attention for privacy, it is mentioned in almost every paper that was analysed for this research. The Dutch government seems to define privacy the same way Brandeis and Warren did as “the right to be alone”(Lukács, n.d.) and portraits privacy as an important value that needs protection. But privacy is also understood to be a complex value where deciding what is right of wrong seems to be difficult. The analysis shows a commitment to privacy by the Dutch government, which is highlighted by the quotes in this paragraph. These quotes illustrate the governments proactive stance in ensuring the privacy of its citizens in the context of AI. The first quote is “Bij het voorkomen van schade is het van belang dat de privacy van mensen wordt gewaarborgd en dat goed wordt omgegaan met persoonsgegevens.” (Algemene Rekenkamer, 2022, p. 30). This quote stresses the importance of safeguarding privacy and handling data in a proper way and shows that privacy is a sensitive value. It illustrates the potential harm data collection and the misuse of it can pose for the individual, and this is recognised by the Dutch government. The second quote is one that was taken out of a policy brief written by the Ministry of the Interior and Kingdom Relations “Het gebruik van persoonsgegevens voor AI-systemen bevestigt ook de noodzakelijkheid om de digitale veiligheid op orde te hebben” (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2022, p. 11). This policy letter focuses on AI, public values and human rights, and this passage specifically highlights the recognition by the ministry, and thus the government, that digital security is of high importance. Since the word “noodzakelijk” was used in this document, it shows to be envisioned one of the fundamental tasks to ensure safe use of AI in the eyes of the Dutch government.

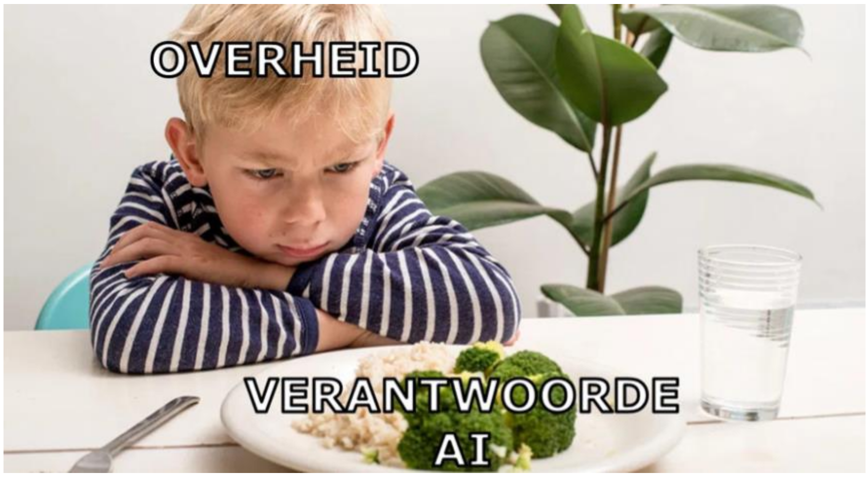

Figure 2: Meme used in a presentation by the National Organization for Development, Digitalization and Innovation (Rijksorganisatie voor Ontwikkeling, Digitalisering en Innovatie, 2023)

Naturally, the interpretation of privacy cannot be only positive and in the interest of protecting privacy. There is also the negative sentiment towards the concept of privacy, while the majority of the expressions around the topic of privacy are positive, there are a few examples that show possible threats for privacy in the Dutch policy discourse. The first example is surprisingly enough a meme, that was used in a presentation explaining AI to people working at the government, given by the National Organization for Development, Digitalization and Innovation. In this presentation there is attention for both sides of the discussion. On the one hand the use of AI, and most importantly brings attention to the fact that AI is not something that is fantasy or can happen in the future anymore, hence the title "AI is geen Science Fiction" (Rijksorganisatie voor Ontwikkeling, Digitalisering en Innovatie, 2023, p. 19). The picture shows a child looking angry at its plate, where broccoli is laying. The kid is the government in this meme, and the broccoli or his plate represents responsible AI. This is interesting because earlier in the presentation, privacy infringement is illustrated as one of the biggest risks that AI can have impact on. And looking at this picture it almost seems that the government does not want responsible AI and take its responsibility in protecting against the risks AI can pose. The second example is a passage from a letter to parliament titled: *Aanbiedingsbrief (overheidsbrede) visie op generatieve AI*. In this letter, the main focus is the vision of the Dutch government that they have for generative AI. The quote "Risico's en uitdagingen Het gebruik van generatieve AI kan negatief van invloed zijn op publieke waarden zoals non-discriminatie, privacy en transparantie" (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2024a, p. 4) shows awareness about a possible threat AI could be to privacy and other values but indicates it as a mere possibility rather than a reality. It shows that privacy is a concept which is positioned complexly related to other values in this discussion. Privacy shows to be an ambiguous concept, where even the government is not sure sometimes what it is, but they are sure that it is something that is worth protecting. This quote also illustrates that privacy is used as a buzz word, to signal importance of the topic, not really being aware what that would contain. Or even just leaving it with empty words, since this quote does say it is found important to protect, but this has not action tied to it. They are ‘simply” words without volume, and often not followed up on with action to strengthen.

The Dutch policy discourse on AI presents a dichotomy. On the one hand a strong commitment to privacy, illustrated by the frequent mention in the analysed papers, and the proactive stance of the government in ensuring the privacy of its citizens. This positive sentiment is shown in the emphasis on the importance of safeguarding privacy and proper data handling, by the government and other actors. The government recognises the potential harm that the use of AI and data collection can pose to individuals. On the other side, there are a few indications of potential threats to privacy and they seem to be not taken too seriously by the Dutch government, analysing the language and certain words used in its communication. Overall, the Dutch government shows more attention how to ensure privacy rather than endanger it. This contrast is well illustrated in the quote “Er is veel aandacht voor privacy, beeldvorming en transparantie, maar tegelijkertijd wordt de impact op publieke waarden en de grondrechten van burgers slechts zijdelings meegenomen in de ontwikkeling van AI” written in a report by TNO (TNO, 2023, p. 28). While there seems to be much attention to privacy, this fundamental right is not always considered to be the most important value or thing to account for in the discussion of the development and use of AI. It is often used as a buzz word to keep emotions quiet by mentioning the word frequently, but in reality actions lag behind the intentions the Dutch government seems to have in its policy discourse on social media.

4.3. Safety – the main argument but two sides of the same coin

The main reason for the Dutch government to use AI seems to be safety, as can be found in various documents that were analysed. Safety seems to be the main motivation of the Dutch government, and this can be found in the definition in a document of the Ministry of Defence. "Social media monitoring is het bijhouden en analyseren van uitingen in de sociale media. Dit kan voor verschillende doeleinden worden toegepast zoals het snel op vragen en kritiek vanuit de samenleving/consumenten kunnen reageren, het analyseren van trends (bijv. of men positief of negatief spreekt over een organisatie), voor het monitoren van evenementen ten behoeve van de veiligheid en beveiliging of situational awareness" (Ministerie van Defensie, 2022, p. 14), this passage does not only clearly defines social media surveillance, as it is understood by the ministry of Defence, but it also entails the main envisioned goal, safety. It focuses on analysing trends and big batches of data, and this is a similar definition that can be found in the literature. These both focus on analysis and data as a justification for certain choices that can be made in the name of safety. (Fuchs, n.d.) This benefit of AI is also shown in the governments vision on generative AI where they state: "Het kabinet wil dat generatieve AI in dienst staat van het vergroten van het menselijk welzijn en autonomie, duurzaamheid, welvaart, rechtvaardigheid en veiligheid" (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2024b, p. 4). Their goal is to make the purpose of AI to be of service to the safety of the citizens and just to serve the people in general. It shows the belief of the Dutch government in AI and the confidence that it can positively impact various aspects of the lives of the people, including the safety aspect. Lastly, the police have an important task in ensuring safety in the Netherlands and they seem to be very clear ‘Het uitgangspunt hierbij is: Veiligheid Voorop’ (Ministerie van Algemene Zaken, 2024, p. 22)

And while the Dutch government recognizes the potential benefits of using AI in order to ensure safety, it also acknowledges the risks and challenges that arise with its use. This is evident in the letter sent to parliament about the progress on AI and algorithms. Here, the worry of using AI shines through in the quote “Wanneer algoritmen of artificiële intelligentie in een verkeerde context, op verkeerde wijze of met het verkeerde doel worden ingezet kan de impact enorm zijn.2 Publieke waarden en fundamentele rechten zoals privacy, non-discriminatie, autonomie en menselijke waardigheid kunnen onder druk komen te staan waardoor burgers in de knel kunnen komen” (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2022b, p. 1). The use of the word ‘wrong’ indicates a value judgment by the Dutch government and seems to be something it wants to prevent. AI can not only pose threat to safety as it is known now, according to the strategical action plan for AI, which was published in 2022, the report also foresees a change in the way safety and threats emerge. “De toenemende toepassing van AI-technologieën in de samenleving maakt dat er nieuwe soorten kwetsbaarheden en veiligheidsdreigingen ontstaan” (Ministerie van Algemene Zaken, 2022, p. 50) points out that the increase of the use of AI technologies in society can lead to the emergence of new types of vulnerabilities and security threats. These documents emphasize a certain level of caution the Dutch government shows in its approach towards the use of AI for safety.

The Dutch government sees big chances in using AI for the sake of ensuring safety of its citizens. The dilemma for the Dutch government is whether the advantages outweigh the disadvantages, and this dichotomy is shows in its statements and sentiment. While the Dutch government sees the potential benefits, they also seem to be aware of the possible risks, it could be described as cautious optimism. They recognize the transformative potential of AI and improving the ways of ensuring safety and enhancing security. The approach of ‘safety first’ is an important argument for the use and development of such technologies and reflects a commitment to the safety of its citizens. On the other hand, the Dutch government is aware of the risks and challenges associated with the use of AI. They acknowledge that when used poorly or with the wrong intentions, AI can have a significant negative impact and endanger public values and fundamental rights. They also recognize that the use of AI, and the increase of it, can lead to the emergence of new types of vulnerabilities and safety threats. The Dutch government sees the potential benefits, but they also are aware of the risks. This awareness informs the approach to regulation, as they strive to ensure that the use of AI does not endanger safety as they are trying to improve it. It is the main argument in favour of the use of AI, since it can improve the direct safety of the society, but nonetheless also pose a threat, there are two sides of the same coin.

4.4. Privacy or safety - a choice the government does not want to make

In total there were 217 quotes highlighted in the whole dataset. Interestingly enough, 148 of them mentioned something about privacy, and only 87 mentioned safety. This might seem that privacy gets more attention, and while it is mentioned more, the focus and the action is more on the side of safety. As the analysis shows, privacy and safety are on their own already conflicting values in the discussion of AI, which the Dutch government tries to navigate as it is a complex issue. And while privacy and safety seem like conflicting issues, this does not seem to be the case in all the communication of the Dutch government. In some instances, the government sees the two values not as opposing and competing values in the discussion but as aspects that can go hand in hand. As stated in a compilation letter to the parliament, about the public control on algorithms the values safety and privacy are mentioned in one and the same sentence, making it look like they seem to be on the same level of priority to the government. "We hebben de plicht om grondrechten en publieke waarden – in het bijzonder veiligheid, democratie, transparantie, zelfbeschikking, non-discriminatie, participatie, privacy en inclusiviteit – te beschermen en de taak om de kansen van de digitale transitie te verzilveren door een innovatief en gelijk economisch speelveld te creëren: met eerlijke concurrentie, consumentenbescherming en brede maatschappelijke samenwerking" (Digitale Overheid, 2022, p. 1), it is not only shown as a priority but pictured as a duty of the government to protect values and constitutional rights of the Dutch citizens. But this quote not only shows a commitment, because after this publication, at the end of 2022, the Algoritme register was published.

This register is a website where organisation have to publish the information on the algorithms that they are using in the context of transparency. And while this kind of transparency is highly encouraged, this still does not make the tension between the values safety and privacy less. This register might provide with transparency, but this is only an action to establish which algorithms are in place. Nor the letter to parliament, the intention document or other documents tie an action to the register, making it mainly a log for algorithms. "Bedrijven en overheden zijn gebaat bij hoogwaardige AI-toepassingen om zowel economische als ethische en veiligheidsredenen" (Ministerie van Algemene Zaken, 2022, p. 34), this quote shows that not only is it important to ensure the safeguarding of certain rights and values in the AI transitions. Businesses and government can also benefit and strengthen these values the government tries to protect. AI is an instrument that can both strengthen and weaken safety and privacy. This can be interpreted as a commitment of the government to ensure the digital transitions benefits all sectors and aspects of society, while safeguarding individual rights and public values. They are the same side of the coin, both crucial in the digital age.

The other side of this coin is the conflicting position safety and privacy seem to be found. This tension between the two values which are supported by the following two quotes. The first one illustrates how safety can be ensured, at the cost of privacy "Deze tools zorgen voor hogere efficiëntie maar de privacy-inbreuk voor de betrokkenen kan ingrijpender zijn" (Ministerie van Defensie, 2022, p. 14). The use of AI can enhance the efficiency of tracking down criminals and prevent public chaos, but the infringement of the individuals' privacy can be at a higher cost than what it brings. It highlights the trade-off between the efficiency of ensuring safety, and privacy and suggests that while technological developments, such as social media surveillance, can improve safety, they can do so at the expense of individual privacy. And these infringements can be more invasive for the individuals involved. The second quote compliments the dilemma: "Een kader waarin bijvoorbeeld staat dat privacy altijd voorgaat op veiligheid past daar niet goed bij" (Digitale Overheid, 2022, p. 5). This illustrates the tension and implies that rigid frameworks that prioritises privacy over safety does not fit the situation. This can be interpreted as the recognition by the government of the conflicting nature of the values safety and privacy. It suggests also that the dilemma between the two values that it is important to be flexible and assess situations not based on a clear rule but based on the situation. It is not possible to prioritise on over the other, and while it might not be the most effective approach, it is necessary to ensure a nuanced balance.

This analysis shows a complex relation between privacy and safety in the Dutch government's approach to AI. The government appears to not view these two values inherently opposing each other, but also as two that can coexist and even have the same importance and priority. This perspective is reflected in the government's commitment to protect individual rights and public values, including safety and privacy, in a time of digital transition. AI technologies can also serve the government in enhancing economic and ethical aspects, including safety and privacy. However, there are instances where safety and privacy are positioned in opposition. The government acknowledges that while AI can enhance safety efficiency, it can also lead to more invasive infringements on individual rights. This recognition of the government of the trade-off emphasizes the need for a flexible approach that assesses each situation individually. A rigid framework I not realistic in this instance that prioritises one value over the other. The Dutch government seems to be not really sure which way to go and what values to prioritise, there is attention for both aspects, and this can be characterised as a cautious way to navigate the tension between privacy and safety. The government is able to reflect both on the transformative potential of AI as well as the possible safety threats its use may introduce.

4.5. Conclusions of the sub-questions

This chapter was a description of the analysis that was done for this thesis. Now that the complex relations between privacy, safety and AI is clear the research question can be answered. In the last paragraph of this analysis chapter, the sub questions from the introduction will be answered based on the observations and analysis that were done during this research. One of the main take aways from the analysis is that both safety and privacy are ambiguous concepts, values, there is not one definition for the, which is followed by the government which makes the questions around the topic of social media surveillance very complex. In the next chapter, the conclusion, the main research question will be answered.

4.5.1 The vision on social media surveillance of the Dutch government

The first question that will be answered is *"How does the Dutch government envision the role of AI in its own social media surveillance?"* and the short answer to this question is that there is no clear published vision of the Dutch government. During the analysis it appeared that both the National Police (Ministerie van Algemene Zaken, 2024) and Defensie (Ministerie van Defensie, 2022, p. 14) are familiar with the technology of social media surveillance. The National Police mentions it in their yearly report as an option, but also shows caution in regard to the use of these technologies. Defensie on the other has already used said technologies but after a report by the data protection officer of the ministry of defence they temporarily paused the majority of these operations. The main motivation for this choice was the lack of legal framework on the base of which these activities could proceed on. The report stated that these activities will be paused until further notice. The main concern of both the National Police as well as from the ministry of Defence around the use of social media surveillance appears to be privacy, but they do see it as a good instrument to get a grip on the complex situation that social media puts safety in, in the current context. And while these two actors are not the Dutch government, it could be reflection of the vision of the government on the use of social media, but more information on that topic is still to be published by the Dutch government.

4.5.2 Privacy and safety as understood by the Dutch government

The second sub question in this thesis is *"How are privacy and safety understood in the context of surveillance by the Dutch government?"* and this is a twofold question. Privacy is something that the Dutch government seems to acknowledge as one of the main arguments against the use of . It is often defined as the right to be let alone and this is also the definition that the

Dutch government seems to be following. When ensuring privacy, this often means that the Dutch government lets the citizens be, as opposed to actively being involved in the details of their live, which is a part of social media surveillance. Safety is understood by the Dutch government as an important value that needs protection from the Dutch government. It is one, if not the main argument in favour of the use of social media surveillance and AI. While the use of AI could possibly not only protect safety and ensure it, the government sees also possible dangers to safety when the use of AI will be increased. But which of these two value is perceived as more important than the other is not clearly described by the Dutch government. It is quite the opposite where the government sees it as a task to balance these two values, not defining which one precedes the other.

4.5.3 Tension between privacy and surveillance

The last sub question that needs to be answered is specifically regarding the tension between privacy and surveillance. The answer to the question *"How does the Dutch government view the tensions between privacy and surveillance?"* is that it is a complicated relation. The Dutch government clearly acknowledged that there is a complex relation and sees the topic from two sides. On the one had they see AI surveillance as something that is possibly a huge threat to the individual privacy of their citizens. It can improve the overall safety of individuals and the society, but probably at the cost of individual privacy. They do show a strong commitment to privacy and emphasise the importance of safeguarding privacy, and the responsibility that lies with the government. On the other hand, there are also chances in the use of such AI technologies to improve the privacy of citizens. But most importantly to improve the safety of the society, which the government also sees as an important value to protect. The benefits that the use of AI surveillance bring, seem to outweigh in some situations the threat it poses to privacy. This dilemma is distinctly reflected on in the publication that were analysed. The Dutch government is planning to proceed with caution when planning and in the end implementing technologies as such. But this dichotomy also suggests that while there is a lot of attention to privacy, it is not always the most important argument in the discussion of the development and use of AI. The Dutch government tries to balance the benefits of AI with the needs to protect privacy.

5. CONCLUSION

5.1. The discussion of privacy and safety in the Dutch policy discourse

This research explored how the Dutch government, in its policy discourses, envisions the relationship between privacy and public safety in its social media surveillance via AI. The central question that will be answered in this conclusion is *"How does the Dutch government, in its policy discourses, envision the relationship between privacy and public safety in its social media surveillance via AI"*. This complex issue is a core topic in the debate on the use of technologies for maintaining safety and order. The Dutch government's discourse recognises both the potential and the risks that are associated with the use of social media surveillance and AI. On one hand, the use of AI technologies offer significant benefits in terms of assuring public safety, they are able to enhance efficiency of tracking down criminals, predicts potential threats via social media. (Ministerie van Algemene Zaken, 2024) All this with the use of extensive data analysis, as is discussed in scientific research published on the topic of social media surveillance (Trottier, 2012). These capabilities are crucial for maintaining safety in an increasingly digitalised world. The discourse shows huge advantages for safety, if AI can be used for that purpose, thus the discourse reflects quite positive on the use of AI for safety. However, in the discourse of the Dutch government, a strong commitment to privacy is highlighted. Privacy is a value that is seen as a fundamental right, that needs protection as new technologies emerge. This commitment and awareness are reflected in various policy documents and statements, where privacy is mentioned not once as a value and right that must not be endangered. Research shows that Dutch citizens show great trust in their government when it comes to protection of their privacy and this is not without reason (Hartog et al., 1999) . The government acknowledges the potential risks that extensive data collection, which is needed for social media surveillance, and AI can pose to individual privacy and freedom. There is therefore a clear recognition of the need to balance the benefits of the enhancement of safety and the obligation to protect personal privacy.

With the introduction of AI for surveillance, the theory is that a new level of complexity is added to the discussion and the tension between privacy and safety (Carmody et al., 2021), it was expected that this tension would also appear in the real life world. This assumption was correct since the tension between these two values, is also a topic that is discussed frequently in the Dutch policy discourse. While the government sees AI as a valuable tool for enhancing public safety it also emphasises the importance of safeguarding privacy. The duality of this topic is evident in the cautious approach the government is showing towards the implementation of AI technologies. Policy documents often stress the need for a legal framework and transparency to ensure that AI does not infringe upon individual rights. At the same time, the Dutch policy discourse shows awareness that a rigid framework is not always the answer for the dilemma's that the use of AI brings with it and recommends a case by case approach. In summary, the Dutch government's policy discourse views the relationship between privacy and public safety in its AI-driven social media surveillance as one that needs careful balancing. This does not come as a surprise since many political actors have struggled or are struggling with the balancing act and research showed the same phenomenon. (Simone, 2009) The government shows in its discourse the intention to use AI for public safety, while maintaining a strong commitment to the protection of individual privacy. The balancing act is framed in the discourse as caution, transparency and ethical responsibility, ensuring that the use and implementation of AI technologies align with the values of the Dutch democratic society of today.

5.2. Suggestions for further research

Previous research that was done on this topic, focused on privacy and safety as values on their own. One of the goals of this research was to close the knowledge gap that was identified in the introduction chapter of this thesis, which is how the Dutch government perceived social media surveillance in combination with AI, and the tension that safety and privacy add to the discussion. And although the Dutch government seems to not have a clear vision yet on how they envision social media surveillance, this research provided with insights how the Dutch government interprets the values privacy and safety. The reports of the National Police and Defensie have given a slight insight in to how social media surveillance is perceived by these organisations but this does not fully reflect the policy discourse of the Dutch government. Nevertheless, social media surveillance is already happening in the Netherlands, but not very vocally, These insights might be useful when it comes to further research that can be done further on this topic. While this thesis provided valuable insights into the Dutch government's understanding of privacy and safety in the context of AI, it also highlights areas for further investigation. A comparative analysis on different countries their approach to AI surveillance could be of help for the Dutch government as to how to shape possible policies in the Netherlands. This research could help understand how other democratic nations balance privacy and safety in their policies and how these could be adopted in the Netherlands. Another thing that requires further research are the practical implications of these policies, further research could focus on how these policies are translated into practice and how they impact both the public safety and individual privacy. This research could be done at a moment when social media surveillance is implemented and used by the government. It would be possible to look into already existing cases to predict possible results for the Dutch situation.

5.3. Practical implications

This research is not only of value for the scientific world, based on this research several practical implications can be drawn for policy makers. The most important one is the clear need for developing a legal framework that clearly define boundaries and ethical guidelines for the use of AI surveillance. In order to achieve this it is firstly important that the debate on this topic keeps going, this means the public debate but also the debate in parliament needs to keep going to exert pressure on the legislators. This is a political issue that needs to be solved in the political arena. The main issue is the lack of guidance and legal framework that executive powers, such as the National Policy and Defensie, face right now on the topic of social media surveillance and the use of AI. The question at stake is then how the Dutch government envisions the role of AI at this moment, but also in the future. Due to the rapid development of these technologies it is of utmost importance to not only make legislation for this moment but look further how these questions can be overcome in the future. These frameworks should ensure that these technologies are used responsibly and according to the democratic standards. Lastly, this thesis also could provide with more understanding, for the public but also for policy makers what the situation is at the moment and hopefully relax the tension between privacy and safety in the discussion of social media surveillance and AI and ensure that technological development serve the public without compromising fundamental rights.

REFERENCES

Algemene Rekenkamer. (2022, May 17). *Algoritmes getoetst*. Rapport | Algemene Rekenkamer. https://www.rekenkamer.nl/onderwerpen/algoritmes/documenten/rapporten/2022/05/18/algoritmes-getoetst/

Autoriteit Persoonsgegevens. (2023, January 16). *Algoritmetoezicht AP van start*. Retrieved May 19, 2024, from https://www.autoriteitpersoonsgegevens.nl/actueel/algoritmetoezicht-ap-van-start

Brown, I. (2014). Social media surveillance. *The International Encyclopedia of Digital Communication and Society*, 1–7. https://doi.org/10.1002/9781118767771.wbiedcs122

Buro Jansen & Janssen. (2017, October 4). *Social Media Surveillance in Nederland*. Retrieved April 2, 2024, from https://www.burojansen.nl/observant/social-media-surveillance-in-nederland/

Carmody, J., Shringarpure, S., & Van De Venter, G. (2021). AI and privacy concerns: a smart meter case study. *Journal of Information, Communication & Ethics in Society*, *19*(4), 492–505. https://doi.org/10.1108/jices-04-2021-0042

Digitale Overheid. (2022, December 23). *Kamerbrief Publieke controle op algoritmen - Digitale Overheid*. https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/publieke-waarden/dossier-documenten/kamerbrief-publieke-controle-op-algoritmen/

Feldstein, S. (2022). AI & Big Data Global Surveillance Index (2022 updated). *Mendeley Data*. https://doi.org/10.17632/gjhf5y4xjp.4

Freedom House. (n.d.). Social media surveillance. In *Freedom House*. https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance

Fuchs, C. (n.d.). *Social media surveillance*. https://web.archive.org/web/20190711113414id_/http://www.fuchs.uti.at:80/wp-content/DS.pdf

Fuchs, C., & Trottier, D. (2017). Internet surveillance after Snowden. *Journal of Information, Communication & Ethics in Society*, *15*(4), 412–444. https://doi.org/10.1108/jices-01-2016-0004

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *ACM*. https://doi.org/10.1145/1102199.1102214

Hartog, D. N. D., House, R. J., Hanges, P. J., Ruiz-Quintanilla, S. A., Dorfman, P. W., Abdalla, I. A., Adetoun, B. S., Aditya, R. N., Agourram, H., Akande, A., Akande, B. E., Åkerblom, S., Altschul, C., Alvarez-Backus, E., Andrews, J., Arias, M. E., Arif, M. S., Ashkanasy, N. M., Asllani, A., . . . Messallam, A. A. (1999). Culture specific and cross-culturally generalizable implicit leadership theories. ˜ *the œLeadership Quarterly/˜ the œLeadership Quarterly*, *10*(2), 219–256. https://doi.org/10.1016/s1048-9843(99)00018-1

Houwing, L. (2023, October 18). *Koninklijke Marechaussee laat zien waarom we geen gezichtsherkenning willen*. Bits of Freedom. https://www.bitsoffreedom.nl/2023/10/18/koninklijke-marechaussee-laat-zien-waarom-we-geen-gezichtsherkenning-willen/

Jones, R. H. (2020). Discourse Analysis and Digital Surveillance. *Cambridge University Press eBooks*. https://doi.org/10.1017/9781108348195

Keukenkamp, S. (2022, October 7). *Overheid verzamelt tweets zonder dat je het weet. 'Problematisch', stellen experts*. Trouw. Retrieved May 19, 2024, from https://www.trouw.nl/economie/overheid-verzamelt-tweets-zonder-dat-je-het-weet-problematisch-stellen-experts~b0263e44/

Lukács, A. (n.d.). What is Privacy? The History and Definition of Privacy. *CORE Reader*. https://core.ac.uk/reader/80769180

Lyon, D. (2015). *Surveillance after Snowden*. https://cippic.ca/uploads/Lyon-SurveillanceAfter%20Snowden.pdf

Ministerie van Algemene Zaken. (2022, June 7). *Strategisch Actieplan voor Artificiële Intelligentie*. Beleidsnota | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/beleidsnotas/2019/10/08/strategisch-actieplan-voor-artificiele-intelligentie

Ministerie van Algemene Zaken. (2024, May 14). *Jaarverantwoording Politie 2023*. Jaarverslag | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/jaarverslagen/2024/05/15/nationale-politie-2023

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2022a, January 18). *Handreiking non-discriminatie by design*. Rapport | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/rapporten/2021/06/10/handreiking-non-discriminatie-by-design

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2022b, December 4). *Beleidsbrief AI publieke waarden en mensenrechten*. Beleidsnota | Kennis Van De Overheid.

https://www.kennisvandeoverheid.nl/documenten/beleidsnotas/2019/10/08/beleidsbrief-ai-publieke-waarden-en-mensenrechten

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2024a, January 18). *Overzicht moties en toezeggingen die betrekking hebben op de overheidsbrede visie op generatieve AI*. Publicatie | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/publicaties/2024/01/18/overzicht-moties-en-toezeggingen-die-betrekking-hebben-op-de-overheidsbrede-visie-op-generatieve-ai

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2024b, February 7). *Overheidsbrede visie Generatieve AI*. Rapport | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/rapporten/2024/01/01/overheidsbrede-visie-generatieve-ai

Ministerie van Defensie. (2022, December 19). *Onderzoek naar social media monitoring bij het ministerie van Defensie*. Rapport | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/rapporten/2022/08/25/onderzoek-naar-social-media-monitoring-bij-het-ministerie-van-defensie

Rijksorganisatie voor Ontwikkeling, Digitalisering en Innovatie. (2023, June 23). *AI is geen Science Fiction* [Slide show]. https://www.rijksorganisatieodi.nl/binaries/rijksorganisatieodi/documenten/publicaties/2023/06/22/presentatie-odi-ai-20-juni-2023/20230620+-+Presentatie+ODI+V3+-+pdf.pdf

Roeser, S., Hillerbrand, R., Sandin, P., & Peterson, M. (2012). *Handbook of Risk Theory*. SpringerLink. https://link.springer.com/referencework/10.1007/978-94-007-1433-5

Ronchi, A. M. (2019). Safety and security. In *Springer eBooks* (pp. 43–108). https://doi.org/10.1007/978-3-030-00746-1_4

Simone, M. A. (2009). Give me liberty and give me surveillance: a case study of the US Government's discourse of surveillance. *Critical Discourse Studies*, *6*(1), 1–14. https://doi.org/10.1080/17405900802559977

Taylor, S. (2013). *What is Discourse Analysis?* https://doi.org/10.5040/9781472545213

Tiainen, M. K. (2017). (De)legitimating electronic surveillance: a critical discourse analysis of the Finnish news coverage of the Edward Snowden revelations. *Critical Discourse Studies*, *14*(4), 402–419. https://doi.org/10.1080/17405904.2017.1320296

TNO. (2023, March 7). *Quickscan AI in publieke dienstverlening II*. Rapport | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/rapporten/2021/05/20/quickscan-ai-in-publieke-dienstverlening-ii

Trottier, D. (2012). *Social media as surveillance: Rethinking Visibility in a Converging World*. Ashgate Publishing, Ltd.

Trottier, D., & Lyon, D. (2012). *Internet and Surveillance: The challenges of Web 2.0 and social media: Key Features of Social Media Surveillance*.

Van Der Parre, H. (2024, January 12). *Klimaatactivisten op Schiphol niet vervolgd na fouten met identificatie*. NOS. https://nos.nl/artikel/2504589-klimaatactivisten-op-schiphol-niet-vervolgd-na-fouten-met-identificatie

Van Nieuwenhoven, E. (2019). *Ongelofelijk politiek, maar onbegrijpelijk genoeg genegeerd: Een discoursanalyse op het snijvlak van de Nederlandse omgang met politiek, datatechnologie en toekomstliteratuur* (By Faculteit Geesteswetenschappen Universiteit Utrecht; S. Vitse & S. Pieterse, Eds.) [Thesis]. https://studenttheses.uu.nl/bitstream/handle/20.500.12932/32825/Ongelofelijk%20politiek%20maar%20onbegrijpelijk%20genoeg%20genegeerd%20-%20RMAscriptie%20Evelien%20van%20Nieuwenhoven%2c%20juni%202019.def.pdf?sequence=2&isAllowed=y

Von Piekartz, H. (2021, May 18). *Gemeenten kijken op grote schaal en in het geheim mee met burgers op sociale media*. Volkskrant. Retrieved May 19, 2024, from https://www.volkskrant.nl/nieuws-achtergrond/gemeenten-kijken-op-grote-schaal-en-in-het-geheim-mee-met-burgers-op-sociale-media~bb40d4c7/

Zeng, Y., & Wong, S. H. (2022). Social media, fear, and support for state surveillance: The case of China's social credit system. *China Information*, *37*(1), 51–74. https://doi.org/10.1177/0920203x221088141

APPENDIX

Appendix 1 – Analysed documents

Algemene Rekenkamer. (2022, May 17). *Algoritmes getoetst*. Rapport | Algemene Rekenkamer. https://www.rekenkamer.nl/onderwerpen/algoritmes/documenten/rapporten/2022/05/18/algoritmes-getoetst/

Autoriteit Persoonsgegevens. (n.d.-a). *Rapportage AI- & algoritmerisico's Nederland (RAN) - najaar 2023*. https://www.autoriteitpersoonsgegevens.nl/documenten/rapportage-ai-algoritmerisicos-nederland-ran-najaar-2023

Autoriteit Persoonsgegevens. (n.d.-b). *Rapportage Algoritmerisico's Nederland (RAN) - voorjaar 2023*. https://www.autoriteitpersoonsgegevens.nl/documenten/rapportage-algoritmerisicos-nederland-ran-voorjaar-2023

Dekker, S. (2019, November 29). *Waarborgen tegen risico's van data-analyses door de overheid*. Tweede Kamer Der Staten-Generaal. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019Z19084&did=2019D39751

Digitale Overheid. (2023a, June 29). *Beleidsbrief AI, publieke waarden en mensenrechten - Digitale Overheid*. https://www.digitaleoverheid.nl/document/beleidsbrief-ai-publieke-waarden-en-mensenrechten/

Digitale Overheid. (2023b, December 5). *Handreiking Algoritmeregister - digitale overheid*. https://www.digitaleoverheid.nl/document/handreiking-algoritmeregister/

Kamerstukken II. (2019). Richtlijnen voor het toepassen van algoritmes door overheden. In *Bijlage Bij Brief Over Waarborgen Tegen Risico's Van Data-analyses Door De Overheid*. https://zoek.officielebekendmakingen.nl/blg-904102.pdf

Lijst van vragen over waarborgen tegen risico's van data-analyses door de overheid. (2019, November 29). Tweede Kamer Der Staten-Generaal. https://www.tweedekamer.nl/kamerstukken/detail?id=2019D48953&did=2019D48953

Ministerie van Algemene Zaken. (2022, November 7). *Verzamelbrief publieke controle op algoritmen*. Kamerstuk | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/kamerstukken/2022/10/07/verzamelbrief-publieke-controle-op-algoritmen

Ministerie van Algemene Zaken. (2023, January 24). *Kamerbrief over het algoritmeregister*. Kamerstuk | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/kamerstukken/2022/12/21/kamerbrief-over-het-algoritmeregister

Ministerie van Algemene Zaken. (2024a, May 14). *Jaarverantwoording Politie 2023*. Jaarverslag | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/jaarverslagen/2024/05/15/nationale-politie-2023

Ministerie van Algemene Zaken. (2024b, May 14). *VI Justitie en Veiligheid - Rijksjaarverslag 2023*. Jaarverslag | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/jaarverslagen/2024/05/15/justitie-en-veiligheid-2023

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2022a, January 18). *Code goed digitaal Openbaar bestuur*. Rapport | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/rapporten/2021/04/30/code-goed-digitaal-openbaar-bestuur

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2022b, January 18). *Handreiking non-discriminatie by design*. Rapport | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/rapporten/2021/06/10/handreiking-non-discriminatie-by-design

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2022c, January 18). *Kamerbrief voortgang algoritmen en artificiële intelligentie*. Kamerstuk | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/kamerstukken/2021/06/10/kamerbrief-voortgang-algoritmen-en-artificiele-intelligentie

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2022d, December 4). *Beleidsbrief AI publieke waarden en mensenrechten*. Beleidsnota | Kennis Van De Overheid. https://www.kennisvandeoverheid.nl/documenten/beleidsnotas/2019/10/08/beleidsbrief-ai-publieke-waarden-en-mensenrechten

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2024a, January 18). *Overzicht moties en toezeggingen die betrekking hebben op de overheidsbrede visie op generatieve AI*. Publicatie | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/publicaties/2024/01/18/overzicht-moties-en-toezeggingen-die-betrekking-hebben-op-de-overheidsbrede-visie-op-generatieve-ai

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2024b, February 7). *Kamerbrief bij overheidsbrede visie generatieve AI*. Kamerstuk | Rijksoverheid.nl.

https://www.rijksoverheid.nl/documenten/kamerstukken/2024/01/18/kamerbrief-bij-overheidsbrede-visie-generatieve-ai-artificiele-intelligentie

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2024c, February 7). *Overheidsbrede visie Generatieve AI*. Rapport | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/rapporten/2024/01/01/overheidsbrede-visie-generatieve-ai

Ministerie van Defensie. (2022, December 19). *Onderzoek naar social media monitoring bij het ministerie van Defensie*. Rapport | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/rapporten/2022/08/25/onderzoek-naar-social-media-monitoring-bij-het-ministerie-van-defensie

Ministerie van Economische Zaken en Klimaat. (2022a, June 7). *Kamerbrief met Strategisch Actieplan voor Artificiële Intelligentie*. Kamerstuk | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/kamerstukken/2019/10/08/kamerbrief-ai

Ministerie van Economische Zaken en Klimaat. (2022b, June 7). *Kamerbrief met Strategisch Actieplan voor Artificiële Intelligentie*. Kamerstuk | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/kamerstukken/2019/10/08/kamerbrief-ai

Motie van de leden Middendorp en Drost over voorwaarden voor het ontwikkelen van een richtlijn voor het gebruik van algoritmes door overheden. (2020, April 20). Tweede Kamer Der Staten-Generaal. https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2019D26547&did=2019D26547

Motie van de leden Verhoeven en van der Molen over toezicht op het gebruik van algoritmes door de overheid. (2020, April 20). Tweede Kamer Der Staten-Generaal.

https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2019D22116&did=2019D22116

Politie-eenheid Zeeland - West Brabant. (2015). *Online media monitoring: tool en proces (2)*. https://respubca.home.xs4all.nl/pdf/politiebesluitprovidenceobi4wanonlinemediatool.pdf

Rathenau Instituut. (2014). Opwaarderen - Borgen van publieke waarden in de digitale samenleving. In *Bericht Aan Het Parlement*. https://www.rathenau.nl/sites/default/files/2018-02/Bericht%20aan%20het%20Parlement_Opwaarderen.pdf

Rijksorganisatie voor Ontwikkeling, Digitalisering en Innovatie. (2023, June 23). *AI is geen Science Fiction* [Slide show]. https://www.rijksorganisatieodi.nl/binaries/rijksorganisatieodi/documenten/publicaties/2023/06/22/presentatie-odi-ai-20-juni-2023/20230620+-+Presentatie+ODI+V3+-+pdf.pdf

TNO. (2019). Quick scan AI in de publieke dienstverlening. In *TNO*. https://publications.tno.nl/publication/34634897/00bsaM/veenstra-2019-quick.pdf

TNO. (2023, March 7). *Quickscan AI in publieke dienstverlening II*. Rapport | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/rapporten/2021/05/20/quickscan-ai-in-publieke-dienstverlening-ii

Appendix 2 – Used citations

‘Bedrijven en overheden zijn gebaat bij hoogwaardige AI-toepassingen om zowel economische als ethische en veiligheidsredenen’ (Ministerie van Algemene Zaken, 2022, p. 34),

‘Bij het voorkomen van schade is het van belang dat de privacy van mensen wordt gewaarborgd en dat goed wordt omgegaan met persoonsgegevens.’ (Algemene Rekenkamer, 2022, p. 30)

‘De toenemende toepassing van AI-technologieën in de samenleving maakt dat er nieuwe soorten kwetsbaarheden en veiligheidsdreigingen ontstaan’ (Ministerie van Algemene Zaken, 2022, p. 50)

‘Deze tools zorgen voor hogere efficiëntie maar de privacy-inbreuk voor de betrokkenen kan ingrijpender zijn’ (Ministerie van Defensie, 2022, p. 14).

‘Een kader waarin bijvoorbeeld staat dat privacy altijd voorgaat op veiligheid past daar niet goed bij’ (Digitale Overheid, 2022, p. 5).

‘Er is veel aandacht voor privacy, beeldvorming en transparantie, maar tegelijkertijd wordt de impact op publieke waarden en de grondrechten van burgers slechts zijdelings meegenomen in de ontwikkeling van AI’ (TNO, 2023, p. 28)

‘Het gebruik van persoonsgegevens voor AI-systemen bevestigt ook de noodzakelijkheid om de digitale veiligheid op orde te hebben’ (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2022, p. 11)

‘Het kabinet wil dat generatieve AI in dienst staat van het vergroten van het menselijk welzijn en autonomie, duurzaamheid, welvaart, rechtvaardigheid en veiligheid’ (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2024b, p. 4).

‘Risico’s en uitdagingen Het gebruik van generatieve AI kan negatief van invloed zijn op publieke waarden zoals non-discriminatie, privacy en transparantie’ (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2024a, p. 4)

‘Social media monitoring is het bijhouden en analyseren van uitingen in de sociale media. Dit kan voor verschillende doeleinden worden toegepast zoals het snel op vragen en kritiek vanuit de samenleving/consumenten kunnen reageren, het analyseren van trends (bijv. of men positief of negatief spreekt over een organisatie), voor het monitoren van evenementen ten behoeve van de veiligheid en beveiliging of situational awareness’ (Ministerie van Defensie, 2022, p. 14)

‘Wanneer algoritmen of artificiële intelligentie in een verkeerde context, op verkeerde wijze of met het verkeerde doel worden ingezet kan de impact enorm zijn.2 Publieke waarden en fundamentele rechten zoals privacy, non-discriminatie, autonomie en menselijke waardigheid kunnen onder druk komen te staan waardoor burgers in de knel kunnen komen’ (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2022b, p. 1).

‘We hebben de plicht om grondrechten en publieke waarden – in het bijzonder veiligheid, democratie, transparantie, zelfbeschikking, non-discriminatie, participatie, privacy en inclusiviteit – te beschermen en de taak om de kansen van de digitale transitie te verzilveren door een innovatief en gelijk economisch speelveld te creëren: met eerlijke concurrentie, consumentenbescherming en brede maatschappelijke samenwerking (Digitale Overheid, 2022, p. 1)

Veiligheid Voorop’ (Ministerie van Algemene Zaken, 2024, p. 22)

(Rijksorganisatie voor Ontwikkeling, Digitalisering en Innovatie, 2023, p. 19)