SyRI: when the remedy is worse than the disease

A study of the engagement of civil society organisations against the governmental algorithmic risk
assessment program SyRI

Erasmus University Rotterdam

Master Thesis in Sociology - Arbeid Organisatie en Management

Elmo Voeten

482540

Rogier van Reekum

Freek de Haan

9988 words

Abstract

In this thesis study the efforts of civil society organisations combating SyRI are examined. SyRI was a risk profiling system that used large amounts of personal data from Dutch citizens to detect welfare and tax fraud. A lawsuit was set up by the CSO coalition after a successful campaign. The court ruled SyRI unenforceable on the fifth of February 2020. SyRI was violating privacy rights by using personalised data from social institutions to compute lists of possible suspects. The research question is: *"How are civil society organisations engaging with the controversial use of the AI supported risk assessment program SyRI by the Dutch government?"*. By conducting semi structured interviews with the CSO actors, this subject was researched. The findings proved that the campaign of the CSO coalition was successful in the sense that they won the lawsuit, but the discourse of the Dutch government regarding the usage of these systems has not altered. The conclusion of this study offers 5 possible explanations: the visibility of the problem, the slow speed of social and political change, the electoral blockade, the difficulty of advocating against a system that combats fraud and the current political discourse of digitalising all the social services.

Keywords:

Contents

1. Introduction

On the fifth of February 2020 it was declared in court that the accused party; the Dutch government, could not justify how the personal information of citizens was being protected in the system of SyRI (Systeem Risico Indicatie) (Ministerie van Sociale Zaken en Werkgelegenheid, 2020). SyRI was in violation of the European Court of Human Rights (ECHR) and was declared unenforceable. The Dutch government ceased further usage of the system. The case regarding state usage of algorithm programs was unprecedented until then. SyRI was meant for detecting welfare and tax fraud and was used by the municipalities of Rotterdam, Haarlem, Eindhoven and Capelle aan den Ijssel (ANP, 2020). SyRI was a risk profiling system that gathered and analysed large quantities of personal data of citizens, ranging from data on labour, property, education, business criminal records etc. (PILP, 2020). SyRI had access to multiple data banks to calculate risk of fraud (Boeke, 2018). Using data from institutions and other personal data SyRI makes a risk calculation of which groups of citizens are more likely to commit fraud. The system then produces a list of individuals who have a high possibility to commit fraud and delivers it to the applying government agency. This procedure is done via a so-called 'black box' method which creates a pseudonym for each name that is used. It reverts the names of the high probability cases back to the original names once computing is finished, to ensure that suspects and non-suspects are treated the same (Boeke, 2018).

A coalition of civil society organisations (CSOs) founded the *Bij Voorbaat Verdacht*[1] campaign. They claimed that the government was withholding information as to how the algorithms of SyRI worked. State secretary Van Ark assured the Dutch house of representatives that SyRI was not being used to build preventive risk profiles, but the plaintiffs refused to believe this claim (Willen, 2018). The government also stated that the secrecy about the algorithm functionality was necessary to prevent 'gaming' (Polhuis, 2020). This occurs when actors purposely provide false information to an algorithmic system to manipulate the results.

The verdict of the judge stated two different privacy violations by the implementation of SyRI. Firstly, almost all the personal data of citizens are being used by the system. This increases the chance of discrimination and stigmatisation, e.g., people can be singled out based on personal characteristics; ethnicity, job status, living status and their socio-economic status (Kager, 2020). Connecting different types of personal data in such a manner is a direct violation

---

[1] 'Suspected in advance'

of the European Treaty of Human Rights (Kager, 2020). Secondly, labelling someone as having a higher risk of committing fraud could entail several dire consequences. Citizens are processed and judged without their knowledge which makes it difficult for them to prove their innocence.

Aside from the legal implications, the lawsuit concerning SyRI unveils other underlying issues. It shows how the Dutch government validates the usage of copious amounts of personal data of its citizens to aid them in finding people who commit fraud. The current Dutch government is led by the party leader of the VVD, Mark Rutte. The VVD has been the biggest party in the last decade. Moreover, Dutch prime minister Rutte favours a strict law and order method of governing. Even stating that he would rather not investigate the possible causes of criminal offences, since he is not a sociologist (NOS, 2021). These statements offer some insight into the current discourse of the government. Implying that solving the problem is better than preventing it from happening. In the case of algorithmic risk assessment systems however, due to the complex nature of algorithms, problems are only arising after a substantial amount of time (Deloitte, 2020). Thus, in implementing these systems it is important to heed the possible long term negative outcomes. Rather than making on the spot decisions to patch up the problems the implemented systems are causing.

A good example of this mindset of the government towards AI supported risk programs is the proposal and condoning of a newly founded risk program, only a year after the judge declared that SyRI should be revoked (Te Lintel Hekkert, 2021). The Wet Gegevensverwerking Samenwerkingsverbanden (WGS) was proposed as an alternative to SyRI. The coalition of CSOs dubbed this program 'Super SyRI', as it would be able to receive and combine data from even more social institution databases than SyRI had access to. This new program was approved by the house of representatives on December 17th, 2020, the same day that Dutch news outlets Trouw and RTL nieuws first published their articles on the *toeslagen schandaal*, another public scandal in which the tax agencies discriminated against households with two nationalities by using AI supported risk programs (Trouw, 2020). Luckily the Dutch senate did not follow in the footsteps of the house of representatives and rejected the implementation of Super SyRI (de Vries, 2021). The rejection was based on a statement by the *Autoriteit Persoonsgegevens,* a Dutch governing body which protects the constitutional right of protection of personal data (Autoriteit Persoonsgegevens, 2022). The proposition of Super SyRI shows that the government is not taking heed of the possible negative effects that AI supported risk programs could have on society since the newly proposed legislation made it possible to link even more data from private to public organisations. This discourse is further

explained in the quote below. Explaining how this sentiment of collecting data started and why the current coalition government will not change its course:

"The ministerial committee of fraud was appointed by the minister of justice and security Opstelten, this was in the summer of 2013 during the aftermath of the Bulgarian fraud incident. Under supervision of minister president Rutte they agreed to collect and connect all kinds of data. Believing that this would close the net on fraudsters and would make it impossible for anyone to take advantage of the government. This is where SyRI was born, this is where WGS was born and this is also where the notion of risk profiling was born.
(...) The coalition is always busy with making agreements. 'You do this and I do that'. They are permanently discussing with one another how to best govern the country. It has never occurred that the politicians within the coalition vote freely on a subject. And specifically on this subject they will not let go, because they are constantly making deals with each other. If they want to discuss another topic, they must agree on some, and this is the one that they agree on. Therefore, pressure from the outside is so important."
[2]

This shows that the discourse of the current coalition government regarding data collection and using risk assessment programs is part of a larger sentiment that exists for almost a decade. This will not change because the coalition needs to be united on this topic to be divided on another. Different parliamentarians have different goals that they want to achieve, by voting in favour of these programs they gain more leverage in subjects where they do want to make a change. Therefore, this study focuses on the efforts of CSOs since the current parliament will not change its course. CSOs provide pressure from outside the current political environment. With this thesis research project, the effectiveness of CSOs regarding combating SyRI and the future usage of invasive algorithmic risk assessment programs is being studied. The research question for this thesis has been formulated as: *"How are civil society organisations engaging with the controversial use of the AI supported risk assessment program SyRI by the Dutch government?"*. The SyRI trial will be used as a case in this research as an example of how the Dutch government looks at the employment of algorithmic risk assessment programs in society. The actors of the different CSOs that form the coalition of prosecutors

---

[2] Interview 7: see Appendix C: Interviews

during the SyRI lawsuit will be interviewed to research how they engage with this public issue. Through conceiving the underlying issues of SyRI and studying the response of the Dutch government it can be better understood what the issues of risk assessment programs exactly are and what CSOs can do best to combat these issues. In the following theoretical framework, existing academic literature is used to get a better understanding as to how algorithmic programs work, how the usage of risk assessment programs by the government may facilitate public issues and finally what CSOs can do to combat this public issue. The results of this study will contribute to the existing academic literature of algorithmic systems usage by the government (Zuiderwijk, Chen & Salem, 2021; Wirtz et al., 2019; Sousa et al., 2019), as well as existing literature on CSOs and how they engage in these issues (Zajko, 2022; Robinson, 2020; Rainey, Wakunuma & Stahl, 2017)

2. Literature Review

2.1 AI risk assessment programs

To fully understand what is at stake in the issue caused by AI usage by the government, the inner workings of artificial intelligence reliant risk assessment programs are researched. AI is gaining popularity with governments that use them to predict certain behaviours in the population (Van Eijk, 2020). What AI is exactly, is difficult to determine. AI is a fluid concept which is being applied for different functions. Furthermore, the technology is changing at such a high speed, that newfound scientific definitions tend to not age very well (Bellanova et al., 2021). To have a usable concept for AI to work with, we can use the definition of an EU research, which states that AI "refers to systems that display intelligent behaviour by analysing their environment and taking actions -with some degree of autonomy- to achieve specific goals" (High-Level Expert Group on Artificial Intelligence, 2019). An AI system is also rational; by collecting and analysing large groups of data, an AI system selects the best course of action, and then acts accordingly (High-Level Expert Group on Artificial Intelligence, 2019). AI systems can analyse large amounts of data in an instant. Entire populations can be simplified based on their characteristics, they become statistics which can be analysed. Hence AI programs are being used as the main mediator of power in our society (Van Eijk, 2020). These programs are not being used to make decisions; they are used to inform people who make the decisions.

A risk in using these programs is that people could assume the information generated by AI programs to be completely true. To function, these systems need data. This data could be poorly selected, outdated, incorrect or could contain biases (Niklas & Gangadharan, 2018). When a poor decision is made using this information, it is difficult to hold someone accountable or responsible, since people can shift the blame to these AI, black box systems (Zuiderwijk et al., 2021). These black box systems are unpredictable and may cause harm (Wirtz, Wyerer & Sturm, 2020). Another problem that occurs in using risk programs is the fact that algorithmic predictions are not based on the actions of an individual. An individual being flagged as having a high risk of fraudulent behaviour is based on certain demographic or socioeconomic factors (Starr, 2014; Van Eijk, 2020). To rephrase, the risk does not originate from the actions of the individuals, but it is attributed to the group that they find themselves in. The third issue that arises in the usage of these predictive programs is that the predictions are based on group characteristics. Social marginality, race/ethnicity, gender and age are being used to determine

which individual has a higher statistical chance to commit fraud (Van Eijk, 2017). Socioeconomic characteristics are also being used in the predictive model, allowing the model to base a probability on class attributes such as education or employment. The fourth and final issue regards the futuristic aspect of the predictive models. The model predicts which individuals have more risk at committing fraud. Therefore, individuals are being flagged before they can even act out said act. Schinkel has dubbed this as 'prepression': "*a proactive repression that prematurely squashes certain acts of life and to steer these behaviours in the desired direction*" (Schinkel, 2009). These four problems emerge throughout the found literature. The known issues will be compared with the statements by the different actors within the CSOs.

2.2 Existing problems of AI usage by the government

While the problems of AI usage are exhaustively written about in the existing literature (Sztandar-Sztanderska, et al., 2021; Brady, 2019; Malik et al., 2021), little literature was found on the impact of algorithmic systems on public administration. The literature that was available weighs in on either the legal implication of AI (Scherer, 2015), the implementation of AI practices in government services (Leslie, 2019; Zheng et al., 2018) and literature reviews that focus on mapping out different advantages and challenges when it comes to working with AI as a government (Wirtz et al., 2020; Zuiderwijk et al., 2021; de Sousa et al., 2019). Still, little research is conducted on the possible consequences of the usage of AI by the public sector. The different types of literature review studies do give an insight into the assumed consequences, whether good or bad of AI being used by the government. Zuiderwijk et al. (2021), identified eight different categories of challenges that AI poses to the public sector. These challenges are data challenges, organisational and managerial challenges, skills challenges, interpretation challenges, ethical and legitimacy challenges, political, legal and policy challenges, social and societal challenges and economic challenges. In the light of this study, *the ethical and legitimacy challenges* and the *political, legal and policy challenges* are relevant, for these are the criticisms of the SyRI case. The ethical and legitimacy challenges stated by Zuiderwijk et al. (2021) originate from the unethical use of data, the unethical use of shared data and AI discrimination. Most of these issues relate to removing the human component in decision making. The political, legal and policy challenges relate to the AI usage in a way that undermines the fundamental values of due process, equal protection and transparency (Zuiderwijk et al, 2021). It is difficult to hold people accountable when dealing with 'black box' AI (Bullock, 2019 & Liu et al., 2019).

Aside from the review of Zuiderwijk et al. (2021), Wirtz et al. (2019) identified 17 studies that addressed possible challenges of AI usage within the public sector. They divided the challenges within four major dimensions. These are technology implementation, AI law and regulation, AI ethics and AI society. Once more, the issue regarding responsibility and accountability is mentioned, as well as issues regarding privacy and safety, since these systems need a lot of personal information to work properly (Wirtz et al., 2019). Sousa et al. (2019) stresses the importance of implementing effective legislations and guidelines to prevent mistakes, prejudices and misinterpretations. Also stating that the public sector is increasingly facing issues regarding biases and discrimination in the use of AI. These literature reviews show that a lot of negative consequences of AI usage by the government are already known from the academic perspective. In the interviews of this particular, respondents will be asked about what they believe are the negative consequences of the usage of SyRI. It will be interesting to see whether the respondents provide additional examples of consequences than what is already provided by the literature.

2.3 Engagement with public issues

With the establishment of the negative consequences of AI usage by the government, the question remains as to how certain civil society and non-profit organisations are engaging in this controversy. Furthermore, it is important to examine the types of obstacles CSOs face in their effort to change the behaviour of the Dutch government. Identifying these obstacles and discovering solutions to these issues may increase the effectiveness of the efforts of CSOs to evoke change. The focus point of these organisations is to improve the accountability, fairness, privacy, transparency and responsibility issues that continue to persist within the AI usage by the government (Zajko, 2022; Robinson, 2020; Gibbons, 2021). CSOs want to ensure that marginalised groups are properly represented, as they have a history of having little to no representation in debates concerning agency (Zajko, 2022). The CSOs also want to help marginalised groups to hold people accountable for the negative effects of AI usage. This is often difficult, as there is a large discrepancy in knowledge as well as power between the developers and the users (Robinson, 2020). The solution for this controversy lies in the empowerment of the people who are at the receiving end of AI usage by the state. Their power is participation. Through a collective voice, with the aid of CSOs, moral and social values are implemented into society (Etzioni & Etzioni, 2017). Through this collective channel these norms and values, like transparency, ethics and privacy are translated into legislative action.

Having good values and principles is not sufficient, but they can meddle into the work of legislators, shaping the development of policy and legal norms (Fukuda-parr & Gibbons, 2021).

Advocating for human rights is thus a good strategy to change legislation regarding AI usage by the government. It has led to numerous human right groups to present guidelines which state principles regarding responsible AI design, development and deployment (Fukuda-parr & Gibbons, 2021). These guidelines help shape the narrative surrounding responsible AI design, and in consequently shape legislation. There are already a lot of laws to protect citizens from privacy and data breaches. The General Data Protection Regulation for example, which makes the usage of personal information without explicit consent more difficult.

Zajko (2022) states that there are three general ways of acting against unethical AI usage and enable the citizens to have more autonomy over AI. First, critiquing of current political decisions and the politics of refusal. With this approach, CSOs can raise awareness as to which legislation poses a threat to individual privacy and autonomy. AI engineers often have no clue as to what the social effects of their work are. These issues can be addressed through the work of CSOs who can point out certain flaws. The second suggestion is fighting inequality through technology. Instead of combatting the algorithms that produce and sustain inequality, one can start writing code themselves. This is already being done to a certain extent, with the latest coding research addressing in which ways biases can be prevented (Zajko, 2022). The final approach by Zajko (2022) is participating in the technological governance itself. To be able to be part of the institutions that are causing the public issue, is also enabling oneself to bring about real change. At this moment there is a large knowledge deficit in the field of AI in the public sector, since the private sector pays higher salaries and has better working conditions for AI experts as compared to the public sector (Wirtz, Weyerer & Sturm, 2020). A solution for this issue would be for the government to cooperate with private and CSOs to make use of their knowledge. During the interviews, the representatives of the CSOs have been asked what they think is the best approach for them to facilitate change regarding this social issue. Their statements will be compared against the literature.

2.3.1 Known obstacles of Civil Society Organisations

In studying the effectiveness of the CSOs in combating improper AI usage by the government, the known obstacles of this engagement must be taken into consideration. By conducting this study, a proper assessment can be made whether the 'Bij Voorbaat Verdacht' coalition overcame these known hindrances. In current academic literature, there are several known obstacles which prevent CSOs to evoke change. The foremost possible hindrances are a lack

of funding, a lack of social trust and an overly authoritarian or a lenient state. Finances are at the heart of every organisation; this includes CSOs as well. A key aspect in achieving CSO goals is the funding they can receive (Rainey, Wakunuma & Stahl, 2017). The ability to set up campaigns that have a good possibility of reaching a large audience is directly related to the number of financial means that are available. This constraint is known throughout academic literature and is a prevailing problem in CSO actions (Hess, 2009). Secondly, CSOs are, due to the lack of funding, primarily dependent on voluntary workers. If a society has a low rate of political and social participation, chances are that the CSO memberships are dwindling as well (Sampson, McAdam, Macindoe & Weffer-Elizondo, 2005). Moreover, social trust is also a factor in CSO participation (Newton, 2001). CSOs are neither work, nor family, nor friends: they are something that has to be done as an extra to all of this. Members of CSOs must have full confidence in each other for a CSO to thrive. Lastly, the effectiveness of a CSO is also highly dependent on the current state of the government. The state can neither be too lenient nor too authoritarian, or a CSO will not be effective (Paffenholz & Spurk, 2006). The environment surrounding a CSO needs to be stable, with clear power relations and networks. If a state is too lenient, the lack of networks will not amount to social change. If a state is too authoritarian, this will lead to the state seeing CSOs as competition and will actively try to hinder them.

3. Methodology

In this research, actors of CSOs were interviewed about the consequences of algorithmic risk programs usage by the government and how they are engaging in this public issue. Along with CSO actors, three politicians were also interviewed. The research strategy was to interview respondents that are involved in the SyRI trial. One of the reasons why CSOs were chosen for this research method is that the subject of this study is the defects of a governmental system. Interviewing government officials about these defects might prove to be difficult, whereas actors from the CSO were more willing to talk about this subject. These are more open to interviews because exposure is good for their cause. Hence for this research, CSOs were approached for conducting interviews. Examples of these CSOs are *Platform Bescherming Burgerrechten, FNV, Privacy First and Stichting KDVP* (FNV, 2020). Though, interviewing actors of CSOs on this topic could be susceptible for bias since they are clearly opposing of SyRI. That is also why three politicians were interviewed to get a broader perspective.

The focus was to interview the plaintiffs, those who have worked on taking the case to trial. The actors that are with the CSOs are invested in this issue and could best explain in their own words why the further usage of algorithmic risk assessment programs is problematic on a societal level. This is also why the research method of conducting interviews was chosen. The SyRI program and its defects are complicated to comprehend. Utilising interviews allowed the actors to explain this difficult subject more clearly (Babbie, 2020). Aside from asking the respondents to explain the public issue and the defects of the program an inquiry about the CSO process of combating this issue will be made. To find out the effectiveness of the CSO coalition in their attempts to combat SyRI, the respondents will be asked about the development of the coalition and the campaign. By doing this, possible recommendations can be set up to raise the effectiveness of CSO efforts in the future.

For the interviews a semi-structured approach was utilised. In a semi-structured interview, the topic list and questions are prepared in advance. During the interview however, the interviewer has the possibility to go off script and delve deeper into something that has come up during the interview that is relevant for the research but was not in the questions. This method allows for a more natural kind of interviewing, where the researcher gently steers the conversation in the right direction to get the answers that they are looking for (Babbie, 2020). The semi-structured interviews will contribute to answering the research question and allow for flexibility in conducting the interviews if the respondents say something that was not

expected but is worth exploring. In total seven interviews were conducted, with each of them lasting around an hour. In addition to respondents of the CSOs, respondents that are active within politics were also interviewed. These respondents gave insights into the political impact that the CSOs were able to make, along with how the current Dutch government responded to the coalition efforts.

The data that was retrieved through the interviews was analysed by first being transcribed. Subsequently the transcriptions were coded using Atlas.Ti. The coding of the interviews was done through open, axial and selective coding. With open coding the transcriptions are analysed to find the overarching themes within the different interviews. With axial coding the analysis goes a step further and key concepts are sought after within the larger themes. Lastly, with selective coding the codes are analysed once again to find codes and statements that can be used to answer the research question. Based on the types of codes different quotes are selected for the findings to illustrate the sentiment of the CSO actors.

It was assumed that the CSOs which are involved in the SyRI case are well versed in algorithmic systems and their implications. This was the case with some respondents but not all. Some of the respondents work in CSOs which specialise in protecting data privacy laws when they are threatened by very intricate systems. Other respondents only helped in gaining media and political attention for the coalition to spread awareness. Both types of actors were of course necessary to achieve the goals of the coalition. Their insights will not only contribute to finding out what risks the usage of risk assessment by the government does entail, but also as to how these CSOs are tackling this issue. By interviewing the respondents and combining their responses with published academic literature, the research question was able to be answered. In conducting these interviews certain ethical principles were implemented to provide a safe working environment for the respondents as well as the researcher. Prior to conducting the interview, the respondents each received a consent form. In this form the purpose of this research as well as the purpose of the interview are explained. The respondents were made aware that they, always can: access their data, rectify, erase or restrict the processing of their personal data and withdraw consent at any time and lodge a complaint with a supervisor authority. The respondents were also informed how long their data was used for analysing. Once the respondents read the consent form and agreed to these terms did they partake in the research.

4. Findings

4.1 Effectiveness of the SyRI campaign

For this research, the frontrunners of the CSO coalition were interviewed. These organisations were the FNV, Platform bescherming burgerrechten and Privacy first. They are part of a coalition that strives to stop the SyRI legislation and to spread public awareness about the negative effects of risk assessment programs. During the interviews it became self-evident that the different organisations have very good relations with one another.

> *"The SyRI coalition is a good example of collaboration between civil society organisations, good communication between them and having a shared purpose. And to try and reach goals with that good collaboration. I think that other organisations can learn something from this."[3]*

The excellent cooperation between organisations was demonstrated during the process of approaching respondents for the interviews. CSOs would often redirect to the one person that is seen as the official spokesperson of the coalition and the movement. One respondent credited this to the lack of financial funds within the coalition.

> *"What often is effective is when intrinsically motivated people without financial means want to achieve something. These people are more driven and more successful than the people who get paid."[4]*

Through collaboration and a shared goal in mind the coalition of 'Bij Voorbaat Verdacht' went to work. The first step was to find other organisations and individuals willing to help them build a case against the government. Notable actors joining the case as public watch dogs were filosopher Maxim Februari and author Tommy Wieringa, while law attorney office Public Interest Litigation Project (PILP) joined to provide legal assistance. The next objective was to gain publicity for the cause. As one respondent puts it: *"Court cases are impossible if nobody cares, because if you win, what did you win exactly?"[5]*. The coalition attempted to achieve this

---

[3] Interview 4: See Appendix C: Interviews
[4] Interview 4: See Appendix C: Interviews
[5] Interview 3: See Appendix C: Interviews

by going to the different neighbourhoods in which the SyRI system was active. One of these being Hillesluis in Rotterdam. Hillesluis is a low-income neighbourhood with a population consisting of 71% non-western immigrants (Wijkprofiel Rotterdam, 2022). In this neighbourhood, the FNV rallied the inhabitants by making insinuating statements. They would ask people if they lived here, and if so, they would follow up with: "*Well then you are a suspect, your name is most likely already on a governmental list stating that you are a fraudster*"[6]. The citizens would respond with claiming that this was against the law. To which the FNV could reply that there was already a law in place that authorised these practices. This caused the citizens to be confused, frustrated and angry. The FNV used this tactic deliberately to mobilise people into political action. *"You must get under the skin of these people to make them angry. And if they get angry, they will act, according to theory."*[7]

This practice proved to be successful. The FNV organised a public gathering where they would educate people on the negative effects of SyRI. The FNV also invited several media outlets such as AD, Trouw and the Volkskrant. Even international media outlets showed interest in this public issue. As one journalist from the New York times explained to an FNV employee:

> *"Apparently, they were shocked in the V.S. that this was allowed in the Netherlands. That there was such a law that condoned this, they were appalled. They told me that there was no way that this could ever happen in the states."*[8]

The media attention resulted in a response from local politicians. SyRI was retracted in several parts of the municipality in response to the public upheaval. To make use of the attention that was created, the coalition organised a demonstration in front of the city hall in Rotterdam. They also presented a petition to the local municipality, demanding answers as to why this specific neighbourhood was targeted and what would happen with the acquired personal data. The mayor of Rotterdam, Achmed Aboutaleb, was taken by surprise by this scene. For he was not aware at the time that police information was also being processed by SyRI, for which he did not give permission. After uncovering this fact, Aboutaleb pulled the plug on the program.

---

[6] Interview 1: See Appendix C: Interviews
[7] Interview 1: See Appendix C: Interviews
[8] Interview 1: See Appendix C: Interviews

4.2 Pushing the right rhetoric

It is important for CSOs to choose the right angle in framing a public issue. Framing the problem can result in mobilising large amounts of people. During the campaign of the SyRI coalition they set out to convey to the public what was wrong with SyRI. In the interviews, each respondent was asked what they thought the core problem was:

> *"We are witnessing that the trustful relation between citizens and the state has been severed. All the data that you give to the government or what the government documents of you can be brought together in a SyRI blackbox. This system can use all the data that is being collected by numerous public institutions against you. You can not see, evaluate or check this data yourself. You can not even see if the data that they have of you is correct."[9]*

> *"The right of privacy states that the government can only violate your privacy rights if the cause is demonstrably necessary. With SyRI, the presumption is made that everyone is eligible of being profiled, to be vetted as a potential fraudster or criminal."[10]*

The core problem that is articulated here has nothing to do with welfare fraud. It regards our relationship as citizens with the government. It is a matter of a system which is connecting personalised data from multiple public institutions and using this data to make calculations about citizens, who have no idea that they are even the subject of investigation in the first place. And if they did, there would be nothing that they could say or do to stop this process.

> *"Conclusions are drawn behind the scenes over which you hold no power. The data does not even have to be correct to be able to end up in a rapport like they are real. You are powerless against this as a parent, as a citizen. So, we must show people that this has bad consequences and we have to keep calling out the structural flaws of this system. I think that we should frame it like that, a societal problem."[11]*

---

[9] Interview 2: See Appendix C: Interviews
[10] Interview 2: See Appendix C: Interviews
[11] Interview 2: See Appendix C: Interviews

4.3 Going political

After this local victory, the coalition set their sights on taking the social issue to a national level, into the house of representatives. To achieve political success, even more public uproar was needed. They organised even more actions, sent letters to the house of representatives, organised public appearances by Tommy Wieringa and Maxim Februari, and set up a website with an animation video to explain in informal terms as to why SyRI is a problematic system. To get more media coverage, the FNV organised a 'fraud fishing' event. They made a makeshift pond, filled with fake fish with pictures of proven fraudulent former politicians. During the event, members of parliament could use a fishing rod to catch all the fraudulent fish, while the vice president of the FNV appealed to the members of parliament to start catching the big fish instead of focusing on benefit fraud by using algorithmic mass surveillance programs. The goal of the FNV was to attract as much media attention as possible, to raise political awareness regarding the SyRI case.

> *"You know for certain that when a lot of commotion arises regarding a certain topic, members of the house of representatives have the need to do or say something in regard to this topic. And everybody also wants to be the first party to do something that contributes to the solution of this problem. Then they start calling each other about what they should vote for, and we will additionally apply pressure on the different departments and their subsequent members."* [12]

One method of generating political traction is to convince politicians about the necessity of the problem. To get people to talk about a certain topic may lead to a political outcome. Like the respondent stated above, politicians want to be the frontrunner in subjects that matter to the public. Once a subject has attained enough media coverage and social attention, politicians are quick to give their opinion on the matter.

---

[12] Interview 1: See Appendix C: Interviews

4.4 Taking it to court

According to one respondent, the best tool for CSOs to solicit real change is to take the state or big companies to court:

> *"Historically, there are only three ways one can influence governments. Money, lawsuits and violence. The latter you don't want to use of course. So, the only measure we can implement is lawsuits. The perk of lawsuits is that as a citizen, you are formally equal to the government. In court you both are equal parties to the proceedings. In reality that may be different because the government has so many people and so many means in contrast to a vulnerable citizen, but legally, you are equal."[13]*

To achieve public exposure, going to court is effective for CSOs. This also turned out to be the case with SyRI. The attorneys providing legal assistance figured out a way to, as they described it, "*apply the norms that are captured within international law on a phenomenon such as risk profiling*"[14]. Once the legal support team amped up enough legal arguments to win the case, they took the Dutch government to court. This fared better than the coalition had anticipated. Not only did the judge rule in favour of the coalition party, but the court declared SyRI to be unenforcable. This meant that SyRI could no longer be used by the Dutch government.

> "*This was very unique and almost never happens. We expected the court to implore that the system should be tweaked in order to adhere to the privacy laws. This would have also been a victory for us. But the judge said that since she was not able to check the inner workings of the system the system didn't fulfil the basic need of the right to privacy."[15]*

Apart from the direct advantages, filing a lawsuit also generates positive side effects. As one respondent puts it: "*If you file a lawsuit, you generate a lot of critical attention and awareness in the media, public domain and politics. Politicians often start using your arguments. Sometimes you achieve your goal within the political sphere a lot faster than being in court at all. This also happened with the SyRI case."[16]* This respondent also refers to the reactions of

---

[13] Interview 4: See Appendix C: Interviews
[14] Interview 4: See Appendix C: Interviews
[15] Interview 2: See Appendix C: Interviews
[16] Interview 4: See Appendix C: Interviews

local politics during the proceedings of the trial. Because of the commotion following the lawsuit, the municipalities still using SyRI discarded the system since the topic became too controversial.

4.5 Effectiveness of the SyRI coalition

The campaign of the coalition was highly effective. It was an unprecedented case that got international media attention because of its novelty. The coalition was not only successful in informing citizens about the social risks associated with SyRI, but the politicians and the judge as well. This led to SyRI discarded by municipalities and a verdict by the judge stating that if a system is not transparent enough in its guarantee to protect international data privacy laws, the system should not be used. Despite all these successes, the Dutch parliament voted in favour of a new law, called Wet Gegevensverwerking Samenwerkingsverbanden (WGS) on December 17, 2020. The coalition dubbed this legislation Super SyRI because this new law combined even more data from different public organisations than SyRI. The coalition was taken by surprise for they did not suspect that the parliament would vote in favour so quickly after the verdict of the judge on SyRI. In the period leading up to the WGS being passed through the house of representatives, the coalition was constantly sending letters to politicians to inform them *"what the problems are regarding this legislation and what the consequences will be if this passes"*[17]. During the interviews the respondents were asked about their reaction on this development and what this meant for the effectiveness of the campaign.

"That is a big difference between the way SyRI was treated versus Super SyRI, the WGS, now. With SyRI we could not get any political foothold in the house of representatives or the Senate. With the WGS I saw an intense debate. Even the ruling parties' leaders were involved. D66 was very strong in this debate. But it was not enough because the majority is still convinced we are catching bad guys with this system and are convinced the merit outweighs the negative effects. So there has been a political change but it was not sufficient to have the majority vote against this legislation."[18]

---

[17] Interview 3: See Appendix C: Interviews
[18] Interview 2: See Appendix C: Interviews

"We were convinced that the government would not make the same mistake twice but apparently they will. The self learning capabilities of the government are not very good on this topic"[19]

The campaign was successful in the sense that they did stop the Dutch government from further using SyRI. The campaign was not successful in changing the current course of the Dutch coalition government in collecting and connecting as much data as possible. A reason for this might be the following:

"Mobilising is something that this coalition isn't doing. They are trying it though but privacy organisations are not built this way. They have a lot of individual and intellectual knowledge, which is also important. But it would be good if this would become a more social movement. "[20]

"Sometimes we get called activists but I view ourselves as being something different. We are not politically motivated. We concern ourselves with the minimal prerequisites of the continuation of a constitutional democracy"[21]

Even though the campaign was very effective, the outcome was not impactful since a new risk assessment system was passed in the house of representatives less than one year after SyRI was revoked. Talking to the respondents, multiple explanations came up. Firstly, the problem is not visible enough for the public. People see no impact of the system on their daily lives and can thus live without thinking about the consequences. Secondly, change is a slow process and does not happen overnight. This is recurrent in all efforts of CSOs to evoke societal and political change and this case is no different. Thirdly, political parties do not lose votes if they do not address this problem. Fourth, fraud is viewed as a bad thing, so a program addressing fraud is generally seen as a good thing. Finally, risk assessment programs are part of a new global mindset that views digitalisation as the solution to problems that exist within our society, digitalisation also grants the government more power in respect to citizens. These explanations are further elaborated in the following segments.

---

[19] Interview 1: See Appendix C: Interviews
[20] Interview 7: See Appendix C: Interviews
[21] Interview 3: See Appendix C: Interviews

4.5.1 Visibility of the problem

The issue of risk assessment programs is the fact that citizens are not aware that they are being investigated or are suspected of committing fraud. This makes it difficult for CSOs to convince citizens of the imminent dangers of these programs. During the interviews the respondents often talked about shadow administrations, hinting at an administrative network that is invisible to the eyes of the citizens:

> *"SyRI produces a list with high risk citizens, they get marked without making them aware that this is happening. Behind the scenes a shadow administration is being created which can have dire consequences for citizens who are still unaware of how it functions or that they are even a subject of investigation."[22]*

These digital systems pose real life threats for society. However, getting social traction is difficult as many people are unaware of the existence of these programs. "*Because you do not know, because you do not see it it will not get addressed. And that is indeed the problem*"[23].

4.5.2 The long haul

Another reason for the progress being inadequate is that change, by nature, is a very slow process. Change does not happen overnight, especially when a great deal of money has already been invested in these programs. Not only does it take time to make people aware of the problem, but to mobilise them into taking affirmative action takes even more time. One respondent made the comparison with other time intensive issues.

> *"Likewise how we.. with the climate change issue.. of gender equality, it did not dawn upon us overnight to view these issues differently. So I think we will be busy for a while. I think that it is something that people have to see time and time again that practically, this does not work, this is not desirable and you should set boundaries."[24]*

Though it takes a long time to evoke real change, the CSOs remain optimistic and vigorous in their efforts to combat this issue. *"The government is not easily taken off track. They will*

---

[22] Interview 2: See Appendix C: Interviews
[23] Interview 3: See Appendix C: Interviews
[24] Interview 2: See Appendix C: Interviews

continue, and yes, we will also continue. "[25] This optimism is also very characteristic for CSOs, as they must deal with slow progress all the time.

> *"If you are an activist and you want to maintain your energy you should realise that you will never achieve your idealistic view of the world. Focus on the small successes instead of the things you want to achieve. Because if not you can get very cynical and depressed. You will have no energy and you will get nothing done."*[26]

4.5.3 Electoral Blockade

Current politics prevent effectively solving this issue since the issue is very intricate and difficult to explain. In the house of representatives there are few politicians who have active knowledge on this topic. This is the reason why these legislations still pass the house of representatives. The politicians are actively trying to get re-elected. Voters are not aware of the SyRI case so it would not make an electoral impact for the politicians to focus on this issue.

> *"A lot of people find this material tough. Few people are invested in this topic, thus this means minimal electoral gains. The politicians get more value out of focusing on other topics."*[27]

Politicians may also vote in favour of a legislation they do not necessarily agree with, to get re-elected. This might also be a problem with SyRI since the program combats fraud and being hard on criminals gets you more votes.

4.5.4 Fraud is the problem

In combating a social issue, CSOs want to convince the politicians as well as the citizens that SyRI is a problematic program which has flaws that need to be addressed. This has proven to be difficult since SyRI has been developed to combat fraud. Since SyRI is a complicated issue, not many politicians invest the time to properly understand the problem. If taken at face value, a system that combats fraud is an inherently good system, and thus politicians vote in favour of this legislation.

---

[25] Interview 3: See Appendix C: Interviews
[26] Interview 5: See Appendix C: Interviews
[27] Interview 5: See Appendix C: Interviews

"And what is often the case with privacy related issues is that the advantages are often quick and apparent. As for the disadvantages, while they are impactful, it remains uncertain whether they take place at all. And if they take place it is in the distant future. In human psychology, one always prioritises direct risks, even if these are smaller."[28]

Additionally, cracking down hard on fraud or any criminal activity is seen as a popularity boost among politicians, one that is often used by the leading parties of the cabinet. This is a win-win scenario for the politicians. You do not have to read into the problem and you get votes by doubling down on your ideology that the best response to fraud is to stop at nothing in order to find these offenders. *"Crack down hard sounds very tough, while it simply does not work in most cases. But one must delve into this subject in order to understand that this does not work."[29]*

4.5.5 Digitalisation and Power

Finally, the problem preventing change is the trend of governments to digitalise as much as possible. Digitalisation of public services has brought many benefits to the government. It is the belief in this merit that leads to the creation and the continuation of risk assessment systems like SyRI. Technology is seen as a solution, and not a part of the problem. The CSOs must continually prove that these systems are not the solution. This takes a lot of effort considering that the government already discards privacy laws to make these systems work.

"It is a totally new phenomenon of which we only received the benefits. Now we are approaching a point where the government starts automating all kinds of things which should not be automated."[30]

The clinging to technology as a solution also preserves a lot of governmental power. By continuously connecting personalised data the government can find incriminating evidence against anyone. Furthermore, other social institutions have access to personalised data which they do not need. *"It is attractive for the government to collect large amounts of data and to*

---

[28] Interview 5: See Appendix C: Interviews
[29] Interview 5: See Appendix C: Interviews
[30] Interview 2: See Appendix C: Interviews

connect them. They can do all types of things with this and it works well to keep things under control"[31]

"It always goes on, in the same bad direction, this has been the development of the last decade. In general, the freedoms of citizens get smaller and smaller. And the power of the government and big companies to limit those freedoms and to make people more transparent and vulnerable remain the same"[32]

---

[31] Interview 5: See Appendix C: Interviews
[32] Interview 4: See Appendix C: Interviews

5. Conclusion and Discussion

In this research the effectiveness of CSOs and their efforts to combat the SyRI program was studied. The current study aimed to answer the question: *"How are civil society organisations engaging with the controversial use of the algorithmic supported risk assessment program SyRI by the Dutch government?"*. Looking at the findings of the study it can be concluded that the coalition of CSOs succeeded in their goals to take the Dutch government to court to prevent further use of SyRI. Comparing the literature to the actions of the coalition, they took the right measurements in achieving their objectives. The coalition correctly explained what the dangers of using risk assessment programs are. The algorithmic predictions were based on where a person lived, making the algorithmic programs work with the characteristics of a person and not the actions (Van Eijk, 2017). The coalition also laid an emphasis on the fact that citizens could not defend themselves from being processed by this system, as they did not know they were even processed in the first place. The data that was being collected did not have to be legit to be framed like it was real. Everybody was eligible for being profiled, as a form of 'prepression' (Schinkel, 2019). Furthermore, the coalition was effective in stating the problems of AI usage by the government. They thoroughly described the problems that would arise when copious amounts of data are shared and when the human component of these processes is removed (Zuiderwijk et al., 2021). Since the coalition filed a lawsuit against the government, they made sure to emphasise the central human values that are being under stress with the usage of SyRI (Zuiderwijk et al., 2021).

Furthermore, the CSOs sought out to represent the marginalised people who were at the receiving end of SyRI (Zajko, 2022). They successfully worked on reducing the knowledge and power discrepancy between citizens and government (Robinson, 2020). By actively spreading information to the public. Hereby hinting on the disruptive balance between the government and the citizens. Moreover, the best way to change certain legislatures is to advocate for human rights (Fukuda-parr & Gibbons, 2021). The coalition achieved this by claiming that SyRI violated international data privacy laws (Zajko, 2022). During the lawsuit the coalition also explained the inability of the citizens to request transparency from the system that was investigating them and made it clear that SyRI posed a threat to individual privacy and autonomy.

The coalition also struggled with known obstacles that CSOs face. Lack of financial means was also an issue during the campaign of the coalition (Rainey, Wakunuma & Stahl,

2017). However one respondent stated that having little financial means also had an advantage, as it led to people working in the coalition to be intrinsically motivated, causing them to have more drive and efficiency. The same respondent also credited the coalition members for being highly cooperative, implying a great deal of shared trust (Sampson et al., 2005). Finally, there were no notions of the state actively hindering the engagement of the coalition, implying that the Dutch state is not of authoritative nature (Paffenholz & Spurk, 2006). Nor is the state too weak, the current governmental networks are strong. Maybe even too strong for the CSOs to actively change the current governmental course of data program usage.

While the coalition of CSOs was successful in their efforts to combat SyRI, the real social issue of the government using algorithmic risk assessment programs still prevails. This usage leads to a violation of privacy rights of citizens and carries risk of discrimination and profiling. In discussing the findings, five reasons were stated that explained this outcome. These were the visibility of the problem, the issues of combating against an anti-fraud system and the current discourse of digitalising. These reasons can be attributed to problems which are caused by algorithmic governmental programs. The other two reason were the electoral blockade and the slow speed of political change. These are part of an underlying matter which concerns a broader aspect of factors that influence the outcome of social action by CSOs. These problems are more deeply rooted in our society and political system and illustrate a flaw in our democracy.

The limited visibility of the SyRI problem is a hindrance in achieving social and political change, and this problem is also applicable to other algorithmic programs. These programs are not known by the public, so those affected are not aware that their problems are caused by these programs, problems simply happen to them. The coalition made a good effort to spread information about SyRI and its consequences. Unfortunately setting up campaigns, producing short explainer animations and handing out flyers is expensive. CSOs are known to have little financial support and are mostly dependent on non-paid staff. A possible solution to these financial limitations would be to convince high profile individuals or organisations with lots of social reach to join the cause.

The difficulty of advocating against an anti-fraud program is that one must convince people that the remedy is worse than the disease. The program has good intentions, and it is up to CSOs to steer the conversation away from whether combating fraud is a good thing or not, and towards the privacy issues that arise when using data and algorithmic problems to combat fraud. The coalition did a good job on conveying this message to the public, but they were hesitant to form a political movement. This was partly due to the focus on winning the lawsuit,

but also because of the nature of the privacy CSOs. The CSOs that participated in the coalition have large amounts of specific knowledge about data privacy and protection. During the interviews it became apparent that the focus of the coalition was to spread awareness about the threats of SyRI and to win the lawsuit against the Dutch government, not to sweep up the public to make sure that these kinds of systems are not used again. This way of mobilising populations may prove to be more fruitful in future efforts.

The last algorithmic specific issue is the current discourse of the government to seek salvation within technological and digital advancements. This is partly due to the usefulness of having access to a lot of data of the public. Yet using data, algorithms and statistics is also a very efficient way to control a population. Thus, it becomes a matter of power. Things are changing for the better however. The Dutch government is becoming increasingly aware of all the effects data and digitalisation of public services may have, whether they be good or bad. Increased awareness will hopefully lead to better and sustainable algorithmic programs. However, currently the coalition government is not changing its mind on the usage of algorithmic programs. In the coalition there is no free voting among the parliamentarians. It is a constant struggle for the different parties to get the deals that they want so they can achieve their goals. Sadly, this subject is not of much importance to any party, so they would rather just all vote in favour of these types of programs, for them to make a better deal on another subject. It is very hard to change this status quo. A political revolution of some kind would be helpful to change this current deadlock. Until then the only option is to keep striving for change and to keep engaging in this public issue.

Lastly, the issues of the electoral blockade and the slow process of change are not unique to the subject of algorithmic supported risk assessment programs like SyRI. These issues exist in all the themes that CSOs focus on. To evoke real change, change must happen in the higher echelons of society, in the ruling powers. In a democracy the ruling government is chosen by the people. The people in turn confide in the abilities of the politicians to represent the needs of the people. If the public does not have faith in the capability of a politician or a certain public party, they will not vote for them. The assumption that can be made here is that politicians who are being re-elected are doing a good job of representing the people. The handlings with the SyRI case however, made it obvious that if the politicians do not see clear electoral gain in addressing a certain issue, they will not address this. Despite an issue directly opposing the interests of the public. Only if a subject accumulated sufficient social attention will the politicians opt to address this politically. This is a flaw in our democracy. One that can only be fixed by constantly checking on the decisions that are being made by the government,

by being a vigilant society, which holds its lawmakers and government directly responsible for their own actions. Indubitably, this is a utopian view on how the public should behave proportionate to the government. Yet striving towards achieving this goal is a noble task which resonates clearly within the coalition of CSOs.

In this research the issues of SyRI were exposed, the inner workings of the coalition of CSOs were studied and the impact of this coalition was put in perspective. Some of the limitations of this research were the limited number of respondents that could be interviewed. This was mostly due to time constraints, although it could be somewhat attributed to the fact that for this research, the main subject of research was the coalition of CSOs and there were only a limited number of CSOs active in this coalition. In possible future research, it would be interesting to delve more deeply into the question of why the SyRI campaign was not successful in changing the current course of the Dutch coalition government. This study has shown that current Dutch politics is bureaucratic and very resistant in changing the status quo.

Bibliography

ANP. (2020). Overheid stopt met gebruik SyRI na uitspraak rechter. Het Parool. Geraadpleegd op 1 maart 2022, van https://www.parool.nl/nederland/overheid-stopt-met-gebruik-syri-na-uitspraak-rechter~bbf3993a/?referrer=https%3A%2F%2Fwww.google.com%2F

Autoriteit Persoonsgegevens. (2022). *Het werk van de AP*. Retrieved 6 June 2022, from https://www.autoriteitpersoonsgegevens.nl/nl/over-privacy/het-werk-van-de-ap

Babbie, E. R. (2020). The practice of social research. Cengage learning.

Brady, H. E. (2019). The challenge of big data and data science. *Annual Review of Political Science*, *22*, 297-323.

Bellanova, R., Irion, K., Lindskov Jacobsen, K., Ragazzi, F., Saugmann, R., & Suchman, L. (2021). Toward a critique of algorithmic violence. *International Political Sociology*, *15*(1), 121-150

Boeke, H. (2018). Uitleg over SyRI. Bij Voorbaat Verdacht. Retrieved 3 March 2022, from https://bijvoorbaatverdacht.nl/wat-is-syri/

Bullock, J. B. (2019). Artificial intelligence, discretion, and bureaucracy. The American Review of Public Administration, 49(7), 751–761. https://doi.org/10.1177/02750740198556123.

Deloitte United States. (2020). *Managing algorithmic risks*. Retrieved 6 June 2022, from https://www2.deloitte.com/us/en/pages/risk/articles/algorithmic-machine-learning-risk-management.html

De Sousa, W. G., de Melo, E. R. P., Bermejo, P. H. D. S., Farias, R. A. S., & Gomes, A. O. (2019). How and where is artificial intelligence in the public sector going? A literature review and research agenda. *Government Information Quarterly*, *36*(4), 101392.

De Vries, Y. (2021). Voorstel Super SyRI kan definitief naar de prullenbak. FNV. Retrieved 4 March 2022, from https://www.fnv.nl/nieuwsbericht/sectornieuws/uitkeringsgerechtigden/2021/11/voorstel-super-syri-kan-definitief-naar-de-prullen

Etzioni, A., & Etzioni, O. (2017). Incorporating ethics into artificial intelligence. *The Journal of Ethics*, *21*(4), 403-418.

Fukuda-Parr, S., & Gibbons, E. (2021). Emerging Consensus on 'Ethical AI': Human Rights Critique of Stakeholder Guidelines. *Global Policy*, *12*, 32-44.

Gibbons, E. D. (2021). Toward a more equal world: the human rights approach to extending the benefits of artificial intelligence. *IEEE Technology and Society Magazine*, *40*(1), 25-30.

Hess, D. J. (2009). The potentials and limitations of civil society research: Getting undone science done. Sociological Inquiry, 79(3), 306-327.

High-Level Expert Group on Artificial Intelligence. (2019). A definition of AI: Main capabilities and disciplines. Retrieved from Brussels https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341.

Kager, J. (2020). Algoritmesysteem SyRI in de ban na uitspraak rechtbank. FNV.

Retrieved 1 March 2022, from https://www.fnv.nl/nieuwsbericht/algemeen-nieuws/2020/02/algoritmesysteem-syri-in-de-ban-na-uitspraak-recht

Leslie, D. (2019). Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. *Available at SSRN 3403301*.

Liu, H.-W., Lin, C.-F., & Chen, Y.-J. (2019). Beyond state v Loomis: Artificial intelligence, government algorithmization and accountability. International Journal of Law and Information Technology, 27(2), 122–141. https://doi.org/10.1093/ijlit/eaz001.

Malik, N., Tripathi, S. N., Kar, A. K., & Gupta, S. (2021). Impact of artificial intelligence on employees working in industry 4.0 led organizations. *International Journal of Manpower*.

Ministerie van Sociale Zaken en Werkgelegenheid. (2020). Staat niet in hoger beroep tegen vonnis rechter inzake SyRI. Nieuwsbericht | Rijksoverheid.nl. Retrieved 1 March 2022, from https://www.rijksoverheid.nl/actueel/nieuws/2020/04/23/staat-niet-in-hoger-beroep-tegen-vonnis-rechter-inzake-syri

Newton, K. (2001). Trust, social capital, civil society, and democracy. International political science review, 22(2), 201-214.

Niklas, J., & Peña Gangadharan, S. (2018). Data-driven discrimination: a new challenge for civil society. Impact of Social Sciences Blog.

NOS. (2021). Rutte bezoekt Schilderswijk: 'Ik ga niet zoeken naar sociologische oorzaken'. Retrieved 6 June 2022, from https://nos.nl/video/2366092-rutte-bezoekt-schilderswijk-ik-ga-niet-zoeken-naar-sociologische-oorzaken

Paffenholz, T., & Spurk, C. (2006). Civil society, civic engagement, and peacebuilding. Social Development Papers: Conflict Prevention and Reconstruction, 36(2006), 10-55.

PILP. (2020). Profiling and SyRI. Retrieved 13 June 2022, from https://pilpnjcm.nl/en/dossiers/profiling-and-syri/

Polhuis, P. (2020). Algoritmen en de overheid: wat ging er mis bij SyRI? de-focus.nl. Retrieved 1 March 2022, from https://www.de-focus.nl/politiek_en_mensenrechten/algoritmen-en-de-overheid/

Rainey, S., Wakunuma, K., & Stahl, B. (2017). Civil society organisations in research: A literature-based typology. Voluntas, 28(5), 1988-2010. doi:https://doi-org.eur.idm.oclc.org/10.1007/s11266-016-9816-y

Robinson, S. C. (2020). Trust, transparency, and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI). *Technology in Society*, *63*, 101421.

Sampson, R. J., McAdam, D., MacIndoe, H., & Weffer-Elizondo, S. (2005). Civil society reconsidered: The durable nature and community structure of collective civic action. *American journal of sociology*, *111*(3), 673-714.

Scherer, M. U. (2015). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harv. JL & Tech.*, *29*, 353.

Starr, S. B. (2014). The risk assessment era: An overdue debate. *Fed. Sent'g Rep.*, *27*, 205.

Sztandar-Sztanderska, K., Kotnarowski, M., & Zieleńska, M. (2021). Are the algorithms

misleading? Meta-analysis of the algorithm for profiling of the unemployed used in Poland. *Studia Socjologiczne*, (1 (240)), 89-115.

Te Lintel Hekkert, P. (2021). FNV: Super SyRI is blauwdruk voor meer Toeslagenaffaires. FNV. Retrieved 4 march 2022, from https://www.fnv.nl/nieuwsbericht/sectornieuws/uitkeringsgerechtigden/2021/01/super-syri-is-blauwdruk-voor-meer-toeslagenaffaire

Trouw. (2020. De Toeslagenaffaire. Retrieved 4 March 2022, from https://verhalen.trouw.nl/toeslagenaffaire/

Van Eijk, G. (2017). Socioeconomic marginality in sentencing: The built-in bias in risk assessment tools and the reproduction of social inequality. *Punishment & Society*, *19*(4), 463-481.

Van Eijk, G. (2020). Algorithmic reasoning: The production of subjectivity through data. In *The Algorithmic Society* (pp. 119-134). Routledge.

Wijkprofiel Rotterdam, Hillesluis. (2022). wijkprofielrotterdam. https://wijkprofiel.rotterdam.nl/nl/2022/rotterdam/feijenoord/hillesluis?toon=alles

Willen. (2018). Van Ark: 'algoritmen niet gebruikt voor profileren'. Binnenlandsbestuur. Accessed on https://www.binnenlandsbestuur.nl/sociaal/van-ark-algoritmen-niet-gebruikt-voor-profileren-bijstandsgerechtigden

Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector—applications and challenges. *International Journal of Public Administration*, *42*(7), 596-615.

Wirtz, B. W., Weyerer, J. C., & Sturm, B. J. (2020). The dark sides of artificial intelligence: An integrated AI governance framework for public administration. *International Journal of Public Administration*, *43*(9), 818-829.

Zajko, M. (2022). Artificial intelligence, algorithms, and social inequality: Sociological contributions to contemporary debates. *Sociology Compass*, e12962.

Zheng, Y., Yu, H., Cui, L., Miao, C., Leung, C., & Yang, Q. (2018, April). SmartHS: An AI platform for improving government service provision. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 32, No. 1).

Zuiderwijk, A., Chen, Y. C., & Salem, F. (2021). Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*, *38*(3), 101577.

6. Appendices

6.1 Appendix A: Topic list

Introduction

- Introducing and thanking for the time
- Explaining my research
- Asking again if the conversation can be recorded
- Asking if the respondent has any questions before we begin

Stating the problem

- Could you introduce yourself?
- What was your involvement in the SyRI case?

Effectiveness of the coalition (if the respondent was a CSO actor)

- How did your organisation contribute to solving this issue?
- Did this prove to be successful? Why/ Why not?
- What would an improved version of SyRI look like?

Politics (if the respondent was an active politician)

- What do you think about the response of the house of representatives on this matter?
- How could CSOs influence this?
- How should the Dutch government handle programs like SyRI?
- Do you have a positive outlook on the future regarding this issue?
- What does the current situation say about our democratic rule of law?

6.2 Appendix B: Ethics and Privacy checklist

ERASMUS UNIVERSITEIT ROTTERDAM

CHECKLIST ETHICAL AND PRIVACY ASPECTS OF RESEARCH

INSTRUCTION

This checklist should be completed for every research study that is conducted at the Department of Public Administration and Sociology (DPAS). This checklist should be completed *before* commencing with data collection or approaching participants. Students can complete this checklist with help of their supervisor.

This checklist is a mandatory part of the empirical master's thesis and has to be uploaded along with the research proposal.

The guideline for ethical aspects of research of the Dutch Sociological Association (NSV) can be found on their website (http://www.nsv-sociologie.nl/?page_id=17). If you have doubts about ethical or privacy aspects of your research study, discuss and resolve the matter with your EUR supervisor. If needed and if advised to do so by your supervisor, you can also consult Dr. Jennifer A. Holland, coordinator of the Sociology Master's Thesis program.

PART I: GENERAL INFORMATION

Project title: 'SyRI: when the remedy is worse than the disease: A study of the engagement of civil society organisations against the governmental algorithmic risk assessment program SyRI'.

Name, email of student: Elmo Voeten - 482540ev@eur.nl

Name, email of supervisor: Rogier van Reekum - vanreekum@essb.eur.nl

Start date and duration: 4/10/2021 - aprox. 19/6/2022

Is the research study conducted within DPAS YES

If 'NO': at or for what institute or organization will the study be conducted? (e.g. internship organization)

PART II: HUMAN SUBJECTS

1.	Does your research involve human participants. YES

	If 'NO': skip to part V.

	If 'YES': does the study involve medical or physical research? NO

2.   Does your research involve field observations without manipulations
      that will not involve identification of participants.   NO

      If 'YES': skip to part IV.

    3.   Research involving completely anonymous data files (secondary
          data that has been anonymized by someone else).   NO

          If 'YES': skip to part IV.

PART III: PARTICIPANTS

1.   Will information about the nature of the study and about what
      participants can expect during the study be withheld from them?   NO

2.   Will any of the participants not be asked for verbal or written
      'informed consent,' whereby they agree to participate in the study?   YES

3.   Will information about the possibility to discontinue the participation
      at any time be withheld from participants?   NO

4.   Will the study involve actively deceiving the participants?   NO
      *Note: almost all research studies involve some kind of deception of participants. Try to
      think about what types of deception are ethical or non-ethical (e.g. purpose of the study
      is not told, coercion is exerted on participants, giving participants the feeling that they
      harm other people by making certain decisions, etc.).*

      1. Does the study involve the risk of causing psychological stress or
          negative emotions beyond those normally encountered by
          participants?   NO

      1. Will information be collected about special categories of data, as defined
          by the GDPR (e.g. racial or ethnic origin, political opinions, religious or
          philosophical beliefs, trade union membership, genetic data, biometric
          data for the purpose of uniquely identifying a person, data concerning
          mental or physical health, data concerning a person's sex life or sexual
          orientation)?   NO

      1. Will the study involve the participation of minors (<18 years old) or
          other groups that cannot give consent?
                                                                       NO
      1. Is the health and/or safety of participants at risk during the study?
                                                                       NO

      1. Can participants be identified by the study results or can the
          confidentiality of the participants' identity not be ensured?   NO

      2. Are there any other possible ethical issues with regard to this study?
                                                                       NO

If you have answered 'YES' to any of the previous questions, please indicate below why this issue is unavoidable in this study.

_____
_____
_____
_____

What safeguards are taken to relieve possible adverse consequences of these issues (e.g., informing participants about the study afterwards, extra safety regulations, etc.).

> All participants are made aware before conducting the interviews that, if they would want to, they could end the interview at any time. There is no need for stating a specific reason for this. The participants will be ensured that all gathered data about them is deleted if they stop during the interview or if they state their discontinuance with the study after the interview has taken place.

Are there any unintended circumstances in the study that can cause harm or have negative (emotional) consequences to the participants? Indicate what possible circumstances this could be.

> No

Please attach your informed consent form in Appendix I, if applicable.

Continue to part IV.

PART IV: SAMPLE

Where will you collect or obtain your data?

> Academic literature, and interviews with respondents.

Note: indicate for separate data sources.

What is the (anticipated) size of your sample?

> Aiming for 8 interview respondents.

Note: indicate for separate data sources.

What is the size of the population from which you will sample?

> Doing a qualitative research method, NA.

Note: indicate for separate data sources.

Continue to part V.

Part V: Data storage and backup

Where and when will you store your data in the short term, after acquisition?

> Google drive

Note: indicate for separate data sources, for instance for paper-and pencil test data, and for digital data files.

Who is responsible for the immediate day-to-day management, storage and backup of the data arising from your research?

> Me, Elmo Voeten

How (frequently) will you back-up your research data for short-term data security?

> Data in google drive is backed up automatically

In case of collecting personal data how will you anonymize the data?

> When transcribing the interviews, the respondents will get numbers instead of names. From this point forward, no respondent is being mentioned by his or her name.

Note: It is advisable to keep directly identifying personal details separated from the rest of the data. Personal details are then replaced by a key/ code. Only the code is part of the database with data and the list of respondents/research subjects is kept separate.

PART VI: SIGNATURE

Please note that it is your responsibility to follow the ethical guidelines in the conduct of your study. This includes providing information to participants about the study and ensuring confidentiality in storage and use of personal data. Treat participants respectfully, be on time at appointments, call participants when they have signed up for your study and fulfil promises made to participants.

Furthermore, it is your responsibility that data are authentic, of high quality and properly stored. The principle is always that the supervisor (or strictly speaking the Erasmus University Rotterdam) remains owner of the data, and that the student should therefore hand over all data to the supervisor.

Hereby I declare that the study will be conducted in accordance with the ethical guidelines of the Department of Public Administration and Sociology at Erasmus University Rotterdam. I have answered the questions truthfully.

Name student: Elmo Voeten   Name (EUR) supervisor:

Date: 3-3-2022   Date:

APPENDIX 1: Informed Consent Form

Informed Consent Form Master Thesis

Introduction

You are invited to participate in a research graduation project that is being carried out under the auspices of the Erasmus School of Social and Behavioural Sciences (ESSB), which forms part of the Erasmus University Rotterdam, The Netherlands.

The title of the research project is SyRI: when the remedy is worse than the disease: A study of the engagement of civil society organisations against the governmental algorithmic risk assessment program SyRI. In this project the impact of AI usage by the Dutch government is being researched. This is done through the perspective of the civil society organisations, who openly oppose improper and illegitimate usage of AI programs.

For more information about the research and the invitation to participate, you are welcome to contact the thesis student at any time: Elmo Voeten, 482540ev@eur.nl

Data collection

This interview takes place at a location of your choice and takes about 60 minutes. The interview will be audio recorded and transcribed. Your contact information will be replaced by a unique code and stored in a separate protected file. Reports of our analysis can never be traced back to individual persons.

Potential inconvenience & risks

There are no physical, legal or economic risks associated with your participation in this study. It is not mandatory to answer all questions. Your participation is voluntary, and you can stop at any time.

Reimbursement

This study does not include a reimbursement.

Data sharing

The collected data will be used only by the researcher conducting this study.

Confidentiality & data protection

The collected data will be used for an aggregated analysis and no confidential information or personal data will be included in the publications of the research, unless you give permission in the consent form. The data is stored in a secure location at the Erasmus University Rotterdam and will be kept for approximately 1 year after graduation.

Voluntary participation & individual rights

Your participation is voluntary, and you can stop at any time. When you participate in the research, you have the right to request more information about the data collection, analysis or withdraw the consent and ask for data erasure before the dataset is anonymized or manuscript submitted for publishing. You can exercise your rights by submitting an online request on the Data subject rights request portal of Erasmus University Rotterdam.

This research is supervised by Erasmus University Rotterdam. If you have any complaints regarding the processing of personal data in this research, please contact the Data Protection Officer via fg@eur.nl. You also have the right to submit a complaint at the Dutch Data Protection Authority.

Consent form: Combatting the Societal Impact caused by AI usage of the Dutch Government

Upon signing of this consent form, I confirm that:
- I've been informed about the purpose of the research, data collection and storage as explained in the information sheet;
- I've read the information sheet, or it has been read to me;
- I've had an opportunity to ask questions about the study; the questions have been answered sufficiently;
- I voluntarily agree to participate in this research;
- I understand that the information will be treated confidentially;
- I understand that I can stop participation any time or refuse to answer any questions without any consequences;
- I understand that I can withdraw my consent before the dataset is anonymized or manuscript submitted for publishing.

Additionally, I give permission to:

	Yes	No
I give permission to audio record the interview		
I give permission to use quotes from my interview		
I give those concerned my permission to approach me in the future for a follow-up study		

Name of research participant: _____

Date: _____

Signature: _____

_____

I hereby confirm that I've informed the research participant of all the aspects of the study.

Name of researcher: _____

Date: _____

Signature: _____

Ensure a copy for both the researcher and participant.

6.3 Appendix C: Interviews

**Table 1**

List of respondents

	Organisation	Date	Expertise
1.	FNV	11-04-2022	Had prior experience of working on public campaigns
2.	Bij Voorbaat Verdacht/Platform Bescherming Burgerrechten	25-04-2022	Was the campaign leader of Bij Voorbaat Verdacht
3.	Platform Bescherming Burgerrechten	09-05-2022	Past director of Platform Bescherming Burgerrechten, Founder of Stichting Bescherming Burgerrechten
4.	Privacy First	04-05-2022	Director at Privacy First, Legal advisor
5.	Piratenpartij	23-05-2022	Politician, Party leader
6.	Groenlinks Rotterdam	26-05-2022	Employee of Groenlinks Rotterdam
7.	Socialist Party SP	13-06-2022	Politician, current member of parliament and leading advocate in the toeslagen schandaal

6.4 Appendix D: Codes

Image 1
Code spheres
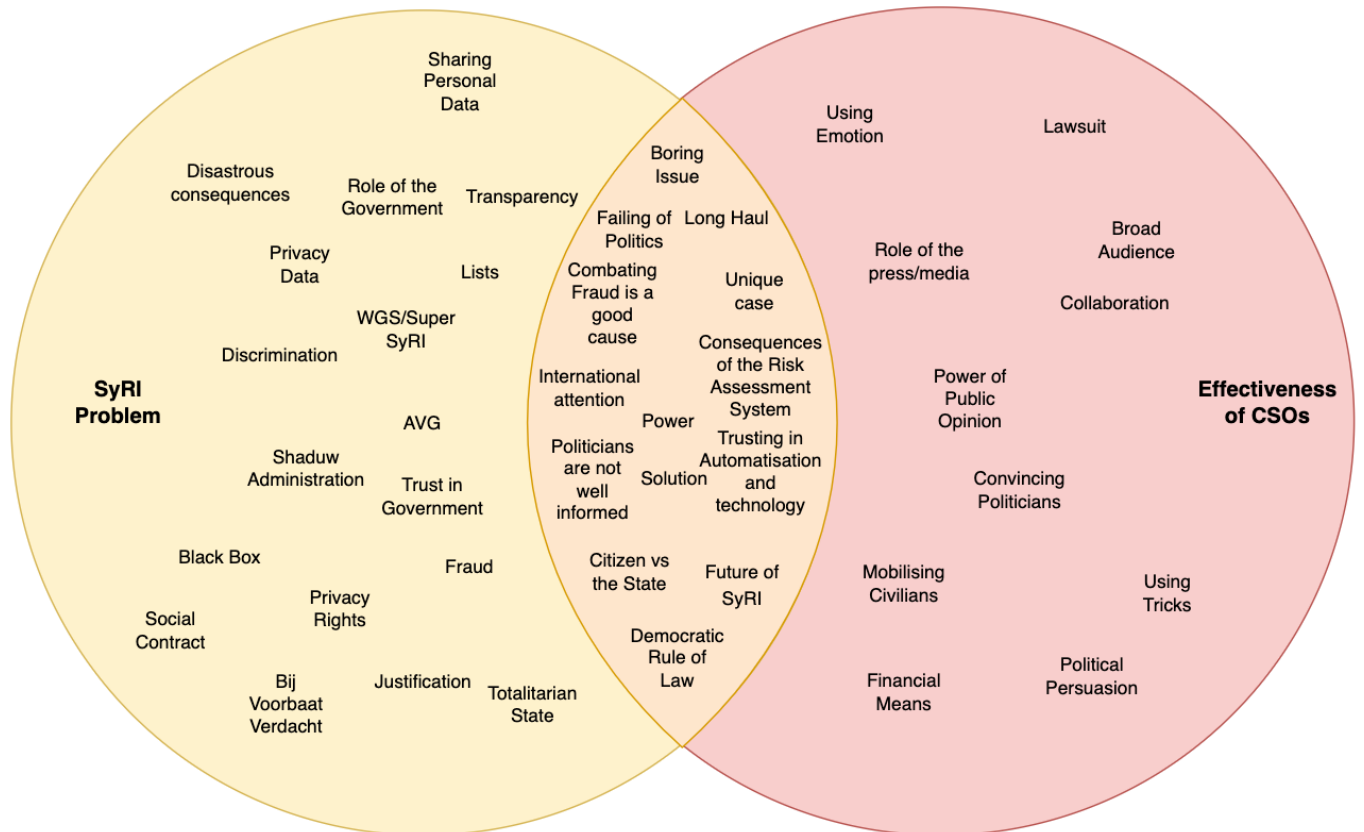
Note: The codes that were used to analyse the transcripts were placed in either the left sphere: regarding anything related to SyRI, or the right sphere: regarding anything that impacts the effectiveness of CSOs. Codes that have an impact on both were placed in the overlapping section in the middle.