Chapter 24
Fundamental Rights in Digital Welfare States: The Case of SyRI in the Netherlands

Sonja Bekker

Contents

Abstract Public authorities are increasingly using new technologies to perform public services. Worldwide, there are many examples of what the United Nations calls 'digital welfare states'. Although governments argue that new technologies make their services more efficient and cost-effective, many however express concern about the 'surveillance' of citizens. Given the widespread emergence of digital welfare states, universal guidelines are needed to explore the opportunities they offer but also their legitimate boundaries. A Dutch court case on the System Risk Indication (SyRI) is one of the first to use human rights as a basis to assess the use of new technologies for fighting social security fraud. The court case may serve as an example of how human rights may offer relevant guidance to public authorities using new technologies in a responsible manner and making sure that these contribute to the economic and social wellbeing of all citizens.

Sonja Bekker holds the Jean Monnet Chair European Social Policy and is Associate Professor at Utrecht University and Tilburg University, both in the Netherlands. S.Bekker@uu.nl.

S. Bekker (✉)
Utrecht University, Utrecht, the Netherlands
e-mail: S.Bekker@uu.nl

O. Spijkers et al. (eds.), *Netherlands Yearbook of International Law 2019*, Netherlands Yearbook of International Law 50,
https://doi.org/10.1007/978-94-6265-403-7_24

Keywords Digital welfare state · Privacy · SyRI

24.1 Introduction

Big data not only promises a wealth of information to scientists and private companies. Public authorities also have an increasing interest in using big data. The United Nations (UN) even speaks of emerging and already existing 'digital welfare states'.[1] These may be found in many part of the world, and have many different forms. Yet, digital welfare states always consist of systems of social protection and assistance which are '… increasingly driven by digital data and technologies that are used to automate, predict, identify, surveil, detect, target and punish'.[2] This contribution gives a key example of the use of a digital system in the context of social security in the Netherlands, named SyRI (System Risk Indication). SyRI matches several public data sources in order to detect an increased risk at social security fraud.[3] SyRI has been the subject of one of the first legal challenges, which considers human rights in digital welfare states. The UN has called the recent court decision a landmark ruling.[4] Thus, the SyRI case is a unique example of litigation in which the use of digital tools to prevent and detect welfare fraud has been challenged on grounds of human rights.[5] The purpose of this contribution is to map out which human rights feature in this court case, and to explain why the plaintiffs as well as the court find these human rights relevant. It thus provides input into international debates on human rights in the digital welfare state.

Scholars argue that digitalisation, the use of big data, algorithms and artificial intelligence raises a range of questions on human rights protection.[6] Not only privacy is at stake. Questions expand to the impact of digitalisation on public and ethical values, autonomy, human dignity and wellbeing.[7] Such fundamental questions go beyond the single case of SyRI in the Netherlands, but feature in any developing e-government and digital welfare state.[8] Additionally, they do not concern solely the use of an algorithm or technology, yet cover the broad social and political context in which technological tools are designed and used. Bertelsmann Stiftung and Algorithm Watch argue that the focus should be on the entire society that '…. affect

[1] UN 'Report of the Special rapporteur on extreme poverty and human rights' Seventy-fourth session, Item 72(b) on the provisional agenda, A/74/48,037, 11 October 2019.

[2] Id, p. 1.

[3] Decision on SyRI (Besluit SyRI), Ministry of Social Affairs and Employment the Netherlands, 17 April 2014, number 0056263.

[4] UN 'Landmark ruling by Dutch court stops government attempts to spy on the poor—UN expert', Press release, 5 February 2020.

[5] Ibid., at 1.

[6] Gerards 2019; Yeung and Lodge 2019; Jak and Bastiaans 2018; Mantelero 2018.

[7] Gantchev 2019; Mantelero 2018; Rathenau Instituut (2018) Doelgericht digitaliseren – Hoe Nederland werkt aan een digitale transitie waarin mensen en waarden centraal staan. Rathenau Instituut, The Hague; Allen 2016.

[8] Rathenau Instituut (2018) Doelgericht digitaliseren – Hoe Nederland werkt aan een digitale transitie waarin mensen en waarden centraal staan. Rathenau Instituut, The Hague.

justice, equality, participation and public welfare, either directly or indirectly'.[9] Taking a holistic approach includes assessing the broad socio-technological framework, encompassing the decision-making model, the algorithm that converts this model into a computable code, the data this code uses as an input, as well as the political and economic environment surrounding its use. This context is also relevant to assess the use of SyRI, including its specific purpose to fight fraud. Questions about SyRI thus cover whether the use of the data is legal and what decision-making model is applied.[10] Does this decision-making model have certain problematic biases (e.g. using a biased data set or being developed by people with underlying prejudices that were not controlled for)? Why did the government come up with the idea to use SyRI? Is there a problem that cannot be addressed in any other way (e.g. viewing the inherent complexity of the problem)? What role did austerity measures have in deciding to limit the number of 'human' caseworkers, and start using automation as a cheaper option? Were decisions taken in a political climate leading to increased pressure on poor people to take on low-paying jobs?[11] Studying SyRI and the arguments used in court helps sketching the implications of the use of big data and algorithms in welfare provision for the protection of human rights, including the political context and societal implications. Therefore, the recent court decision is seen as a landmark ruling, which sets a strong legal precedent for other courts.[12]

This contribution first sketches the main characteristics of the SyRI system and the context of the court case. Then, it reviews the main fundamental rights challenges, mainly focusing on the respect of private life, the protection of personal data, and the right to a fair trial. Subsequently, it gives the key points of the court ruling. It concludes with an outlook on fundamental rights in digital welfare states.

24.2 Development of SyRI and Its Characteristics

"I think that people underestimate what the threat of SyRI can do to people. My mother is panicking. She has a spare bed for guests. Sometimes my grandmother spends the night at our house. Due to SyRI my mother is scared. She is afraid that the spare bed might be explained as us having a housemate, which would affect her benefit entitlements".[13] This quote is from a worried son, living in a neighbourhood in Rotterdam that was part of a SyRI project. The quote not only sketches the context

[9] Bertelsmann Stiftung and Algorithm Watch (2019) Automating Society; Taking Stock of Automated Decision Making in the EU, Bertelsmann Stiftung and Algorithm Watch, Berlin. Bertelsmann Stiftung and Algorithm Watch 2019:9.

[10] Bertelsmann Stiftung and Algorithm Watch 2019:9.

[11] Ibid., at 10.

[12] Ibid., at 4.

[13] FNV 2019. Press release, FNV en bewoners Rotterdamse wijken Hillesluis en Bloemhof vieren intrekking SyRI-project Rotterdam, 16 July 2019, https://www.fnv.nl/nieuwsbericht/sectornieuws/uitkeringsgerechtigden/2019/07/fnv-en-bewoners-rotterdamse-wijken-hillesluis-en-b(last accessed 9 July 2020).

in which SyRI was created and used: a focus on detecting fraud in vulnerable neighbourhoods. It also shows the operation and impact of SyRI: citizens not knowing whether they are surveilled and what behaviour 'the system' sees as suspicious. This might result in fear and anxiety. Such elements of a lack of transparency and anxiety feature both in the arguments of the plaintiffs and in the ruling of the court.

It is not surprising that Dutch citizens do not know whether they are inspected by SyRI, or which characteristics lead to a suspicion of committing fraud. SyRI may gather a wide range of personal data, and its analytical methods are deliberately kept secret. SyRI enables public administrations in the Netherlands to combine stand-alone data sources containing personal data. The purpose is to detect social security fraud, tax and social premium fraud, or violation of labour law by individuals or companies. Data matching via SyRI is quite extensive, making it an example of the wide range of different systems that governments may use to understand and monitor citizens.[14] SyRI did not emerge suddenly. Like in many states, the Netherlands has a long history of incorporating new technologies in the operation of its social security provisions, including for detecting fraud.[15] Such early practices already received critical comments by the Dutch Data Protection Authority (DPA) on the scope of data processing vis-à-vis the principles of proportionality and transparency.[16] The Dutch DPA also posed critical questions about follow-up initiatives of these early practices. Relevant issues included linking stand-alone databases in order to detect fraud, but also starting investigations without having a prior suspicion of fraud. Moreover, the insufficient purpose limitation and transparency rights of individuals were criticised.[17] Arguably, such criticisms have been a reason for the Dutch government to develop a legal basis for data matching projects, eventually leading to the implementation of SyRI. Around 2012, the Dutch government started developing ideas on the design of SyRI, and these were discussed in the Second Chamber of Parliament. SyRI was not developed as a separate Act, but as an amendment of the existing Act SUWI (Structure of the Implementation of the Labour and Income Act of 2001). SUWI arranges the structure of the different public organisations that provide different types of social security, such as welfare, pensions, child-care allowances and unemployment benefits.[18] As SyRI was only a small amendment of Act SUWI, it is called the Decision on SyRI (*Besluit SyRI*). The court, in its ruling, however calls it SyRI-legislation.

Originally, SyRI combined different aims. It should enable sharing data between different public service providers in order to prevent and fight fraud.[19] Moreover,

[14] Ibid., at 1. Van der Sloot and Van Schendel 2019.

[15] Gantchev 2019; Olsthoorn 2016; Brief by the United Nation Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550,982/HA ZA 18/388).

[16] Gantchev 2019, at; Brief by the United Nation Special Rapporteur, at 15.

[17] Gantchev 2019; Brief by the United Nation Special Rapporteur, at 15.

[18] Act SUWI of 29 November 2001: Wet structuur uitvoeringsorganisatie werk en inkomen.

[19] Kamerstukken II 2012–2013, 33 579 nr. 7, 25 June 2013.

SyRI should increase the efficiency of public administration, creating one data entry-point for citizens, after which other public administrations could make copies. Additionally, SyRI would reduce implementation costs. Later on, the aim to fight fraud started to prevail. This all happened in a context of austerity measures on public administrations, and experiments with digitalization of public services.[20]

The decision on SyRI mentions a number of 'partners' in data sharing, including the Dutch Tax and Customs Administration, the Labour Inspectorate, the Public Employment Service, municipalities, the organisation that implements the Dutch national insurance schemes (SVB), the Ministry of Social Affairs and Employment and the Ministry of Finances. These public organisations all have single databases with data of citizens and/or companies. Article 64(1) of Act SUWI adds that, depending on the particular SyRI project and its goals, other administrative bodies and persons may become partner in data sharing as well, if they perform public law tasks. The Ministry of Social Affairs and Employment is formally responsible for the processing of personal data.[21] The Act SUWI lists the categories of personal information that feed the algorithm.[22] It includes 17 different categories of which one or more may be used, including information on employment, detention, sanctions, fiscal information, and information on education, pension, child-care allowances, benefit receipt, health insurance. This data may stem from different databases of the government, which may be linked to each other in order to get a more complete profile of persons.[23] Public administrations collect this data for various reasons, for instance because they are responsible for establishing the right to child-care benefits or provide for pensions. In the explanatory note attached to the decision on SyRI, the legislator explains that the list does not include sensitive personal data, for instance because no data on the health of people is processed, but only data on their health insurance.[24]

24.2.1 Concerns in the Drafting Stage of the Decision on SyRI

Already in the drafting of the decision on SyRI, concerns have been raised, notably by key advisory bodies to the government. The Dutch DPA has given two negative advices on legislative proposals to implement SyRI, both in 2012[25] and in 2014.[26]

[20] Bekker 2020.

[21] Ibid., at 19.

[22] Besluit [Decision] SyRI Article 2 on the preconditions for the use of SyRI.

[23] Article 3 Besluit [Decision] SyRI.

[24] Explanatory note (Nota van Toelichting), p. 7.)

[25] At that time still called SARI (System Anonymous Risk Indication), CPB, Advice for the Ministry of Social Affairs and Employment, 4 June 2012, number z2012-00237.

[26] CPB, Advice to the Ministry of Social Affairs and Employment, 18 February 2014, number z2013-00969.

It has had a number of remarks and critiques, yet the main ones refer to Article 8 of the European Convention on Human Rights (ECHR) on the right to respect for private and family life, home and correspondence. The DPA argues that the government should describe in more detail which types of data may be processed of which groups of citizens, which circumstances require the processing of data, and what procedures apply. Moreover, it has made comments on the principles of specified, explicit and legitimate purposes of data processing, data minimisation and storage limitation.[27] The 2014 advice repeats some of these concerns, specifically addressing issues such as the principle to 'select before you collect' in order to limit the risk of including data of too many individuals. Moreover, the Dutch DPA questions practices that make profiles based on negative characteristics such as debts, violations and sanctions, as this risks breaching an individual's privacy to a larger degree than might be necessary. In addition, the government's idea to collect and process special categories of personal data was criticised. Data sharing includes information on detention and health. The Dutch DPA argues that using such sensitive data requires more convincing arguments.[28] In 2014, another key institution in the Netherlands, the Council of State, has given similar concerns in its advice on the decision on SyRI to the government and Parliament.[29] It has advised the government to assess critically the large number of categories of personal information gathered, and the necessity to have that much data included in data sharing and profiling activities. It advices the government to explore less intrusive methods to detect social security fraud. The Council of State finds that the list of types of personal data is very extensive, and can hardly think of data that would not be included in data sharing and profiling activities. To the Council of State, it even seems that the government wants to keep all options open, whereas the government should mind data minimisation. A second main concern, which is similar to the Dutch DPA's conclusion, is the use of special personal data on health and sanctions. The Council of State recommends to take these types of data out of the proposed Act. Third, the Council points at the principle of 'select before you collect' and advices to improve the proposal. Fourth, it argues that the government should consider informing persons that they are subject of investigations which might lead to a risk alert. Regarding the latter, in SyRI, a certain combination of scores on indicators leads the system to identify persons (or organisations) with a higher risk of committing fraud. The Council argues that such a risk alert is not insignificant, as a risk alert points at a concern of breaking the law, which is then reported to the public organisation responsible for further investigating the suspicion. If such an investigation does not lead to a sanction (e.g. because the person is innocent), that person is not likely to find out that he or she was subject of

[27] Ibid., at 23.

[28] Ibid., at 23.

[29] The Council of State (Raad van State) advises the government and Parliament on legislation and governance. Its advice is Raad van State 'Ontwerpbesluit houdende regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens (Besluit SyRI), met nota van toelichting', W12.14.0102/III, 15 May 2014, Staatscourant 2014, number 26306.

investigation. Hence, he or she will never inquire whether or not (s)he is registered as a person with a high risk of committing fraud.

The concerns raised in the drafting stage of the decision on SyRI led to some alterations of the proposal, however these have found to be quite superficial or pragmatic.[30] Although SyRI was discussed by the Second Chamber of Parliament, many feel that this discussion was not extensive enough, viewing the act's far-reaching impact.[31] Eventually, SyRI entered into force in 2014, offering a legal basis to data-sharing practices that had already been taken place.[32]

24.2.2 SyRI in Operation

The past years SyRI has been in operation several times, making information available on its use and effectiveness. This has given rise to further concerns, which also have been raised in court. SyRI operates as follows. For each SyRI project, the project goal determines which databases and data is required. Each project has its own set of indicators, or risk model, which is seen as predictive for higher risks at committing social security fraud. The collected personal data is encrypted and then matched by the body responsible for the data analysis.[33] If data matches the risk model, the respective personal data are decrypted and send back to the public administration. Moreover, the risk notification is added to a central register, which will keep the notification for two years.[34] The risk notifications may be used by the public administrations that are part of the particular SyRI project in order to conduct follow-up research into the high-risk fraud case. So far, SyRI has been used in neighbourhoods of four Dutch cities, mostly neighbourhoods with a higher concentration of poorer and more vulnerable groups.[35] Seemingly, this has not led to a conviction or sanction of people committing social security fraud.[36] In the court case, both in the hearing and in the ruling, many concerns have played a role, which were expressed already in the

[30] Gantchev 2019.

[31] See Parliamentary documents Kamerstukken II 2012–2013, 3357, nr. 7; Olsthoorn 2016, who interprets the limited Parliamentary discussion as the Act getting unanimous support.

[32] Olsthoorn 2016.

[33] Gantchev 2019.

[34] Gantchev 2019.

[35] Brief by the United Nation Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550,982/HA ZA 18/388.

[36] RTL Nieuws, 'Blijf met je klauwen van m'n wijkie af': vier vragen over fraudedetector SyRI, 29 October 2019; see also data on use, number of households surveilled and evaluation on effectiveness in the document: Ministry Social Affairs and Employment, wob-verzoek over Systeem Risico Indicatie, 26–06-2019, 2018–0,000,185,252, notably the annex. Last accessed 03–02-2020, https://www.rijksoverheid.nl/documenten/wob-verzoeken/2019/06/26/besluit-op-wob-verzoek-over-systeem-risico-indicatie; Olsthoorn 2016 gives some numbers for uncovering fraud before 2014 (thus before SyRI yet using data linkage), taken into account a wider range of fraud detecting activities than welfare fraud only.

drafting stage of the decision on SyRI. The plaintiffs in the court case have requested a thorough check of SyRI against the requirements of international law. They claim that SyRI has never been subject to an integral check against legal principles, the more so because it passed the Parliament without notable discussions, in spite of negative advices and criticisms by the Dutch DPA and the Council of State.[37]

24.2.3 Context of Court Case

Eights parties have formed a coalition and started a lawsuit against the state, including NGOs, the largest Dutch trade union (FNV) and two citizens, challenging the practice of mass profiling of citizens who are not suspected of any violation or crime.[38] SyRI, they argue, profiles whole neighbourhoods in order to assess the likelihood that citizens commit fraud when using social security provisions. The algorithm on which SyRI runs is not transparent and consequently cannot be checked. A salient factor is that SyRI has been used especially in neighbourhoods and areas with a higher concentration of people experiencing poverty or people belonging to vulnerable groups.

A combination of concerns has led the UN Special Rapporteur on extreme poverty and human rights, Philip Alston, to write an amicus brief to the Dutch district court, presenting his views on the case from the perspective of human rights. His interests include the possible legal precedent which the case may set concerning human rights protection of poor and vulnerable individuals living in a digital welfare state.[39] In particular, Alston addresses the right to social security and the right to privacy. He sees the broad coalition of diverse NGOs entering into the legal proceeding, as a sign of widely shared concerns about the human rights implications of SyRI. Moreover, while focusing on specific groups of people, SyRI might be expanded to larger groups of individuals, likely affecting everyone's rights in the future. The next sections zoom in on the main human rights categories that play a role in the court case: respect for private life, the protection of personal data, and the right to a fair trial. The hearing

[37]In December 2019, the Dutch DPA published a list that further details when a Data Protection Impact Assessment should be made, before the processing of personal data may start. This list includes the large-scale processing and/or structural monitoring of (sensitive) personal data for the purpose of fighting fraud. It gives as an example fighting fraud by social services or by insurance companies.

[38]The coalition of plaintiffs exists of: Platform for the Protection of Civil Rights (Stichting Platform Bescherming Burgerrechten), Dutch Committee of human rights lawyers (Nederlands Juristen Comité voor de Mensenrechten (NJCM), Privacy First Foundation (Stichting Privacy First), Foundation Psychotherapists and Psychologists (Stichting Koepel van DBC-vrije Praktijken van Psychotherapeuten en Psychiaters (KDVP), and the National Board of clients (representing associations of e.g. pensioners and people who have a chronic disease - Landelijke Cliëntenraad), supported by authors Tommy Wieringa and Maxim Februari. In July 2018, the national trade union FNV (Federatie Nederlandse Vakbonden) joined the coalition.

[39]Brief by the United Nation Special Rapporteur at 15.

in the district court has taken place on 29 October 2019 and the ruling was given on 5 February 2020.[40]

24.3 Respect for Private Life and Protection of Personal Data

Privacy is one of the first human rights concerns mentioned when debating the use of personal information, by either private companies, research or public administrations.[41] Such concerns feed overarching questions on big data and privacy.[42] Do certain privacies face extinction, and if so, does this matter? Are privacy rights fundamental or only optional? Do individuals still have ethical responsibilities to care for the protection of their personal information?[43] Individuals might feel or be quite powerless in their attempts to safeguard their personal data. Thus, is there a need to develop a collective and political approach to the protection of privacy?[44] Related to governments and public administrations, some authors call to strengthen and protect public values when developing and using digital tools for public services.[45] This should include safeguarding the relationship between citizens, the government, and businesses. Others sketch the dilemma for the state to protect personal freedom of citizens while also being responsible for the security of its citizens.[46] Indeed, fighting fraud in order to maintain support for social security has been a main reason for the Dutch government to develop SyRI.[47] Moreover, by introducing SyRI, the government provided a legal basis for already existing data matching activities.[48]

In the court case, the plaintiffs have brought forward Article 8 EHCR and Articles 7 and 8 of the European Charter of Fundamental Rights (Charter) on the respect for private and family life and the protection of personal data, underlining that citizens should be protected against disproportionate and arbitrary interference of public authorities in their private lives.[49] Exceptions to this rule are possible, yet should

[40] Case number C/09/550,982/HA ZA 18/388, the Netherlands.

[41] Gerards 2019; Rathenau Instituut (2018) Doelgericht digitaliseren – Hoe Nederland werkt aan een digitale transitie waarin mensen en waarden centraal staan. Rathenau Instituut, The Hague.

[42] The set of questions is asked by Allen 2019: 1.

[43] Allen 2019: 1.

[44] Allen 2016.

[45] E.g. Van der Sloot and Van Schendel 2019; Bertelsmann Stiftung and Algorithm Watch 2019:9, Automating Society; Taking Stock of Automated Decision-Making in the EU; ibid., at 1.

[46] Broeders et al. 2017; Gerards 2019.

[47] Kamerstukken II 2012–2013, 33 579 nr. 7, 25 June 2013.

[48] Olsthoorn 2016.

[49] Pleitnotities NJCM c.s. Solv. and Ekker, for Court hearing of 29 October 2019, Case number C/09/550,982/HA ZA 18/388. Reference is also made to Article 17 of the International Covenant on Civil and Political Rights, determining that: 17(1) no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 17 (2) Everyone has the right to the protection of the law against such

be subject to strict demands. It has to be '… in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'[50] The plaintiffs and the government agree that the decision on SyRI limits these rights.[51] However, then citizens are entitled to information and transparency, the plaintiffs argue. Moreover, limitations to such rights have to be necessary, and there should be an effective and independent reviewer.[52] Similar rules on the necessity, proportionality and subsidiarity are part of the European General Data Protection Regulation (GDPR).

24.3.1 Necessity, Proportionality and Transparency

Article 8(2) ECHR thus sets that if the right to respect for private life is curtailed, this has to be prescribed by law, necessary, and there should be an independent inspectorate. A first question thus concerns whether it is indeed necessary for the Dutch government to match and run personal data from various public authorities in order to prevent and detect fraud. The (still) little effectiveness of SyRI to detect welfare benefit fraud points at the state having more effective tools to fight fraud which moreover requires less data processing (i.e. special police officers investigating fraud and only scrutinising a few people). The plaintiffs argue that necessity should be checked against the existence of a pressing social need, and question this given the ineffectiveness of SyRI.[53] However, if large-scale data matching is necessary, a second question refers to transparency. Many arguments are attached to this second question. The plaintiffs summarise these as the requirement that the law should be accessible, foreseeable, and sufficiently precise, and moreover should take safety measures against abuse and arbitrary decisions.[54]

One difficult issue emerges already at the start of data collection. Each public administration collects data of citizens for a different purpose. This purpose might be legitimate, for instance to know whether someone is resident of a municipality. However, this citizen does not know that this data will or might be used for fraud

interference or attacks. See Dagvaarding bodemprocedure SyRi, Deikwijs advocaten, 27 March 2018. See Gantchev 2019 for outlining related EU General Data Protection Regulation (GDPR) such as Article 5 on the principle of lawful, transparent and fair data processing, as well as purpose limitation and Article 6 on proportionality.

[50] Article 8.2 EHCR.

[51] Kamerstukken II, 2012–2013, 33,579 nr.3 The government argues in its explanations to Parliament that it has weighed the aims of the protection of economic welfare fighting fraud against the protection of privacy, and finds the former to have a larger weight, section 3a.

[52] See Dagvaarding bodemprocedure SyRi, Deikwijs advocaten, 27 March 2018.

[53] Pleitnotities NJCM c.s. Solv. and Ekker, for Court hearing of 29 October 2019, Case number C/09/550,982/HA ZA 18/388, section 7.1 to 7.3.

[54] Dagvaarding bodemprocedure SyRi, Deikwijs advocaten, 27 March 2018, section 4.7.

detection as well. In addition, while sharing some data with a public administration might be harmless, the interconnection of databases converts isolated data into a rich description of someone's life. Moreover, citizens can hardly ever opt-out from giving their data to the government, for instance people are obliged to declare their income and savings to the tax authorities. Authors argue that defining the purpose of data collection is an important question when dealing with big data, as this often involves the reuse and matching of data. This characteristic of big data seems at odds with the requirements that personal data may only be collected and processed for a specific purpose.[55] The plaintiffs in the court case argue that specifically described purposes are not only a requirement by law. They are also necessary in order to check whether data processing is necessary and proportionate.[56] The plaintiffs address this issue partly under the heading of purpose limitation. They refer to the government's deliberate aim to use a wide definition of purpose limitation, in order to facilitate the cooperation of public administration when detecting fraud. The government acknowledges this, but argues that by defining a specific purpose in each SyRI investigation, the amount of data will be limited. The purpose of the investigation determines which data needs to be shared by whom.[57] The plaintiffs argue that such *wide* purpose *limitation* could be seen as a *contradiction in terminis*.[58]

Additionally, the plaintiffs find that by using data sources that were never intended for 'secret' investigations, every interaction between citizens and the government may have legal consequences. They call it 'shadow accounting' by the state. This may have a large impact on the trust citizens have in the government, potentially leading to a chilling effect on the willingness of citizens to share their data with public administrations.[59] This effect is increased by the lack of an independent inspectorate checking the SyRI system,[60] and the lack of information to citizens about the processing of their data. Both the special rapporteur of the UN and the plaintiffs state that SyRI's data-linking exercises might give a very intimate picture of individuals' lives[61] collected via an intrusive process, using data that was originally collected for and justified by reference to a specific goal, and via SyRI gets used in

[55] Kool et al. 2015; Rathenau Instituut 2018. The explanation of Article 5a.1 explicitly mentions that data collected by public services in order to establish the legitimacy of benefit receipt, may be used also for SyRI projects, based on Article 64 Act SUWI. See Nota van Toelichting, Staatsblad 2014, 320; 11–09-2014.

[56] Pleitnotities NJCM c.s. Solv. and Ekker, for Court hearing of 29 October 2019, Case number C/09/550,982/HA ZA 18/388, sections 6.4 and 6.5.

[57] Kamerstukken II, 2012–2013, 33,579 nr.3 https://zoek.officielebekendmakingen.nl/kst-33579-3.html

[58] Dagvaarding bodemprocedure SyRi, Deikwijs advocaten, 27 March 2018, 5.11.

[59] Dagvaarding bodemprocedure SyRi, Deikwijs advocaten, 27 March 2018, section 1.7.

[60] See Article 13 ECHR.

[61] E.g. Municipalities collect personal data to establish residence of people, including names, gender, date and place of birth, home address, family constellation and social security number. Public employment services might have data on work history and, depending on a person's situation, re-integration activities, extent to which someone is found fit to work, benefit receipt, etc. Such sources are linked.

ways that were not foreseen and unannounced.[62] The plaintiffs argue that the purpose of data processing is extremely broad, meaning that there is no meaningful limitation of the competences of the government.[63] Additionally, the plaintiffs and the special rapporteur of the UN find that the SyRI-legislation lacks clarity. This means that citizens will face difficulties in knowing or expecting in advance about how SyRI could affect their rights. SyRI only gives a very general idea of its functioning and what effect this will have.

24.3.2 Does SyRI Make (Automated) Decisions?

Related to above, an important question to answer is whether SyRI actually takes a decision. Additionally, it is relevant to know that if SyRI makes decisions, whether or not this is automated decision-making. The GDPR arranges the right not to be subject to a decision based solely on automated processing.[64] According to the Dutch government, SyRI merely checks for discrepancies between the data within the different databases, and this does not involve automated decision-procedures.[65] If there are discrepancies between the data sources, one or more of the administrative bodies involved in the particular SyRI project should conduct further research prior to taking decisions that may have an effect on people's legal rights.[66] This means that SyRI merely signals discrepancies between the data and the designated risk indicators, after which investigations by humans follow (if one of the public bodies indeed decides to start further research). Could SyRI thus be viewed as just a tool that does not make decisions itself? Does the use of SyRI lead to decisions *solely* based on automated processing?

In the literature there is much debate on such questions. One such line of debate involves at which moment in time we should speak of a *decision*: before, during

[62] Brief by the United Nation Special Rapporteur at 15; and Pleitnotities NJCM c.s. Solv. and Ekker, for Court hearing of 29 October 2019, Case number C/09/550,982/HA ZA 18/388.

[63] Pleitnotities NJCM c.s. Solv. and Ekker, for Court hearing of 29 October 2019, Case number C/09/550,982/HA ZA 18/388, section 6.5. See also similar remarks of the Council of State on the draft legislation in 2014, which the Council of State repeated in its unsolicited advice in 2018.

[64] Article 22 GDPR 'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.'.

[65] Letter to Dutch Parliament of 8 June 2018: Kamerstukken II, 2017–2018, 32 761, nr. 122; repeated in a government reaction to the unsolicited advice of the Council of State, Ongevraagd advies over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen, Number W04.18.0230/I, 31 August 2018.

[66] Letter to Dutch Parliament of 8 June 2018: Kamerstukken II, 2017–2018, 32 761, nr. 122; repeated in a government reaction to the unsolicited advice of the Council of State, Ongevraagd advies over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen, Number W04.18.0230/I, 31 August 2018.

or after the automated processing?[67] Follow-up questions include the role of civil servants. Do they base their decision on whatever the automated outcomes suggest? The Guidelines on Automated individual decision-making and Profiling explain that human involvement in decision-making should be meaningful, and not just a token gesture.[68] Additionally, questions should be posed on the effect of decisions. Do decisions have a 'legal' or 'similarly significant' effects on people?[69] Here, the parties in the court case have different views. The government speaks of merely checking for 'discrepancies between data sources', after which the real investigation and decision-taking is done by humans. Others speak of 'risk alerts' or 'flagging', which already refers to a more serious effect on people.[70] The UN interprets such flagging, as a result of data base combinations by SyRI, as individuals being quite significantly 'inconvenienced' by becoming the object of government scrutiny.[71] Also the Council of State finds that being 'flagged' is not insignificant,[72] specifically as all risk alerts pointing at potential fraud are collected in a central data base and stored for two years.[73] Moreover, individuals may never find out that they have been flagged, if no sanction or conviction follows. The UN finds that also without being flagged, individuals are 'inconvenienced' for the mere fact that their personal data becomes part of much higher level of analysis than citizens who are not part of the database.[74] Building on the question concerning clarity, the plaintiffs argue that automated data processing and decision-making requires particularly, clear descriptions of the circumstances in which and the conditions under which public governments may exercise their rights.[75] They find that SyRI does not meet this requirement, as it is an unspecified automated processing of personal data based on risk models. Moreover, these risk models remain unknown to the public and are deliberately kept secret, an argument

[67] E.g. Jak and Bastiaans 2018; Rathenau Instituut (2018) Doelgericht digitaliseren – Hoe Nederland werkt aan een digitale transitie waarin mensen en waarden centraal staan. Rathenau Instituut, The Hague. Such questions may also include what the minimum role of humans should be at which stage of decision-making.

[68] Jak and Bastiaans 2018; Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p.21.

[69] Article 22 GDPR.

[70] Vetzo et al. 2018.

[71] Brief by the United Nation Special Rapporteur at 15: 9.

[72] As explained above as an argument by the Council of State 2014.

[73] Article 6 Decision on SyRI.

[74] Brief by the United Nation Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550,982/HA ZA 18/388): 9.

[75] Ibid., pleading note, section 6.1. Plaintiffs refer to the case of S. AND MARPER v. THE UNITED KINGDOM, ECHR 4 December 2008, no. 30562/04 and 30,566/04. See also Jak and Bastiaans 2018 arguing that automated decision-making should be based preferably on specific legal bases.

that refers back to the principle of transparency.[76] In this respect it is also problematic that SyRI does not operate reactively, but proactively.[77] This means that citizens are not investigated based on suspicious individual situation or actions. Rather, they are investigated because they are part of a specific group or category of citizens, for instance because they live in a certain neighbourhood. This means that SyRI goes beyond the scope targeted search, yet represents a way of reasoning based on statistics, including the falls positive and negative conclusions that are part of any exercise based on statistics.[78]

24.4 The Right to a Fair Trial

The transparency that feeds the right to a fair trial might be difficult to realise when algorithms are involved in decision-making. Algorithms are described as '…. non-transparent, non-neutral, human constructs', which are designed, programmed, trained and used by human beings.[79] They might thus include the same flaws in reasoning and decision-making as humans. Also, the data that are put into the algorithm might have biases or flaws whereas also the users of algorithms might be non-neutral in their judgement or misinterpret the outcome.[80] It seems therefore of eminent importance that the algorithm and its functioning can be assessed in order to find out possible flaws or biases. Here, also the societal and political context is relevant, in which automatic decision-making systems are designed and the purpose for which they are used. Referring to social security, the UN finds that the balance between fair eligibility standards and strict control is easily tipped towards detecting and preventing benefit fraud. Within this context of fighting fraud SyRI was designed and implemented. The UN qualifies this as a part of a partisan political trend.[81] It refers to article 9 of ICESCR, requiring that qualifying conditions to welfare benefits should be "reasonable, proportionate and transparent". The withdrawal from such rights as well the reduction or suspension of benefits should be 'circumscribed, based on grounds that are reasonable, subject to due process, and provided for in national law'.[82] Here, thus, the lack of clarity of SyRI (see above), giving citizens at best a very general idea about its functioning, may mean that SyRI lacks the necessary

[76] See also Brief by the United Nation Special Rapporteur at 15.

[77] Pleitnotities NJCM c.s. Solv. and Ekker, for Court hearing of 29 October 2019, Case number C/09/550,982/HA ZA 18/388, section 4.7.

[78] Ibid., section 4.7. See also Zwenne et al. 2016.

[79] Gerards 2019, p. 205.

[80] Gerards 2019.

[81] Kamerstukken II, 2012–2013, 33,579; The letter of the United Nations Special Rapporteur, p. 7. This refers also to Article 22 of the UDHR 1948 and Article 25 on the right to an adequate standard of living; Article 9 of the 1966 International Covenant on Economic, Social and Cultural Rights (ICESCR).

[82] Ibid., p. 7.

fundamental and procedural safeguards.[83] As the operation of SyRI may include deciding on social security entitlements, the UN rapporteur also links the case of SyRI to the right to social security.[84]

The plaintiffs refer to Articles 6 and 13 ECHR[85] on the right to a fair trial and the right to an effective remedy. They argue that the European Court of Human Rights gives a wide interpretation, letting Article 6 ECHR cover issues concerning social security and welfare benefits. The plaintiffs point out that SyRI lacks an equality of arms. Due to a lack of transparency, citizens cannot know the risk model or algorithm used and therefore cannot defend themselves against decisions based on SyRI. The government, on the other hand, knows the risk model and has chosen to keep this a secret. The government argues that the secrecy is needed, as otherwise (potential) violators would be able to circumvent the system. After all, violators would know which indicators to dodge.[86] For instance, in a pre-SyRI scheme called 'Waterproof' the government reasoned that a low use of water could point at welfare fraud, as someone could secretly live somewhere else, while collecting welfare on their address. If people would know that water use is a risk indicator for fraud, they could turn the tap water on from time to time and thus void becoming a suspect.[87] However, keeping grounds of decision-making secret, goes against relevant principles, including the rule of law which requires that laws are made public. Moreover, all parties in a court proceeding should have equal access to information.[88] Counter questions include whether a risk model is the same as a law, or whether it is merely an internal procedure. Here also, the UN argues that these risk models potentially determine who is keeping and who is losing his or her right to social security and is therefore of public concern.

24.5 Court Ruling: SyRI Violates Human Rights

On 5 February 2020, the District Court of The Hague has ruled on the SyRI case, concluding that SyRI violates human rights.[89] To the UN it is a landmark ruling that may have large relevance to practices in other digital welfare states.[90] The court particularly refers to Article 8 ECHR on the respect for private life, and pays special

[83] Ibid., p.8.

[84] Brief by United Nations Special Rapporteur. Refers to Article 22 of the UDHR 1948 and Article 25 on the right to an adequate standard of living; Article 9 of the 1966 International Covenant on Economic, Social and Cultural Rights (ICESCR).

[85] As well as Article 47 of the Charter, on Right to an effective remedy and to a fair trial.

[86] See also Brief by the United Nation Special Rapporteur at 15.

[87] See also Brief by the United Nation Special Rapporteur at 15.

[88] Gerards 2019.

[89] Court The Hague, SyRI-wetgeving in strijd met het Europees Verdrag voor de Rechten voor de Mens, Press release, 5 February 2020. See court ruling number ECLI:NL:RBDHA:2020:865.

[90] UN 'Landmark ruling by Dutch court stops government attempts to spy on the poor – UN expert', Press release, 5 February 2020.

attention to Article 8(2) on a fair balance between societal relevance and the limitation of the right on the respect of private life. It finds that the state has a special responsibility to safeguard this fair balance when using new technologies. It rules that SyRI, in its present form, does not meet the requirements of Article 8(2) ECHR. The court finds that SyRI lacks transparency about its functioning. This lack of information could result in unfair judgements on the basis of socio-economic or migrant status. Moreover, the court is concerned about the effect of risk indications ("flagging") on the privacy of affected individuals.

The District Court has explained its ruling in 36 pages, thus paying ample attention to the details of the case and the arguments. The court finds that the government may use new technologies in order to fight fraud. Thus, the SyRI legislation has a legitimate aim to safeguard the economic wellbeing of the society.[91] However, equally, new technologies spark questions on the right to the protection of personal data. The court finds that adequate protection of privacy, also in case of data sharing between public administrations, contributes to the trust people have in their governments.[92] Thus, both fighting fraud and privacy protection contribute to trust. The court agrees with the plaintiffs that inadequate and untransparent protection of the right on the respect of private life, could lead to a chilling effect, making citizens less willing to share their data with the government. Therefore, on grounds of Article 8 ECHR, the government has a special responsibility to respect private life when using new technologies and come to a fair balance. Based on the law, every citizen should have a reasonable expectation that the use of SyRI sufficiently respects private life. The court finds that the SyRI legislation does not meet this requirement.[93]

In addition, SyRI legislation does not meet the requirements of Article 8(2) ECHR requiring that limiting the right to respect private life should be necessary, meaning that it is proportionate and related to the purpose of the data processing. The court refers to the EU's data protection regulations (GDPR and Charter) to spell out more clearly which shortcoming SyRI has, thus harming a fair balance. In particular, the court uses the principles of transparency, purpose limitation and data minimisation.[94] It rules that the implementation of SyRI is insufficiently transparent and cannot be checked. Therefore, it judges that Articles 65 and 64 SUWI, which constitute SyRI, as well as chapter 5a of the decision on SyRI, violate Article 8(2) ECHR and declares these Acts to be non-binding.

Some specific details of the ruling are worth mentioning a bit more in-depth. The court paid much attention to establishing the extent to which SyRI limits the right on the respect of private life, in order to assess this limitation in the light of Article 8(2) ECHR. The court is bound by limited information, as the state did not provide details on the operation of SyRI. It therefore cannot verify whether SyRI merely compares data bases, using a simple decision-making tree.[95] The law does

[91] Ruling District Court The Hague ECLI:NL:RBDHA:2020:865, section 6.4.
[92] Ruling District Court The Hague ECLI:NL:RBDHA:2020:865, section 6.5.
[93] Ruling District Court The Hague ECLI:NL:RBDHA:2020:865, section 6.6.
[94] Ruling District Court The Hague ECLI:NL:RBDHA:2020:865, section 6.7.
[95] Ruling District Court The Hague ECLI:NL:RBDHA:2020:865, section 6.49.

not provide information on this either, yet, leaves options open to move towards decision-making with feedback and learning effects. The law gives, however, a list of categories of data which may be fed into SyRI. The court judges this list is limited (and not unlimited as the plaintiffs argued), however also finds that the seventeen categories listed by SyRI are broad, each category covering a wide range of issues and possible data.[96] Moreover, the court notes that the SyRI legislation lacks an obligation to provide information to citizens whose data is processed. Another relevant question to assess the degree of limitation to the right on the respect of private life, is whether a risk assessment or "flagging" imposes private life. An additional question is whether SyRI does this by using profiling or automated decision-making. The court judges that SyRI does not intend to generate legal effects. However, a risk alert does have an effect on the private life of people getting such a risk alert. In this respect the court refers to the guidelines of the Article 29 Data Protection Working Party.[97] This view takes into account that the risk alert is stored for two years, whereas also the police and the public prosecutor may request access to the list of risk alerts. Moreover, the court does not find it relevant to know whether decision-making is automatic in order to assess Article 8 ECHR.[98] The fact that a risk alert affects someone's private life suffices. It weighs that citizens are entitled to information about the processing of their data and should be allowed to track the processing of their data in a reasonable way.

In its judgement, the court does not go into the question whether the SyRI-legislation is sufficiently accessible and foreseeable.[99] However, it finds that SyRI fails to convince of its necessity in a democratic society. Therefore, SyRI does not meet the requirements of Article 8 (2) ECHR. Both parties in the court hearing agree that the purpose of fraud detection is a legitimate aim. The disagreement is on whether there is a 'pressing social need' to use the method of SyRI. Here, the court underlines again that fighting fraud is a legitimate goal. Also, it does not see SyRI as an ineffective or an a priori not proportionate instrument to reach its goal.[100] The court also finds the choice of the legislator sufficient to create a legal basis in Article 64 Act SUWI as well as the choice to process data using an instrument such as SyRI, in the light of Article 8(2) ECHR. However, the court argues, this does not mean that the instrument that has been chosen, being SyRI, and the related procedures and legal safeguards sufficiently acknowledges the right on the respect of private life.[101] Given that a large quantity of data may be processed; using indicators and a risk model that are not public and therefore unknown to those whose data is processed;

[96] Ruling District Court The Hague ECLI:NL:RBDHA:2020:865, section 6.50.

[97] Ruling District Court The Hague ECLI:NL:RBDHA:2020:865, section 6.59; Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

[98] Ruling District Court The Hague ECLI:NL:RBDHA:2020:865, section 6.60.

[99] Referring to S. AND MARPER v. THE UNITED KINGDOM, ECHR 4 December 2008, no. 30562/04 and 30,566/04; Ruling District Court The Hague ECLI:NL:RBDHA:2020:865, section 6.72.

[100] Ruling District Court The Hague ECLI:NL:RBDHA:2020:865, section 6.77.

[101] Ruling District Court The Hague ECLI:NL:RBDHA:2020:865, section 6.79.

the space the law gives to adjust the risk model based on the feedback of results; as well as the fact that citizens are unaware of having a risk alert, whereas this has a significant impact on their private lives, the court rules that SyRI does not meet the requirement of a fair balance.

24.6 Outlook on Fundamental Rights in Digital Welfare States

The UN Special Rapporteur not only applauded the judgment onSyRI because it is a first time that a court has stopped the use of digital technologies and abundant information by welfare authorities, on grounds of human rights.[102] He finds it also a key ruling because it sets a strong legal precedent for other courts to follow. It moreover encourage activists elsewhere to file similar legal challenges to address the risks of digital welfare states which have been emerging everywhere in the world.[103] Potentially negative and devastating consequences of the use of new technologies are not always taken into account, especially from the perspective of human rights of the poorest and most marginalized.[104] The threat of having negative effects on society, including distrust and chilling effects, seems largest if automated decision-making is developed in a socio-political context driven by negative associations, such as fraud fighting. This even leads to questions on the right to social security and equal treatment if fraud detection activities are driven by the conviction that certain areas or persons should be surveilled more deeply than others. This underlines the relevance of transparency for citizens whose data is processed. Bertelsmann Stiftung and Algorithm Watch therefore advocate for empowering citizens and NGOs so that they can learn to adapt to new challenges and address the consequences of automated decision-making. Yet, they also argue to empower public administrations so that they can build sufficient expertise to oversee the operation of automated decision-making and its societal impact. The UN points out that, within alternative political and societal context, digital tools and big data could also be used to help people who experience poverty and to safeguard human rights.[105] Lastly, an inspiring question is whether there is a need to develop a collective and political approach to the protection of privacy.[106] Even if individuals have access to information on automate decision-making and the processing of their data, it could be quite complex for individuals to read into this and keep track of all data processing initiatives by the government. Therefore, several authors suggest to create better collective facilities, including

[102] UN 'Landmark ruling by Dutch court stops government attempts to spy on the poor—UN expert', Press release, 5 February 2020.

[103] Blauw 2020.

[104] Ibid., at 1.

[105] Ibid., at 1.

[106] Allen 2016.

adequate oversight bodies,[107] or data attorneys who have access to and insight in algorithms.[108]

Acknowledgements I would like to acknowledge the inspiring input of Arjen Kamphuis, teacher in data protection. His introduction into the GDPR was excellent. He never ceased to address the wider context and implications of privacy, underlining the importance of privacy to safeguard human rights, freedom and democracy.

References

Allen AL (2016) Protecting one's own privacy in a big data economy. Harvard Law Review 130:F.71.
Allen AL (2019) Imagine an unimaginable future, Speech for Dies Natalis, given at Tilburg University, 5 December 2019. https://www.tilburguniversity.edu/sites/tiu/files/download/Speech%20Anita%20Allen.pdf Last accessed 14 January 2020.
Bekker S (2020) Towards an inclusive labour market: ambitions of the Dutch Public Employment Service. Peer Review paper on "Employer service delivery". Amsterdam, 26–27 March 2020.
Blauw S (2020) An algorithm was taken to court – and it lost (which is great news for the welfare state). The Correspondent 10 February 2020.
Broeders D, Schrijvers E, Hirsch Ballin E (2017) Big Data and Security Policies: Serving Security, Protecting Freedom. WRR-Policy Brief 6. WRR, The Hague.
Gantchev V (2019) Data protection in the age of welfare conditionality: Respect for basic human rights or race to the bottom? European Journal of Social Security, 21(1):3-22.
Gerards J (2019) The fundamental rights challenges of algorithms. Netherlands Quarterly of Human Rights 37(3):205–209.
Jak N, Bastiaans S (2018) De betekenis van de AVG voor geautomatiseerde besluitvorming door de overheid. Een black box voor een black box? NJB 40:3018–3024.
Kool L, Timmer J, van Est R (2015) De datagedreven samenleving. Achtergrondstudie, Rathenau Instituut, The Hague.
Mantelero A (2018) AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. Computer Law & Security Review 34(4):754–772.
Olsthoorn P (2016) Big Data voor fraudebestrijding. Working Paper nr. 21. WRR, The Hague.
Van der Sloot B, Van Schendel S (2019) De modernisering van het Nederlands procesrecht in het licht van big data. Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving. TILT/WODC, Tilburg.
Vetzo M, Gerards J, Nehmelman R (2018) Algoritmes en grondrechten, Boom Juridisch, The Hague.
Wolfswinkel CJ (2020) Willekeur of algoritme? Laveren tussen analoog en digitaal bestuursrecht. Oratie Tilburg University.
Yeung K, Lodge M (2019) Algorithmic Regulation. Oxford University Press, Oxford.
Zwenne GJ, Steenbruggen W, Reker M (2016) Rechtsbescherming bij het gebruik van big data door toezichthouders: een verkenning. Tijdschrift voor Toezicht (7)4:29–44.

[107] Bertelsmann Stiftung and Algorithm Watch 2019:9; Wolfswinkel 2020.

[108] Van der Sloot and Van Schendel 2019.