UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

# Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands

Appelman, N.; Ó Fathaigh, R.; van Hoboken, J.

**Publication date**
2021
**Document Version**
Final published version
**Published in**
Journal of Intellectual Property, Information Technology and Electronic Commerce Law
**License**
Other

Link to publication

**Citation for published version (APA):**
Appelman, N., Ó Fathaigh, R., & van Hoboken, J. (2021). Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, *12*(4), 257-271. https://www.jipitec.eu/issues/jipitec-12-4-2021/5407

**General rights**
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

**Disclaimer/Complaints regulations**
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

*UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)*

Download date:14 Sept 2026

# Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands

by **Naomi Appelman, Ronan Ó Fathaigh and Joris van Hoboken***

**Abstract:** This article discusses the use of automated decisioning-making (ADM) systems by public administrative bodies, particularly systems designed to combat social-welfare fraud, from a European fundamental rights law perspective. The article begins by outlining the emerging fundamental rights issues in relation to ADM systems used by public administrative bodies. Building upon this, the article critically analyses a recent landmark judgment from the Netherlands and uses this as a case study for discussion of the application of fundamental rights law to ADM systems by public authorities more generally. In the so-called SyRI judgment, the District Court of The Hague held that a controversial automated welfare-fraud detection system (SyRI), which allows the linking and analysing of data from an array of government agencies to generate fraud-risk reports on people, violated the right to private life, guaranteed under Article 8 of the European Convention on Human Rights (ECHR). The Court held that SyRI was insufficiently transparent, and contained insufficient safeguards, to protect the right to privacy, in violation of Article 8 ECHR. This was one of the first times an ADM system being used by welfare authorities has been halted on the basis of Article 8 ECHR. The article critically analyses the SyRI judgment from a fundamental rights perspective, including by examining how the Court brought principles contained in the General Data Protection Regulation within the rubric of Article 8 ECHR as well as the importance the Court attaches to the principle of transparency under Article 8 ECHR. Finally, the article discusses how the Dutch government responded to the judgment. and discusses proposed new legislation, which is arguably more invasive, with the article concluding with some lessons that can be drawn for the broader policy and legal debate on ADM systems used by public authorities.

Keywords: Automated decision-making; Fundamental rights; Social welfare ; Risk profiling; Digital administrative state

© 2021 Naomi Appelman, Ronan Ó Fathaigh and Joris van Hoboken

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8.

Recommended citation: Naomi Appelman, Ronan Ó Fathaigh, and Joris van Hoboken, Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands, 12 (2021) JIPITEC 257 para 1.

## A. Introduction

1 In October 2019, the UN Special Rapporteur on extreme poverty and human rights warned about the dangers of the digital transformation of the State, where digital technologies are being used to "automate, predict, identify, surveil, detect, target and punish" individuals.[1] Indeed, the UN Special Rapporteur on the right to privacy has recommended that because more and more decisions affecting the daily lives of individuals are being automated, "their impact on human rights needs to be carefully and continuously evaluated".[2] For the public and pri-

* Naomi Appelman, PhD Researcher, Institute for Information Law (IViR), Faculty of Law, University of Amsterdam; Dr. Ronan Ó Fathaigh, Senior Researcher, Institute for Information Law (IViR), Faculty of Law, University of Amsterdam; and Prof. Dr. Joris van Hoboken, Professor of Law, Chair "Fundamental Rights and Digital Transformation," Vrije Universiteit Brussel (VUB), and Associate Professor, Institute for Information Law (IViR), Faculty of Law, University of Amsterdam (the Chair at VUB is established at the Interdisciplinary Research Group on Law Science Technology & Society, with the support of Microsoft).

1 Report of the Special Rapporteur on extreme poverty and human rights, UN Doc A/74/493 (11 October 2019), para 3.

2 Report of the Special Rapporteur on the right to privacy, UN Doc A/73/438 (17 October 2018), para 41.

vate sector, the digital transformation involves the processing of "vast quantities" of data from numerous sources, and using "predictive analytics to foresee risk, automate decision-making and remove discretion from human decision makers".[3] This digital transformation has only accelerated during the Covid-19 pandemic. Indeed, in the summer of 2020, five UN Special Rapporteurs, including the UN Special Rapporteur on the right to privacy, expressed their deep concern over "patterns of abuse" that had emerged through States leveraging digital technologies during the pandemic, and called for greater scrutiny of the gap between State commitments to fundamental rights and "actual practices".[4]

**2** A recent landmark judgment from the Netherlands creates an opportunity to scrutinise in detail the use of ADM systems by administrative authorities, and its impact on fundamental rights. In the SyRI case,[5] the District Court of The Hague considered a controversial automated welfare-fraud detection system called *Systeem Risico Indicatie* (SyRI), which allows the linking and analysing of data from an array of government agencies to generate fraud-risk reports on people. These risk reports result in individuals being subject to investigation by authorities for possible fraud.[6] The system was criticised for its lack of transparency, the fact it was "used exclusively in areas with a high proportion of low-income residents, migrants and ethnic minorities", had "hugely negative impact on the rights of poor individuals without according them due process", and as such, was labelled as an implementation of a "surveillance state for the poor".[7] In its judgment, The Hague Court held that the legislation underpinning SyRI violated the right to private life, guaranteed under Article 8 of the European Convention on Human Rights (ECHR).[8]

**3** The purpose of this article is to analyse the use of machine-learning algorithms and ADM systems by public administrative bodies, particularly systems to combat social-welfare fraud. We analyse such use from a fundamental rights perspective, using the landmark SyRI judgment in the Netherlands as a case study. First, (Section B) the article outlines the emerging fundamental rights issues in relation to the use of ADM systems by the administrative state and discusses the legal and standard-setting instruments at European level in relation to ADM systems and fundamental rights, under both the Council of Europe (COE) and European Union (EU) legal frameworks. Next, (Section C) the article discusses the SyRI judgment and focuses in particular on (I.) how The Hague Court brought principles contained in the EU's General Data Protection Regulation within the rubric of Article 8 ECHR; (II.) the importance the Court attaches to the principle of transparency; and (III.) the finding that the legislation lacked sufficient safeguards, in violation of Article 8(2) ECHR. Finally (IV.), the article critically analyses how the Dutch government responded to the judgment, with further legislation which is arguably more draconian than the SyRI legislation. We conclude with some lessons that can be drawn for the broader policy and legal debates on the digital transformation in Europe.

## B. The Digital Transformation and Fundamental Rights

**4** This article is focused on the digital transformation of the administrative state, involving the use of machine-learning algorithms and ADM systems by public administrative bodies, for decisions by a range of authorities, such as in the area of welfare, health, education and taxation.[9] As UN Special Rapporteur on extreme poverty and human rights Philip Alston describes, the digital transformation involves "processing of vast quantities of digital data" from many sources, and use "predictive analytics to foresee risk, automate decision-making".[10] In addition to this technological dimension, Alston notes how it tends to "remove discretion from human decision makers".[11] Notably, Coglianese and Lehr highlighted in 2017 that the use of machine-learning algorithms and ADM systems by public administrative bodies

3 UN Doc A/74/493 (n 1) para 3.

4 UN Office of the High Commissioner, 'UN experts warn of closing digital space amid COVID-19 pandemic' (30 July 2020) <www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26139&LangID=E>.

5 Rb Den Haag 5 February 2020, ECLI:NL:RBDHA:2020:1878 (hereinafter: *SyRI*).

6 ibid para 3.2

7 Special Rapporteur on extreme poverty and human rights, 'The Netherlands is building a surveillance state for the poor, says UN rights expert' (16 October 2019) <www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25152&LangID=E>.

8 Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS No 5.

9 For an overview of ADM systems being used in public administration in Europe, see Fabio Chiusi, Sarah Fischer, Nicolas Kayser-Bril, and Matthias Spielkamp (eds), *Automating Society Report 2020* ( AlgorithmWatch and Bertelsmann Stiftung 2020) <https://automatingsociety.algorithmwatch.org/>.

10 UN Doc A/74/493 (n 1) para 3.

11 ibid.

has "escaped sustained analysis".[12] Similarly, Alston has stated that the use of ADM systems in public administrative contexts, for example in relation to the welfare state, has "garnered remarkably little attention".[13] However, scholars have been recently examining the use of ADM systems by public administrative bodies from a number of important perspectives, such as the influential work by Eubanks, who has examined the impact of ADM systems by public authorities on those living in poverty.[14] In Europe, Choroszewicz & Mäihäniemi have approached the use of ADM systems by public authorities from a sociolegal perspective, and examined specific national legislation in EU member states on ADM in the public sector.[15] In this regard, Ranchordás has argued how digitisation of the administrate state can lead to digital exclusion in Europe.[16]

Further, Ranchordás and Schuurmans have highlighted the influential role of private actors in automated welfare-fraud systems.[17]

**5** We build upon this work and approach the question of the ADM systems operated by public administration specifically from a European fundamental rights perspective, in order to understand the fundamental rights frameworks that exist at European level for ensuring that ADM systems operated by national governments do not violate fundamental rights. This is because ADM systems can impact upon an array of rights and freedoms guaranteed under European fundamental rights law, including the right to a fair trial and due process, the rights to private life, freedom of expression, freedom of assembly, the right to an effective remedy, and the prohibition of discrimination. Indeed, we focus on the SyRI judgment as a case study in order to demonstrate the distinct issues and difficulties that national courts may encounter in applying European fundamental rights law to ADM systems operated by administrative bodies.

**6** We also build on the law and technology scholarship that has focused on the discriminatory impact of algorithms, the surveillance state, the use of algorithms by large platforms and the emerging regime of surveillance capitalism.[18] Finally, we take into account recent research by civil society organisations, such as the Berlin-based AlgorithmWatch, has started to shine a light on the widespread use of ADM systems by governments in Europe.[19] In its 2020 report on ADM systems in Europe, AlgorithmWatch warned that the "vast majority of uses tend to put people at risk rather than help them", including risks of discrimination and disproportionate interferences with privacy.[20]

## C. The applicable European fundamental rights framework

**7** In order to begin our analysis, the first question that must be posed is what legal frameworks exist at European level for ensuring that ADM systems operated by national governments do not violate fundamental rights? In this regard, national gov-

12 Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 *Georgetown Law Journal* 1147, 1152. See also Lorna McGregor, Daragh Murray and Vivian Ng, 'International Human Rights Law as a Framework for Algorithmic Accountability' (2019) 68(2) *International & Comparative Law Quarterly* 309.

13 UN Doc A/74/493 (n 1) para 3. For scholarship on the impact of ADM systems on individuals in poverty, see, for example, Virginia Eubanks, *Automating Inequality: How high-tech tools profile, police, and punish the poor* (St Martin's Press 2018); and Virginia Eubanks, 'Algorithms Designed to Fight Poverty Can Actually Make It Worse' (2018) 319 *Scientific American* 68.

14 Virginia Eubanks, *Automating Inequality: How high-tech tools profile, police, and punish the poor* (St Martin's Press 2018); and Virginia Eubanks, 'Algorithms Designed to Fight Poverty Can Actually Make It Worse' (2018) 319 *Scientific American* 68.

15 Marta Choroszewicz and Beata Mäihäniemi, 'Developing a Digital Welfare State: Data Protection and the Use of Automated Decision-Making in the Public Sector across Six EU' (2020) 1(1) *Global Perspectives* 12910.

16 Sofia Ranchordás, 'The Digitalization of Government and Digital Exclusion: Setting the Scene' forthcoming in G Ferreira Mendes & C Blanco de Morais (eds.) *Direito Publico e Internet: Democracia, Redes Sociais e Regulação do Ciberespaço* (FGV /IDP/ Univ. Lisboa, 2020) <http://dx.doi.org/10.2139/ssrn.3663051>. See also Sofia Ranchordás, 'Automation of Public Services and Digital Exclusion' (*I-CONnect: Blog of the International Journal of Constitutional Law*, 11 March 2020) <www.iconnectblog.com/2020/03/automation-of-public-services-and-digital-exclusion/>; Sofia Ranchordás, 'Public Law and Technology: Automating Welfare, Outsourcing the State' (*I-CONnect: Blog of the International Journal of Constitutional Law*, 15 January 2020).

17 Sofia Ranchordás and Ymre Schuurmans, 'Outsourcing the Welfare State: The Role of Private Actors in Welfare Fraud Investigations' (2020) 7(1) *European Journal of Comparative Law and Governance* 5.

18 UN Doc A/74/493 (n 1) para 3.

19 See Chiusi, Fischer, Kayser-Bril and Spielkamp (n 9).

20 ibid 7.

ernments have binding legal obligations pursuant to both membership of the COE and the EU. Beginning with the COE, its Committee of Ministers has been quite explicit in emphasising the basic principle that its member states have a legal obligation under the ECHR to ensure that the use of algorithmic systems by public authorities does not violate the ECHR rights of individuals within their jurisdiction, such as the right to private life under Article 8 and right to a fair trial and due process under Article 6.[21] As Wagner et al. have examined, ADM systems can impact upon an array of rights and freedoms guaranteed under the ECHR, including the right to a fair trial and due process, the right to private life, freedom of expression, freedom of assembly, the right to an effective remedy, and the prohibition of discrimination.[22] Thus, any national legislation relating to the use of ADM systems, national court judgments interpreting such legislation, and decisions of administrative authorities, must be consistent with the rights guaranteed under the ECHR.

**8** The European Court of Human Rights (ECtHR) is tasked with interpreting the ECHR, and while the ECtHR has not yet considered an ADM system operated by a public authority, it has delivered numerous judgments on the use of automated systems and data collection systems used for government surveillance. For example, the ECtHR has held that an electronic-surveillance system in operation in Hungary violated the right to respect for private life under Article 8 ECHR. Crucially, the ECtHR emphasised that surveillance systems using "automated and systemic data collection" had "reached a level of sophistication which is hardly conceivable for the average citizen".[23] Indeed, the Court warned about the capacity of governments to acquire "detailed profile[s] of the most intimate aspects of citizens' lives", which may result in "particularly invasive" interferences with the right to private life.[24] Similarly, the ECtHR has found a violation of Article 8 over a system in the United Kingdom allowing storing of a person's photograph in a police database, where the police could apply facial recognition and facial mapping techniques to the image.[25] The Court emphasised the essential importance of Article 8 to guard against the "risk of arbitrariness" which flows from vesting "obscure" powers with the State, and "especially where the technology available is continually becoming more sophisticated".[26]

**9** Article 8 (1) ECHR guarantees the right to respect for private life, and Article 8 (2) ECHR allows interferences with the right to private life only under certain conditions. For an interference with private life to be consistent with Article 8 ECHR, it must be "in accordance with law", "pursue a legitimate aim", and "necessary in a democratic society".[27] Crucially, for an interference to be in accordance with law, it is simply not enough, for example, for a system of surveillance to be set out in legislation. This test also encompasses whether there are sufficient safeguards to protect against "arbitrary interference by public authorities."[28] Indeed, the Court has found national legislation in specific cases to be deficient in this regard, such as legislation on surveillance failing to have appropriate safeguards to protect specific groups of individuals, such as journalists, from government surveillance.[29]

**10** Notably, the COE's Committee of Ministers adopted an important Recommendation in 2020 on the human rights impacts of algorithmic systems, given the current "digital transformation" European societies are undergoing.[30] This is important, as the ECtHR can rely upon recommendations from the Committee of Ministers to provide "guidance as to the approach

21 Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (8 April 2020), preamble.

22 Ben Wagner et al, *Algorithms and Human Rights: Study on the human rights dimensions of automated data processing techniques and possible regulatory implications* (Council of Europe 2017) 10.

23 *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016) para 68.

24 ibid para 70.

25 *Gaughran v UK* App no 45245/15 (ECtHR, 13 February 2020) para 70.

26 ibid para 86.

27 See, for example, *Telegraaf Media Nederland Landelijke Media BV and Others v the Netherlands* App no 39315/06 (ECtHR, 22 November 2012) para 89.

28 ibid para 90.

29 ibid para 102. Van der Sloot has even argued that the ECtHR has transformed into a "European Constitutional Court" with its recent case law on government surveillance, by "formally assesses the quality of Member States' laws and even advises Member States' legislative branch on how to amend its legal system in order to be Convention-compliance" (see Bart van der Sloot, 'The Quality of Law: How the European Court of Human Rights gradually became a European Constitutional Court for privacy cases' (2020) JIPITEC 160, 177. See also, Eleni Kosta, 'Algorithmic state surveillance: Challenging the notion of agency in human rights' (2020) *Regulation & Governance* <https://doi.org/10.1111/rego.12331>).

30 Recommendation CM/Rec(2020)1 (n 15).

which should be taken to interpreting" ECHR rights, and has applied these recommendations in its case law.[31] Notably, the Recommendation singles out the use of algorithmic systems by States for their public services, warning that such algorithmic systems can prompt a "particular, higher risk to human rights", because an individual may "not have a possibility to opt out," where its use is prescribed by law, or when she/he "suffers negative consequences as a result of the decision to opt out".[32]

**11** The Recommendation defines "high risk" as including the use of algorithmic systems in situations where the lack of alternatives "prompts a particularly high probability of infringement of human rights, including by introducing or amplifying distributive injustice".[33] This is the case where the ADM system produces "serious consequences for individuals", such as legal consequences, or for predictive or individual risk assessment by public authorities.[34] Thus, the Committee of Ministers is acutely aware of the possibility of violations of ECHR rights through ADM systems used in public services, and how such systems can perpetuate existing inequalities. This view echoes the observation from the UN Special Rapporteur on extreme poverty that the use of algorithmic systems for risk calculation and need classification by welfare authorities can "reinforce or exacerbate existing inequalities and discrimination".[35] This is because such ADM systems may be used to target poor and marginalised individuals already subject to discrimination and most likely to be in need of state aid. Indeed, as discussed below, the SyRI system deployed in the Netherlands exclusively targeted so-called "problem" neighbourhoods, with the Court recognising that the system could "inadvertently" be based on bias, such as a lower socio-economic status or an immigration background.[36]

**12** The final COE instrument to be mentioned is the COE's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[37] In 2018, new Protocol was adopted amending the Convention, which inserts a new Article 9(1)(a), and guarantees a right for every individual not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration.[38] However, there is an exception under Article 9(2), that the right shall not apply if the decision is authorised by a law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests. Thus, any national legislation permitting the use of ADM systems by public administrative authorities which does not allow an individual to exercise their right under Article 9(1)(a) would need to include measure to safeguard an individual's data rights.

**13** In addition to the COE framework, the EU legal framework is particularly important.[39] The EU Charter of Fundamental Rights guarantees many of the rights contained in the ECHR, including the right to a fair trial, respect for private life, freedom of expression and freedom of assembly; in addition to rights not specifically enumerated in the ECHR, such as the right to the protection of personal data.[40] Further, the most significant secondary EU legislation on ADM systems is the GDPR,[41] which applies to the

31 See, for example, *Manole and Others v Moldova* App no 13936/02 (ECtHR, 17 September 2009) para 101 and 102.

32 Recommendation CM/Rec(2020)1 (n 15) s A(11) (Appendix). It should also be recongised that it can be similarly difficult to opt out of ADM-type systems operated by the private sector, and even where there are mechanisms to opt out, these mechanisms may not operate fully as stipulated (see, e.g., Paresh Dave, 'Google faces lawsuit over tracking in apps even when users opted out' *Reuters* (14 July 2020) <www.reuters.com/article/us-alphabet-google-privacy-lawsuit-idUSKCN24F2N4>.

33 ibid.

34 ibid.

35 UN Doc A/74/493 (n 1) para 28.

36 *SyRi* (n 5) para 6.93.

37 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, ETS No 108. See Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Guidelines on Artificial Intelligence and Data Protection*, T-PD(2019)01 (25 January 2019).

38 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10 October 2018, CETS No 223, art 9(1).

39 See also High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI* (European Commission 2019).

40 Charter of Fundamental Rights of the European Union [2012] OJ C326/391. See also Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/1.

41 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

processing of personal data wholly or partly by automated means.[42]

**14** Crucially, Article 22(1) GDPR provides (subject to exceptions in Article 22(2) GDPR) that data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.[43] Profiling is defined as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[44] However, Article 22(2) GDPR contains important exceptions to the prohibition on ADM and profiling, including when it is authorised by national law which "lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests".[45] These measures include the right to obtain human intervention, and to express one's point of view and to contest the decision.[46] In relation to ADM systems used by public authorities, it is important to note that Recital 71 of the GDPR expressly recognises that ADM and profiling "should be allowed", where it is authorised by national law, including for "fraud and tax-evasion monitoring and prevention purposes".[47] Thus, the drafters of the GDPR clearly envisaged that ADM, and specifically, profiling, by public authorities should not be in principle interfered with, especially where it is deployed in the fight against fraud.

**15** In 2021, the European Parliament adopted a Resolution on artificial intelligence, including AI systems in the decision-making process of public authorities.[48] The Resolution warns of many risks associated with ADM systems specially used by public authorities. Significantly, the Parliament called on the European Commission, and the European Data Protection Board, to issue guidelines and recommendations on the criteria and conditions applicable to decisions based on profiling and the use of AI by public authorities.[49] First, the Resolution stressed that AI systems in the decision-making process of public authorities can result in "biased decisions that negatively affect citizens".[50] As such, the Parliament recommended that such ADM systems should be subject to "strict" control criteria in terms of security, transparency, accountability, non-discrimination, and social responsibility.[51] Indeed, EU member states were urged to assess the risks related to AI-driven decisions by public authorities "before" automating activities connected with the exercise of state authority.[52] Further, the Resolution recommends that there should be safeguards, including meaningful human supervision, transparency and the possibility to contest a decision.[53] Finally, the Parliament called for the explainability of algorithms, transparency and regulatory oversight when AI is used by public authorities, and for impact assessments to be conducted before tools using AI technologies are deployed by state authorities.[54]

**16** In terms of the risk of ADM systems used by public authorities, the UN Special Rapporteur on poverty points out that seemingly neutral terms such as the "digital transformation" should not conceal the "politically driven character" of ADM systems.[55] These systems are promoted as improving "efficiency" and "rooting out fraud".[56] However, the Rapporteur argues that digital technologies are presented as neutral and scientific, but may in fact facilitate, justify and shield "values and assumptions that are far removed from, and may be antithetical to, the prin-

42 ibid art 2(1).

43 ibid art 22(1).

44 ibid art 4(4).

45 ibid art 22(2)(b).

46 ibid art 22(3). There has been considerable debate over these provisions: see, for example, Andrew Selbst and Julia Powles, 'Meaningful information and the right to explanation' (2017) 7 *International Data Privacy Law* 233; and Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" is Probably Not the Remedy You Are Looking For' (2017) 16 *Duke Law & Technology Review* 18.

47 ibid recital 71.

48 European Parliament resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice, P9_TA-PROV(2021)0009.

49 ibid para 62.

50 ibid para 52.

51 ibid.

52 ibid para 71.

53 ibid para 52.

54 ibid para 62.

55 UN Doc A/74/493 (n 1) para 6.

56 ibid.

ciples of human rights".[57] As such, diverging views around the risk and benefits of ADM systems used by public authorities may go some way to explaining how national courts struggle to apply COE and EU legal frameworks when considering the compatibility of these systems with European fundamental rights law. As the following section demonstrates, The Hague Court did indeed struggle on how to apply such frameworks.

## D. The SyRI Judgment

**17** Before delving into different aspects of the SyRI Judgment relevant for understanding the impact of fundamental rights law on the use of ADM systems by public authorities, this section will outline the facts of the case, focussing on how the SyRI system operates. The case was initiated by a coalition of civil society organisations who brought legal proceeding against the Dutch Government in The Hague District Court in March 2018, over the operation of the SyRI system, claiming a violation of Article 8 ECHR. Crucially, the Court ruled in favour of the coalition, and declared the SyRI legislation is in violation of Article 8 ECHR due to, which will be discussed in depth in the following sections, a lack of transparency and appropriate safeguards in the connection with the linking of personal data across government agencies.[58]

**18** First, as to what SyRI actually is, the Court defined SyRI as a "legal instrument",[59] which the Dutch government created with the purpose of preventing and combating illegal use of government funds and government schemes in the area of social security and income-dependent schemes, and in order to prevent and combat "taxes and social security fraud and non-compliance with labour laws."[60] The Court went on to explain how the actual SyRI-projects work to achieve these aims. Concretely, when, based on the SyRI legislation, a SyRI-project is started, data from different government agencies is linked and analysed in order to produce a risk report of people. When a risk report is filed on an individual, this means they are "deemed worthy of investigating with regard to possible fraud".[61] The aim is that this automated analysis would help in tracking down social welfare fraud.

**19** Importantly, in its history SyRI has only been used to analyse people in specific neighbourhoods, referred to as "problem" neighbourhoods (i.e. with lower socio-economic inhabitants), which was confirmed by the government in its submissions to the Court.[62] As to the government agencies involved, these range from municipal governments, the Netherlands Tax and Customs Administration, the Social Insurance Bank, the Immigration and Naturalisation Service, the Employee Insurance Agency, as well as supervisory authorities such as the Social Affairs and Employment Inspectorate.[63] The data shared by these government agencies covers an enormous range, totalling on 17 general types of data, including data on health, finance, education, fiscal payments, employment and "integration".[64]

**20** The different steps involved in a SyRI project are as follows. Importantly, a SyRI project starts when a number of the government agencies involved organise in a "collaborative alliance" and create a proposal to use SyRI in a specific neighbourhood.[65] This proposal is submitted to the Minister who, after hearing the advice from the steering group consisting of all the government agencies involved,[66] then officially decides to apply SyRI.[67] The relevant data of the different agencies is then collected, pseudonymised and analysed according to the risk indicators and model as outlined in the proposal.[68] The cases of people flagged by the risk model are then analysed by the Ministry before a definite risk report is submitted, and the relevant government agency conduct further research into possible fraud.[69] The people whose data is involved in the project are only informed when an official investigation follows upon a risk report.[70] Importantly, the risk model and indi-

57 ibid.

58 *SyRI* (n 5) para 5.1.

59 ibid para 3.1.

60 ibid para 4.4.

61 ibid para 3.2.

62 ibid para 3.9-10, 4.24, 6.93. Notably, the Court did *not* find that the use of SyRI in "problem" neighbourhoods in and of itself was disproportionate or in violation of Article 8. However, it did find that *there is a risk* that SyRI "inadvertently creates links based on bias, such as a lower socio-economic status or an immigration background". (see para 6.93).

63 ibid para 3.3; art 64 lid 1 Wet SUWI.

64 Art 5a.1(2) Besluit SUWI.

65 *SyRI* (n 5) para 3.3, 4.20-22; art 64 lid 2 Wet SUWI.

66 ibid para 3.6.

67 ibid para 3.3.

68 ibid para 4.22, 4.28 - 4.29.

69 ibid para 4.29 - 30.

70 ibid para 6.54. Notably, Dutch media has reported that SyRI has not led to the discovery of a single case of fraud.

cators, threshold values, types of data and people involved are unknown to both the Court, the citizens involved and wider society.[71]

**21** Having thus set out the operation of SyRI, the Court then turned to compatibility of the system with the right to private life under Article 8 ECHR, to which we now turn. Concretely, the following sections will focus on four aspects related to the SyRI judgment. First, the way in which the Court involved the general principles of the GDPR in its application of Article 8 ECHR will be considered. Then, the different ways in which the Court ran into issues related to a lack of transparency on how the SyRI systems operate concretely is analysed, followed by a discussion of the possible safeguards for the protection of the right to private life that could be employed. Finally, proposed legislation in the Netherlands that is following in the footsteps of the now void SyRI legislation is discussed.

## I. The relationship between the EU Charter, GDPR and Article 8 ECHR

**22** One of the most striking aspects of the SyRI judgment is the way in which The Hague Court related the GDPR to Article 8 ECHR. The Court used the general principles of data protection from Article 5 GDPR to substantiate the requirements of Article 8 ECHR, more specifically, the criterion that any interference should be "necessary in a democratic society".[72] Using (secondary) EU legislation to interpret ECHR provisions is not uncontroversial as, despite many connections, the EU and the COE remain distinct legal orders.[73] It would seem more appropriate to interpret Article 8 ECHR based on the case law of the ECtHR, and the principles established in the case law, rather than relying on a piece of EU secondary legislation.

This section will trace how the Court came to this line of reasoning and what the possible consequences can be.

**23** As the claimants based their main claim on a violation of Article 8 ECHR, the Court, subsequently centred the judgment around the question whether the SyRI legislation constituted a violation of the fundamental right to a private life as protected by Article 8 ECHR.[74] Basing claims directly on international human rights obligations and, especially, the ECHR, instead of the Dutch Constitution, is common legal practice in the Netherlands. This is due to constitutional provisions that prohibit Dutch Courts from constitutional review of Dutch legal provisions, but does allow for direct application of international human rights treaties.[75] In the judgment, the Court extensively discussed the applicable legal framework, differentiating between, on the one hand, the COE with Article 8 ECHR, and on the other, the EU with Article 7 and 8 of the EU Charter, and the GDPR as relevant secondary legislation.[76] The Court recognised the nature of the ECHR as providing "for a minimum level of protection of the fundamental right to respect for private life",[77] and that within the EU Charter, there is "at least the same minimum level of protection as the ECHR", although the Charter and the GDPR do provide protection that is "specified in more detail and in some instances extends beyond the protection under the ECHR".[78] The Court, more specifically, considered the general principles of data protection in GDPR to be an extension of the fundamental rights protection of the Charter.[79]

**24** As stated, the Court took the striking step to take into account the general principles of data protection from the EU Charter and the GDPR in its review of whether the SyRI was compatibility with Article 8 ECHR. Thus, applying Article 8 ECHR entailed that the SyRI legislation "must meet the aforementioned general principles of data protection, as laid down in Union law in the Charter and the GDPR, such as the principle of transparency, the principle of purpose limitation and the principle of data minimisation."[80] The Court used this conclusion to employ the general principles of data protection from the GDPR to substantiate the "necessary in a democratic society" criterion as part of the Article 8 ECHR test.[81] More specifically, the principles of transparency, data minimisation and purpose limitation were used

See Charlotte Huisman, 'Fraudesysteem Overheid Faalt' *de Volkskrant* (Amsterdam, 27 June 2019) 6-7.

71 ibid para 6.100.

72 *SyRI* (n 5) para 6.7.

73 See also *Nederlandse Jurisprudentie* 2020/386, Note by E.J. Dommering (Case Comment).

74 *SyRI* (n 5) para 5.1, 6.38.

75 Art 93, 94 and 120 Grondwet.

76 *SyRI* (n 5) para 6.19 – 6.41.

77 ibid para 6.37

78 ibid, referencing EU Charter (n 34) art 52(3).

79 *SyRI* (n 5) para 6.27- 36.

80 ibid para 6.40.

81 ibid para 6.80.

to assess whether the requirements of necessity, proportionality and subsidiarity were met as part of this criterion.[82]

**25** The Court seemed to assume a reciprocity between the ECHR and the EU Charter, including EU secondary legislation such as the GDPR, based on the notion that the Charter explicitly provides that the meaning and scope of its rights also guaranteed in the ECHR must be, at a minimum, the same as those in the ECHR.[83] However, this does not mean that the level of protection offered by the ECHR should be supplemented by the additional protection offered within the EU framework when applying ECHR provisions. As such, the assumed reciprocal relation between the ECHR and the EU Charter, including secondary legislation, is not sufficiently substantiated in the judgment. This begs the question to what extent straining to establish this interdependent relationship between the two different legal orders was necessary when the Court could also have opted to apply the GDPR directly, in parallel to its Article 8 ECHR assessment. An explanation for this notable step by the Court might be found in a combination of the ECHR tradition in the Netherlands in combination with the greater flexibility offered by the ECHR as opposed to the GDPR. As stated, basing claims directly on ECHR provisions is common legal practice in the Netherlands due to the direct effect of these international treaties in the Dutch legal system. This would have made the step of further substantiating with principles from the GDPR shorter. Additionally, including the principles of data protection from the GDPR gave The Hague Court more solid ground in assessing the SyRI ADM-system and allowed for a detailed analysis without having to go through the technical analysis and possible prejudicial questions as when the GDPR would have been directly applied. This allowed the Court to include data protection principles while still sticking solidly to the fundamental rights perspective. However, it remains to be seen whether this step will be followed by other Courts. At this point, we can continue to another striking element: the way in which the concept of transparency functioned throughout the judgment.

## II. The principle of transparency and Article 8 ECHR

**26** Transparency forms an essential element of the SyRI judgment, due mainly to the fact that the system itself is inaccessible and its workings are kept secret from The Hague Court, the citizens involved and wider society.[84] This section will analyse the different problems this posed to the Court on several steps of its legal analysis and how these were dealt with. The lack of transparency consisted of the fact that the risk model and indicators, threshold values, types of data and people involved were and, to this day, are unknown and that the citizens involved are not informed of their involvement.[85] Although a rich body of ECtHR case law exists on how to apply the test of Article 8 ECHR (whether the interference of SyRI amounts to a violation of private life) to secretive government measures,[86] testing this ADM system used in the context of government welfare gave rise to apparent difficulties for The Hague Court in several steps of its Article 8 ECtHR analysis: the extent and seriousness of the interference, whether it was in accordance with law, and whether the interference was necessary in a democratic society. The lack of transparency in how the system operated (models, indicators and data used) and in communications to citizens proved fatal as it was one of the main arguments for the Court's conclusion that the automated social welfare fraud system violated Article 8 ECHR.[87] The judgment reveals both the differentiated and pivotal role transparency plays in adjudicating such a government ADM system, but it also leaves many questions unanswered on the scope of protection Article 8 ECHR affords to the government's use of ADM systems. This section will analyse at which points transparency, or the lack thereof, played an important role in the judgment in order to draw out lessons on the fundamental rights dimension of the use of ADM systems by the administrative state.

**27** Immediately, at the first substantive step the lack of transparency on how the ADM system functions led to difficulties for the Court in assessing the extent and seriousness of the interference. The lack of transparency on how the SyRI ADM-systems actually operate meant that the Court, at several points, was

82 ibid para 6.80 -6.107.

83 EU Charter (n 34) art 52(3).

84 *SyRI* (n 5) para 6.65.

85 ibid para 6.100.

86 *S and Marper v UK* App nos 30562/04 and 30566/04 (ECtHR 4 December 2008). See Van der Sloot (n 29); and also, for example, *Szabó and Vissy v Hungary* (n 18), and *Big Brother Watch and Others v UK* App nos 58170/13, 62322/14 and 24960/15 (ECtHR 13 September 2018) (referred to ECtHR Grand Chamber). See Bart van der Sloot and Eleni Kosta, 'Big brother watch and others v UK: Lessons from the latest Strasbourg ruling on bulk surveillance' (2019) 5 *European Data Protection Law Review* 252.

87 *SyRI* (n 5) para 6.7, 6.83, 6.95.

unable to verify the opposing parties' positions.[88] This difficulty in assessing the extent of the interference poses an interesting contrast to established ECtHR case law on mass surveillance where the unknown factors were *when* and against *whom* the interference occurred, but the operation of the mass surveillance system's interference itself was clearly established.[89] In this judgment, The Hague Court was confronted with a complex discussion on what (speculative) elements of the SyRI systems are legally relevant as the parties differed widely on not only the nature, but also the legal definition of SyRI.[90] For example, does SyRI make use of big data, profiling, automated decision-making, machine learning, data mining, unstructured data collection and, if so, which of these elements are relevant for the legal assessment of the system?[91] The remaining question is to what extent this debate, in future cases, would be solved with more technical transparency as, in the end, the legally relevant question is what is the impact of these automated risk assessments on an individual citizen's private life and fundamental rights more generally. Putting most of the focus on the legal characterisation of the technology risks decentring the actual effect of their involvement in the projects, the eventual risk report and possible subsequent fraud investigation on citizens' private lives, and the responsibility of the government. As mentioned above, the UN Special Rapporteur on extreme poverty similarly warns that digital technologies in welfare systems are often presented as "scientific" and neutral, although "they can reflect values and assumption that are far removed from, and may be antithetical to, the principles of human rights."[92]

**28** For now, the Court was able to circumvent most of these discussions by either declaring that it was unable to verify the claims due to the government's secrecy, or stating that the claim was irrelevant for the legal question at hand.[93] The Court concluded that SyRI consists of "structured data processing based on existing, available files" and a risk model which "consist of predetermined risk indicators and which gives an indication of whether there is an increased risk" of social welfare fraud.[94] Further, the Court included the government's secrecy towards the Court, and towards the people involved who are at no point informed, as part of the extent and seriousness of the interference with private life.[95]

**29** Subsequently, the Court proceeded to assess whether SyRI is in accordance with law and, again, the secrecy surrounding the actual functioning of the system inhibited the Court applying the Article 8 ECHR criteria straightforwardly. Following the claimants' arguments, the Court based its assessment on mass surveillance case law from the ECtHR, specifically the case of *S and Marper v UK*.[96] Even though the Court emphasised that the context of mass surveillance is substantially different from the SyRI case, it stated that the *S and Marper* judgment contains "considerations of the ECtHR on data protection of a more general nature".[97] The case shows, according to The Hague Court, that the assessment of "whether the interference is in accordance with the law may be closely connected to the assessment whether the interference is necessary in a democratic society".[98] This led The Hague Court to the conclusion that in this particular instance it did not need to make this assessment, as further analysis would show that the legislation was not "necessary in a democratic society".[99]

**30** The reasoning applied by The Hague Court meant the substantive analysis of the "in accordance with law" criterion was sidestepped, or rather skipped over, in favour of the "necessary in a democratic society" criterion. As recognised by the Court, the substantive requirements contained in the "in accordance with law" criterion are to a large extent dependent on the "content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed".[100] It is not clear that the criteria developed for mass surveillance can be applied to the context of social welfare fraud detection and, consequently, that passing over the

88 ibid para 6.49, 6.53-54.

89 See n 64 above.

90 *SyRI* (n 5) para 6.44.

91 ibid para 6.42-6.65.

92 UN Doc A/74/493 (n 1) para 6.

93 *SyRI* (n 5) para 6.56, 60, 63.

94 ibid para 6.62.

95 ibid para 6.60.

96 ibid para 6.67, citing *S and Marper v UK* (n 86).

97 ibid para 6.67. The plaintiffs had argued that processing personal data for the use of SyRI violated various provision of the GDPR, including Article 6 (Lawfulness of processing), 13 (Information to be provided where personal data are collected from the data subject), and Article 22 (Automated individual decision-making, including profiling). However, the Court held it would 'not assess whether the SyRI legislation is contrary to one or more specific provisions of the GDPR on which' the plaintiffs relied.

98 ibid para 6.71.

99 ibid para 6.72.

100 ibid para 6.69, citing *S and Marper v UK* (n 86) para 96.

"in accordance with law" criterion was warranted in this case. Especially as this line of reasoning offers a form of legitimacy to the government's lack of transparency, framing it as a defect that can be amended with sufficient safeguards.

**31** Finally, as elaborated in the previous section, the Court took the remarkable step of letting transparency play a crucial role in the last step of the analysis: assessing whether the interference was necessary in a democratic society. As elaborated on in the previous section, this criterion was substantiated with the principles of data protection, and transparency in particular, as found in Article 5 GDPR.[101] The Court made clear that, at a minimum, insight must be given into "the risk indicators and the risk model, or at least ... further legal safeguards to compensate for this lack of insight".[102] Additionally, insight needed to be given into "which objective factual data can justifiably lead to the conclusion that there is an increased risk".[103] Absent this information, the Court concluded it was unable to "verify how the simple decision tree [in the risk model], to which the State refers, is generated and of which steps it is comprised".[104] This opacity and lack of information also greatly inhibits the ability of the people involved to exercise their rights or defend themselves, especially since they are at no point informed of their (passive) involvement.[105] As such, the judgment requires governments to provide all necessary information, such as their involvement in an ADM-system to detect social welfare fraud and what their risks scores are, to people in order to enable them to exercise their rights and contest unwanted data processing, which is a core aim of the more specific GDPR transparency provisions.[106]

**32** Further, the Court connected both the potential discriminatory biases (e.g. lower socio-economic status or an immigration background) in the system itself, and the discriminatory and stigmatising effect of the system's implementation, as pointed out by the UN Special Rapporteur, to the apparent lack of transparency.[107] Especially considering SyRI's sole implementation in "problem districts" of the Netherlands, and the large amount of (sensitive) data used, the Court explicitly recognised the "risk that SyRI inadvertently creates links based on bias, such as a lower socio-economic status or an immigration background".[108] The Court concluded that "due to the absence of verifiable insights into the risk indicators and the risk model as well as the function of the risk model" it was unable to ascertain whether the risk of stigmatisation and discrimination was "sufficiently neutralised"[109] (i.e., the risk would be neutralized if the specific risk indicators used by SyRI were made public, so it could be analysed properly whether the system is not discriminatory against individuals based on race, national or social origin, or association with a national minority). Via this procedural line of reasoning, the Court, remarkably, brought issues pertaining to racism, discrimination and classism into the fold of Article 8 ECHR, instead of Article 14 ECHR (which prohibits discrimination). Explicitly taking into account the potential harmful social and political effects of these types of ADM systems in the context of social welfare is of crucial importance. However, putting them into a procedural context of "transparency" and "sufficient safeguards" runs the risk of falling into the frame that discrimination or social stigmatisation can be technically solved.[110] This focus on the technological aspect ignores and neutralises the deeply political and social aspects that are especially relevant in the context of social welfare systems that serve the most vulnerable in society (especially the discriminatory element of these systems).

**33** Transparency plays a pivotal role in the SyRI judgment, taking on many guises and appearing at every step of the Court's analysis. What is beyond dispute is the conclusion that the extent to which the Dutch government withheld information and insight into its ADM system does not pass the test under Article 8 ECHR of whether the interference constituted a violation. A minimum of insights into the workings of the system (i.e., the risk indicators and model) is necessary for courts to perform their supervisory role over the executive branch of government, and for the people involved to defend themselves against government overreach. However important this transparency is, it does to a large extent only form a precondition for the truly substantive assessment of whether the impact on people's private life of suspecting them of social welfare fraud, their (passive) involvement in the ADM-system, their risk-report and possible investigation is justified. A possible risk is that the discussion on what transparency should concretely mean, or on how to legally characterise the ADM

101 *SyRI* (n 5) para 6.30.

102 ibid para 6.95.

103 ibid para 6.87.

104 ibid para 6.90.

105 ibid para 6.90.

106 GDPR (n 35) art 13-14.

107 *SyRI* (n 5) para 6.92-94.

108 ibid para 6.93.

109 ibid para 6.94.

110 See UN Doc A/74/493 (n 1).

systems themselves, once they are more transparent, deflects attention from this substantive assessment. For example, the assessment of how increased transparency towards the people involved will actually translate into contestable systems, or what the relation between the government and its citizens should be in the context of social welfare, and what privacy and treatment people can expect.[111]

## III. Lack of safeguards

**34** In addition to transparency, a crucial aspect of the SyRI judgment was the Court's finding that the SyRI legislation contained "insufficient safeguards" to protect the right to private life, in violation of Article 8(2) ECHR.[112] This was because, as the Court held, the SyRI legislation paid "insufficient attention to the principle of purpose limitation and the principle of data minimisation", and thus, violated Article 8(2) ECHR.[113]

**35** First, while the legislation contained an "exhaustive enumeration" of the data categories that qualify for processing,[114] the Court pointedly held it was "hard to imagine any type of personal data that is not eligible for processing in SyRI".[115] Importantly, the Court criticised the SyRI legislation for not providing for a "comprehensive review," or a review by an independent third party, prior to the data processing by the Minister, in order for an assessment of whether or not the interference with private life was "necessary, proportionate and subsidiary in light of all the files that are linked in a project considering the specific purpose of that project".[116] The Court noted that a body called the National Intervention Teams Steering Group (LSI) advises the Minister about the application of SyRI in a specific SyRI project. However, the Court stated that the LSI is "merely an advisory organ", and its advice was "non-binding and lacks an explicit legal basis".[117] Thus, the Court held that the lack of independent assessment prior to the approval by the Minister violated Article 8(2) ECHR, which requires such a safeguard. Crucially, the Court held the LSI was comprised of "representatives of organs which also have an interest in combating and preventing abuse and fraud," including the Social Affairs and Employment Inspectorate, the Tax and Customs Administration, and the police.[118] Moreover, in relation to data protection impact assessments (DPIA), the Court harshly criticised the State's approach. The Court held that the State had "failed to elucidate why, considering the extent and seriousness of the invasion of private life, occasioned by the processing of data in SyRI," a data protection impact assessment was not carried out for each individual project.[119] However, the Court stopped short of finding a violation of Article 8(2) ECHR on the basis of the lack of individual data protection assessments.

**36** The Court concluded that in "view of the large amount of data that qualify for processing in SyRI," no comprehensive and no independent assessment prior to the approval by the Minister, the SyRI legislation therefore contained "insufficient safeguards", in light of the principles of purpose limitation and data minimisation under Article 8 ECHR.[120] This focus on insufficient safeguards was entirely justified, as the SyRI legislation lacked any independent oversight to assess whether it was proportionate to link such a vast amount of personal data from different government agencies for the purpose of a specific SyRI project to develop individual risk profiles of social welfare fraud. Especially important are safeguards that allow for not just a discussion focussed on the workings of the technology used (e.g., the technical properties of the SyRI system) but allows for a substantive

111 Notably, the Court nowhere referred to case law on how the ECtHR conceptualises and protects rights in relation to social welfare, other than through the frame of transparency and privacy under Article 8 ECHR. This case law includes, for example, in relation to Article 6 ECHR, *Zednik v the Czech Republic* App no 74328/01 (ECtHR, 28 June 2005); in relation to Article 1 of Protocol No. 1 ECHR, *Azinas v Cyprus* App no 59498/00 (ECtHR, 20 June 2002); and in relation to Article 14 ECHR, *Van Raalte v the Netherlands* App no 20060/92 (ECtHR, 21 February 1997). For analysis of this case law, see Ingrid Leijten, 'The right to minimum subsistence and property protection under the ECHR: Never the twain shall meet?' (2019) 21 *European Journal of Social Security* 307; Ingrid Leijten, *Core Socio-Economic Rights and the European Court of Human Rights* (CUP 2018); Antonia Baraggia and Maria Elena Gennusa, 'Social Rights Protection in Europe in Times of Crisis: "A Tale of Two Cities"' (2017) 11 *Vienna Journal on International Constitutional Law* 479; and Ana Gómez Heredero, *Social security as a human right: the protection afforded by the European Convention on Human Rights* (Council of Europe Publishing 2007).

112 *SyRI* (n 5) ibid para 6.106.

113 ibid para. 6.96.

114 ibid para 6.98.

115 ibid.

116 ibid para 6.99.

117 ibid para 6.101.

118 ibid para 6.101.

119 ibid para 6.105.

120 ibid para 6.106.

discussion on whether the use of such systems is warranted. Thus, the Court concluded that the SyRI legislation violated Article 8(2) ECHR because (a) it was insufficiently transparent; and (b) contained insufficient safeguards to protect the right to private life, as required under Article 8(2) ECHR. However, the Court's analysis of (and supposed concern for) sufficient safeguards was somewhat undermined, as mentioned above, by its refusal to examine whether the SyRI legislation was "in accordance with law" under the first limb of Article 8(2) review. The Court decided that it would leave "undiscussed in its review whether the SyRI legislation is sufficiently accessible and foreseeable and as such affords an adequate legal basis".[121] Finally, the Court stated, it would not assess whether the SyRI legislation was in violation of specific provisions of the GDPR[122].

## IV. SyRI 2.0

**37** Not long after the of SyRI judgment was delivered, the Dutch government proposed legislation to the Dutch Parliament which critics have dubbed "Super SyRI".[123] The law - *wet gegevensverwerking door samenwerkingsverbanden* (WGS) - is intended to function as a framework for data sharing and the use of ADM systems.[124] The government considers the WGS is needed as it creates a legal basis for the data processing which is currently lacking,[125] and the data sharing and analysis across government agencies is deemed necessary for a more integrated approach to societal problems.[126] This proposed legislation clearly shows the impact of the SyRI judgment, and the fast pace of the digital transformation of the administrative state.

**38** Due to several waves of severe criticism,[127] the proposed WGS has been amended twice, with its most recent version currently being discussed in the Dutch Senate.[128] The latest WGS proposal addresses several of these criticisms and, in essence, functions similarly to SyRI: creating a legal framework basis for data sharing and the use of ADM systems across government agencies. A notable difference is that the WGS is not specifically geared towards social welfare fraud, but is currently aimed at government partnerships in the domain of financial fraud, money laundering, organised crime and complex health and safety cases.[129] However, the law does contain the explicit possibility of adding other partnerships in a broad range of domains, including social welfare, by means of government decree.[130] Despite the substantial reforms to the proposed WGS, the current version is persistently receiving considerable criticism from NGOs, wider society, and the Dutch Parliament itself.[131] The criticism focusses on, still, the reliance on delegated competencies (a framework-law structure) and the vast scope of different domains or goals included in the framework. The combination of both these qualities means the possible scopes of partnerships, types of data and ADM systems are nearly unlimited.

**39** Viewing the proposed WGS in light of the SyRI judgment brings up many questions with regards to the concrete functioning of several of the proposed safeguards, and the de facto extent of the transparency of possible ADM systems. However, the most interesting connection to make will be

121 ibid para 6.72.

122 ibid para 6.107.

123 Peter te Lintel Hekkert, 'Zet Super SyRI op de Lijst met Controversiële Wetsvoorstellen' (*FNV*, 1 Febuary 2021) <https://www.fnv.nl/nieuwsbericht/sectornieuws/uitkeringsgerechtigden/2021/02/verklaar-super-syri-controversieel>; 'Super SyRI: Bestuurd door Black Boxes' (*Bij voorbaat verdacht*, 12 November 2020) <https://bijvoorbaatverdacht.nl/super-syri-bestuurd-door-black-boxes/>.

124 TK 2019-2020, 35 447, nr. 2.

125 Werkgroep verkenning kaderwet gegevensuitwisseling, 'Kennis delen geeft kracht' (2014), bijlage bij TK 2014-2015, 32 761, nr. 79, p. 5; M. P. Beijer, 'Het voorstel voor een nieuw regelgevend kader voor de gegevensverwerking door samenwerkingsverbanden' (2020), TvBSH 6; TK, 2019-2020, 35 447 nr 3, p. 2.

126 TK 2019-2020, 35447, nr. 3, p. 2.

127 See bijlagen bij TK 2019-2020, 35 447, nr. 3; TK 2020-2021, 35 447, nr. 20; TK 2019-2020, 35 447, nr. 4; 'SyRI-coalitie maant kabinet: stop overhaaste invoering 'Super SyRI'' (*Bij voorbaat verdacht*, 25 May 2020) <https://bijvoorbaatverdacht.nl/syri-coalitie-maant-kabinet-stop-overhaaste-invoering-super-syri/>; and Harriet Duurvoort, 'Hoe de Overheid Inbreuk maakt op Privacy is Dubieuzer dan Facebook en Google' *de Volkskrant* (Amsterdam, 27 May 2020). For a summary of the earlier criticism see: M. P. Beijer (2020) (n 116) p. 311.

128 EK 2020-2021, 35 447, nr. Al; TK 2019-2020, 35 447, nr. 1; TW 2019-2020, 35 447, nr. 4.

129 Hoofdstuk 2 WGS.

130 Art 3.1 WGS.

131 'SyRi-coalitie aan Eerste Kamer: 'Super SyRI' Blauwdruk voor meer Toeslagenaffaires' (*Platform Bescherming Burgerrechten*, 11 January 2021) <https://platformburgerrechten.nl/2021/01/11/syri-coalitie-aan-eerste-kamer-super-syri-blauwdruk-voor-meer-toeslagenaffaires/?s=SyRI>; Tommy Wieringa, 'De Wet is een Slang die Alleen Mensen Zonder Schoenen Bijt' *NRC Handelsblad* (Amsterdam, 23 January 2021) 2. TK 2020-2021, 35510, nr. 27.

with a not previously discussed element of the SyRI judgment. As the Court emphasises at several points in the judgment, that it considers, based on ECHR case law, the government to have "a special responsibility when applying new technologies to strike the right balance between the benefits the use of such technologies brings as regards preventing and combating fraud on the one hand, and the potential interference with the exercise of the right to respect for private life through such use on the other hand."[132] This "special responsibility" plays an important role in the Court's weighing of whether SyRI's interference in people's private lives is to be considered necessary in a democratic society.[133] The Court substantiates this responsibility further by emphasising the speed of developments in data-linking and automated analysis, which increases the risk for people's private lives, whilst simultaneously making it more difficult to understand what effect these systems have on people's lives.[134] This is why, according to the Court, the government has a "special responsibility" with the implementation of such technologies, which can be interpreted as raising the bar for a government in those circumstances.

**40** Considering this special responsibility, especially the instrument of a framework law which leaves most particulars to delegated government decrees can be seen as problematic. Any government system geared at fraud detection needs to balance this aim with the fundamental right to private life. This special responsibility seems to imply that the exercise of ensuring this "fair balance" must be conducted with more care or more extensively when implementing ADM systems. The structure of a framework law precludes the possibility of an extensive parliamentary and societal debate, and detailed context-specific deliberations on the implementation of an ADM system by a given (private) partnership. As such, a framework law allowing for the use of ADM systems by the government seems to not take sufficient heed of this special responsibility to substantiate how the "fair balance" between a specific aim and the right a private life is achieved. Interpreted in this way, this idea of a special responsibility as developed in the SyRI judgment is fully in line with the original advice of the Council of State in 2019, where it advised against a framework law, favouring specific sectoral legislation.[135]

132 *SyRI* (n 5) para 6.84, citing *S and Marper v UK* (n 86) para 112.

133 ibid para 6.84 - 85.

134 ibid para 6.85.

135 TK 2019-2020, 35 447, nr. 4.

## E. Conclusion

**41** This article has critiqued the SyRI system in the Netherlands and used The Hague Court's landmark judgment as a lens through which to examine the broader issues arising from the digitisation of the State through the use of ADM systems by public authorities. This discussion raises three concluding points. First, the conceptualisation of the problems and issues with ADM systems seems to be over-focused on the inner workings of the technology used (e.g., the technical properties of the SyRI system), an over-focus on attempting to fit technological questions into specific legal classification regimes (primarily under the GDPR), and with the technology itself being unquestionably connected to progress and efficiency i.e., technological-solutionism. However, this approach risks law becoming merely an overly technologically-centred analysis. Instead, we argue that when looking at the use of ADM systems by public authorities, we should treat the technology as a mere starting point, with the role of law (and human rights law in particular) being to bring in other perspectives, including the role of the technology in its social context and people's actually experience with these systems. This occurred in the SyRI case for instance when the Court was able to take into account the SyRI system was only being used in so-called problem neighbourhoods, and that such uses meant the system could create links based on bias, including lower socio-economic status or an immigration background. Of course, there are limitations to human rights law analysis of ADM systems, as this form of legal review does not allow for a questioning of the underlying policy choices for introducing these systems (beyond the cursory examination of whether an ADM system pursues a legitimate aim). A second connected point concerns the "special responsibility" governments have to safeguard the private life of their citizens when implementing ADM systems. This increased responsibility concretely translates to the need for the government to take extra care in establishing there is a fair balance between the aim the ADM system seeks to fulfil, and any interference with citizens' private lives. General framework laws, such as those implemented in the Netherlands, that leave many of the concrete weighing of these interests and rights to delegated ministerial competencies, do not easily seem to be compatible with this special responsibility, and are a model that should not be followed in other EU member states.

**42** Finally, the analysis demonstrates the difficulty of the application of data protection frameworks (especially Article 22 GDPR on automated individual decision-making) to ADM systems deployed by the administrative state, and to the digital transformation of the State more broadly. This was epitomised by The Hague Court's convoluted approach to the GDPR

and Article 8 ECHR, and choosing the latter as the most appropriate framework for its examination of the SyRI legislation. However, as discussed above, the suitability of current data protection frameworks for protecting individuals from disproportionate interferences with their private life must be questioned. Instead, an assessment of these technologies should recognize that their use "prompts a particularly high probability of infringement of human rights, including by introducing or amplifying distributive injustice", especially where the ADM system produces serious consequences for people, such as legal consequences, losing social welfare, or people forced by law to be subjected to risk profiling by public authorities.[136] As such, we must move beyond treating these technologies are simply "scientific" and "neutral",[137] and question more structural aspects, including the underlying policy choices involved in their deployment. This approach could hopefully obviate the need for courts, such as The Hague Court, to step in to protect individual citizens from the excesses of the use of ADM systems by the State.

136 ibid.

137 UN Doc A/74/493 (n 1) para 6.