ECLI:NL:RBDHA:2020:1878

Instantie	Rechtbank Den Haag
Datum uitspraak	05-02-2020
Datum publicatie	06-03-2020
Zaaknummer	C-09-550982-HA ZA 18-388 (English)
Rechtsgebieden	Civiel recht
Bijzondere kenmerken	Bodemzaak Eerste aanleg - meervoudig
Inhoudsindicatie	

see: ECLI:NL:RBDHA:2020:865 (Dutch version)

SyRI legislation in breach of European Convention on Human Rights

The Hague District Court has delivered a judgment today in a case about the Systeem Risico Indicatie, or SyRI. SyRI is a legal instrument used by the Dutch government to detect various forms of fraud, including social benefits, allowances, and taxes fraud. The court has ruled that the legislation regulating the use of SyRI violates higher law. The court has decided that this legislation does not comply with Article 8 of the European Convention on Human Rights (ECHR), which protects the right to respect for private and family life, home and correspondence.

Review

The court reviewed whether the SyRI legislation is in breach of provisions of international or European law binding on all persons. The court assessed whether the SyRI legislation complies with Article 8 paragraph 2 ECHR. This particular provision requires striking a fair balance between the interests of the community as a whole, which the legislation serves, and the right of the individuals affected by the legislation to respect for their private life and home.

Special responsibility with introduction of new technologies

According to Article 8 ECHR the Netherlands – as a party to the ECHR – has a special responsibility when applying new technologies. It must strike the right balance between the benefits such technologies bring and the violation of the right to a private life through the use of new technologies. This also applies to the use of SyRI.

Use of SyRI insufficiently transparent and verifiable

After a review of the objects of the SyRI legislation, namely preventing and combating fraud in the interest of economic welfare, in relation to the violation of private life by the legislation, the court has drawn the conclusion that in its current form the SyRI legislation fails to comply with Article 8 paragraph 2 ECHR. The court has decided that the legislation does not strike a fair balance, as required under the ECHR, which would warrant a sufficiently justified violation of private

life. In that respect, the application of SyRI is insufficiently transparent and verifiable. As such, the SyRI legislation is unlawful, because it violates higher law and, as a result, has been declared as having no binding effect.

Background

Several civil society interest groups, including the Dutch Section of the International Commission of Jurists (NJCM) and two private individuals, instituted these proceedings against the State of the Netherlands. The Netherlands Trade Union Confederation (FNV) joined as a party in the claimants' proceedings. Claimants want to call 'a halt' to the use of SyRI. They believe that by applying SyRI, the Netherlands government unlawfully violates human rights. The State disagrees and argues that the SyRI legislation contains sufficient safeguards to protect the privacy rights of all.

ECLI:NL:RBDHA:2020:865

Vindplaatsen Rechtspraak.nl

Uitspraak

—

---

vonnis

THE HAGUE DISTRICT COURT

Commerce Team

Case number / cause list number: C/09/550982 / HA ZA 18-388

Judgment of 5 February 2020

in the matter of

1 NEDERLANDS JURISTEN COMITÉ VOOR DE MENSENRECHTEN

established in Leiden,

2. **STICHTING PLATFORM BESCHERMING BURGERRECHTEN**
established in Amsterdam,

3. **STICHTING PRIVACY FIRST** established in Amsterdam,

4. **STICHTING KOEPEL VAN DBC-VRIJE PRAKTIJKEN** established in Amsterdam,

5. **LANDELIJKE CLIËNTENRAAD** established in The Hague,

6. **[claimant sub 6]** of [residence 1] ,

7. **[claimant sub 7]** of [residence 2] ,

eisers,

attorney *mr.* A.H. Ekker of Amsterdam,

and

FEDERATIE NEDERLANDSE VAKBEWEGING established in Utrecht,

intervening third party, joining the claimants,

attorney *mr.* A.H. Ekker of Amsterdam,

versus

THE STATE OF THE NETHERLANDS seated in The Hague,

defendant,

attorney *mr.* C.M. Bitter of The Hague.

Claimants are hereinafter jointly also referred to as NJCM et al. and separately as NJCM, Platform Bescherming Burgerrechten, Privacy First, Koepel van DBC-Vrije Praktijken, Landelijke Cliëntenraad, [claimant sub 6] , and [claimant sub 7] , respectively. The intervening third party is referred to as FNV. The defendant is referred to as the State.

This judgment is structured as follows:

1 The course of the proceedings

1.1. The course of the proceedings is evidenced by the following:

- the summons of 27 March 2018 with exhibits,
- the statement of defence with exhibits,
- the judgment in the procedural issue for joinder of 26 September 2018 along with the documents named therein,
- the document containing comments on the part of FNV of 14 November 2018,
- the reply on the part of the State of 14 November 2018,
- the judgment of 2 January 2019, ordering a personal appearance of the parties,
- the report of the personal appearance of the parties, drawn up without the presence of the parties involved of 29 October 2019 and the document containing exhibits on the part of NJCM et

al., submitted at the hearing, with exhibits.

1.2. The parties were offered the opportunity to file factual comments on the report. The State made use of this opportunity with its letter of 29 November 2019 and NJCM et al. with its letter of 3 December 2019. The court reads the report with due observance of the parties' comments.

1.3. Finally, a date for judgment was scheduled.

2 NJCM et al. and FNV

2.1. NJCM et al. is a coalition of civil society interest groups and two natural persons.

2.2. The Dutch Section of the International Commission of Jurists (*Nederlands Juristen Comité voor de Mensenrechten* – NJCM) is an organisation involved in the protection and strengthening of human rights and fundamental freedoms. The Civil Rights Protection Platform (*Platform Bescherming Burgerrechten*) focuses on the protection of traditional civil rights. Privacy First aims to preserve and promote the right to privacy. The Umbrella Organisation of DBC-free Practices (*Koepel van DBC-Vrije praktijken*) is committed to the protection of the right to privacy of clients of psychotherapists.

2.3. The National Client Participation Council (*Landelijke Cliëntenraad*) was established pursuant to the Work and Income (Implementation Organisation Structure) Act (*Wet structuur uitvoeringsorganisatie werk en inkomen*, hereinafter: SUWI Act or the Act). This organ consists of representatives of national client organisations, municipal client participation organisations and the central client participation councils of the Employee Insurance Agency (*Uitvoeringsinstituut werknemersverzekeringen*, hereinafter: UWV) and the Social Insurance Bank (*Sociale verzekeringsbank*, hereinafter: SVB). The National Client Participation Council is responsible for periodically consulting UWV, SVB, the municipal authorities and the Minister of Social Affairs and Employment (hereinafter: the Minister) about the design and implementation of client participation at the organs in questions, and to consult the Minister about proposals of the National Client Participation Council regarding policy issues in the area of work and income.[1] According to its internal rules, the National Client Participation Council aims to fulfil a key role pertaining to client participation regarding policy issues in the area of work and income, among other things.

2.4. [claimant sub 6] is a philosopher, lawyer, author and columnist. [claimant sub 7] is an author, columnist and presenter.

2.5. The Netherlands Trade Union Confederation (*Federatie Nederlandse Vakbeweging* – FNV) is a trade union. It promotes the interests of its members, guided by – among other things – the fundamental values of equality of all persons, freedom, justice and solidarity.

3 The facts

3.1. The *Systeem Risicoindicatie* (hereinafter: SyRI) is a legal instrument the Netherlands government uses to prevent and combat fraud in the area of social security and income-dependent schemes, taxes and social security, and labour laws. According to the legislator, SyRI is a technical infrastructure with associated procedures with which data can be linked and analysed anonymously in a secure environment, so that risk reports can be generated.[2]

3.2. A risk report means that a legal or natural person is deemed worthy of investigating with regard to possible fraud, unlawful use and non-compliance with legislation.

3.3. The Minister applies the instrument at the request of certain government bodies or other bodies with a public function. These currently are the Municipal Executives (hereinafter: the municipal authorities), UWV, SVB, the Netherlands Tax and Customs Administration (hereinafter: the Tax and Customs Administration), the Immigration and Naturalisation Service (*Immigratie- en Naturalisatiedienst*, hereinafter: IND) as well as supervisory authorities such as the Social Affairs and Employment Inspectorate. These bodies may form a collaborative alliance in which they exchange data. By applying SyRI, the data files which the government or other bodies have available are linked in a structured manner to be able to identify related abuses in the aforementioned areas and increase chances of catching the perpetrators of such abuses.

3.4. According to the legislator, this method leads to an efficient and effective use of the control system.

3.5. The technique used in the application of SyRI is based on a practice predating a legal basis for the use of SyRI. A nationwide structure of intervention teams was established for the purpose of a joint approach to taxes and social security fraud, social benefits fraud, illegal employment and associated abuses.

3.6. In 2003 the bodies involved in this structure concluded a Cooperation Agreement for Intervention Teams. The agreement created a two-level structure: a National Intervention Teams Steering Group (*Landelijke Stuurgroep Interventieteams* – hereinafter: LSI) and projects carried out at the regional level by Anti-Fraud Regional Platforms. The Cooperation Agreement for Intervention Teams was updated in 2017.[3]

3.7. The LSI is chaired by a representative of the Ministry of Social Affairs and Employment and is comprised of representatives of the Social Affairs and Employment Inspectorate, the Tax and Customs Administration, the UWV, the police, the municipal authorities (represented by the Association of Netherlands Municipalities (*Vereniging van Nederlandse Gemeenten* – VNG)), the SVB, the Public Prosecution Service and the IND.

3.8. Legal provisions for linking files[4] have been in place since 2004 pursuant to the Work and Social Assistance Act (*Wet werk en bijstand*, hereinafter: WWB). Section 64 WWB (as of 1 January 2015: Participation Act) obliges certain bodies to provide statements and information to UWV required for the implementation of said act. In 2005 the then State Secretary for Social Affairs and Employment adopted a framework for the accessibility of data sources for the purpose of linking records. In 2005 the Waterproof project was launched. In this project record linkage occurred in which the living situation of recipients of social assistance under the WWB in 65 municipalities was verified by linking the consumption figures of water companies to the living details and pollution units of the water boards. In response to criticism from the Dutch Data Protection Authority (*College voor bescherming van persoonsgegevens* – Cbp) of record linkage in this project, the former Social Security Information and Investigation Service (*Sociale Inlichtingen en Opsporingsdienst* – SIOD, currently the Social Affairs and Employment Inspectorate, investigation department) created an environment which was referred to as the 'black box'. In this environment, the SIOD carried out record linkages and developed risk profiles with the help of these record linkages carried out by order of and for the regional intervention teams. The 'black box' project ended in 2010.

3.9. Between 2008 and 2014, 160 intervention team projects were carried out under the auspices of the LSI. In 22 of these projects SyRI or its precursors had been used. In 19 of the 21 completed intervention team projects a so-labelled neighbourhood-oriented approach had been applied. This approach was clarified by the Minister as follows:

"That is to say, several addresses in a particular neighbourhood of a municipality were investigated by the intervention team in the context of social benefits fraud, tax allowance fraud or taxes fraud. The purpose of these projects is to contribute to the improvement of living conditions

in such neighbourhoods. Therefore, these projects also pay specific attention to offering care and support to persons exhibiting care-avoiding behaviour."[5]

3.10. Since 2015, after the use of SyRI had been regulated by legislation, the following SyRI projects have been launched: 'G.A.L.O.P. II', 'Address fraud Afrikaander neighbourhood in Rotterdam' , 'WGA Vulnerable neighbourhoods Capelle aan den IJssel', 'WGA Rotterdam Bloemhof & Hillesluis' and 'WGA Haarlem Schalkwijk'.[6]

4 The SyRI legislation

General

4.1. The SUWI Act was amended as of 1 January 2014 in order to enshrine in law the application of SyRI.[7] The conditions for the application of SyRI are detailed in the SUWI Decree.[8]SyRI now has a legal basis in Section 65 SUWI Act viewed in conjunction with Section 64 SUWI Act and Chapter 5a SUWI Decree. The then amended SUWI Act and the SUWI Decree are hereinafter jointly referred to as the SyRI legislation. The court will now explain the SyRI legislation in more detail below.

4.2. The term 'data' is defined in Section 1 subsection 2 SUWI Act. It is taken to mean, among other things, personal data within the meaning of the General Data Protection Regulation (hereinafter: GDPR).[9] Up to the date of application of the GDPR on 25 May 2018, reference was made to the Personal Data Protection Act (*Wet bescherming persoonsgegevens*, hereinafter: Wbp Act).

4.3. Also as regards the concepts of processing, controller and processor, Section 1 subsection 2 SUWI Act is in line with the GDPR (Article 4, part 2, 7 and 8) and before 25 May 2018 the Wbp Act.

Data supply for use by a collaborative alliance

4.4. Section 64 subsection 1 SUWI Act provides for a collaboration between several administrative bodies and persons designated for that purpose by or pursuant to the law. Persons here does not refer to natural persons, but to those who are charged with monitoring compliance with or implementation of regulations falling under the responsibility of the Minister. These administrative bodies and persons are expressly referred to in Section 64 subsection 1 SUWI Act, or may be designated by ministerial regulation (hereinafter: the designated government bodies). At this point in time, the bodies referred to above in 3.3 have been designated (hereinafter: government or other bodies). According to the wording of the act, the purpose of collaborating is as follows:

"an integral government action as regards the prevention of and combating the unlawful use of government funds and government schemes in the area of social security and income-dependent schemes, preventing and combating taxes and social security fraud and non-compliance with labour laws."

4.5. Two or more of the designated government or other bodies may conclude a collaborative alliance in which data are processed as required for the aforementioned purpose of that collaborative alliance (Section 64 subsection 2 SUWI Act).

4.6. The starting point is that the designated government or other bodies that participate in a collaborative alliance are obliged to provide that necessary information to each other, in which case they are joint controllers within the meaning of Article 26 GDPR (Section 64 subsection 3 SUWI Act).

4.7. In case of a collaborative alliance in which the participating government or other bodies also wish to apply SyRI, they submit a request to that effect to the Minister. In that case, and contrary to the aforementioned starting point, the necessary information must be provided to the Minister, in

which case the Minister is the controller within the meaning of the GDPR (Section 64 subsection 4 SUWI Act in conjunction with Section 65 subsection 1 SUWI Act).

Legal basis for SyRI

4.8. Section 65 SUWI Act subsequently provides the legal basis for the processing of the aforementioned necessary information in SyRI by the Minister for the purpose of carrying out risk analyses. This section also contains provisions for submitting a risk report, confidentiality, retaining the information that a risk report has been submitted, using a risk report, feedback and removal. Finally, it is specified which further rules are in any event to be laid down by order in council. The latter has been put into effect in the SUWI Decree, and in particular Chapter 5a of said Decree.

4.9. A request to the Minister to process data in SyRI may only be submitted by a collaborative alliance of designated government or other bodies with the intention of applying SyRI. Each of the collaborating bodies must also be a party to the Cooperation Agreement for Intervention Teams (Section 65 subsection 1 SUWI Act in conjunction with Article 1.1 bb and Article 5.a.1 paragraph 1 SUWI Decree).

4.10. The Public Prosecution Service and the police are parties to the Cooperation Agreement for Intervention Teams and represented in the LSI. However they are not one of the designated government or other bodies within the meaning of Section 64 SUWI Act. Therefore, they cannot enter into a collaborative alliance within the meaning of Section 64 SUWI Act and the SUWI Decree. They can therefore also not submit requests for the application of SyRI, nor for that purpose provide data to the Minister pursuant to Sections 65 subsection 1 and 64 subsection 4 SUWI Act. They can – however – receive risk reports at their request insofar as required in the performance of their statutory duty (see Section 65 subsection 3 SUWI Act and also see 4.13 below).

Risk reports, retention obligation, removal from SyRI and confidentiality

4.11. If the Minister processes data in SyRI, the data may only be used to submit a risk report about a natural person or legal person for the purpose as described in Section 64 subsection 1 SUWI Act (Section 65 subsection 1 SUWI Act).

4.12. Section 65 subsection 2 SUWI Act defines a risk report as follows:

"the provision of individualised information from the *systeem risico indicatie* [SyRI] containing a finding of an increased risk of unlawful use of government funds or government schemes in the area of social security and income-dependent schemes, taxes and social security fraud or non-compliance with labour laws by a natural person or legal person, and of which the risk analysis, consisting of coherently presented data from the *systeem risico indicatie* [SyRI], forms part."

4.13. In individual cases, the Minister submits risk reports to the designated government or other bodies which have requested the application of SyRI and insofar as necessary for the proper performance of their statutory duty. The Minister may also submit risk reports to the Public Prosecution Service and the police at their request and insofar as necessary for the performance of their statutory duty (Section 65 subsection 3 SUWI Act).

4.14. A risk report register has been established for the purpose of this information provision to the participating government or other bodies and the Public Prosecution Service and the police, and to inform, at their request, the individuals to whom a risk report pertains. Following an investigation, the individuals involved are not informed separately about the risk reports processed in the register (Article 5a.5 SUWI Decree).

4.15. A risk report is retained by the Minister for not longer than deemed necessary for the purpose of processing risk reports and for a period of no more than two years. The designated government or other body that has received the risk report may make use of the risk report for two years and

must give feedback to the Minister about the results of the risk report. That feedback must be provided within 20 months from the start of the SyRI project. Apart from this, the data processed in SyRI must in any event be removed from SyRI no later than two years following its submission into SyRI (Section 65 subsections 5, 6 and 7 SUWI Act and Articles 5a.3 and 5.a.5 SUWI Decree).

4.16. The act also provides for a duty of confidentiality for all who, pursuant to Section 65 SUWI Act, gain access to data recorded in a risk report pertaining to a natural or legal person, with analogous application of the duty of confidentiality as regards the data (Section 65, subsections 3 through to 7 SUWI Act and Articles 5a.5 through to 5a.7 SUWI Decree).

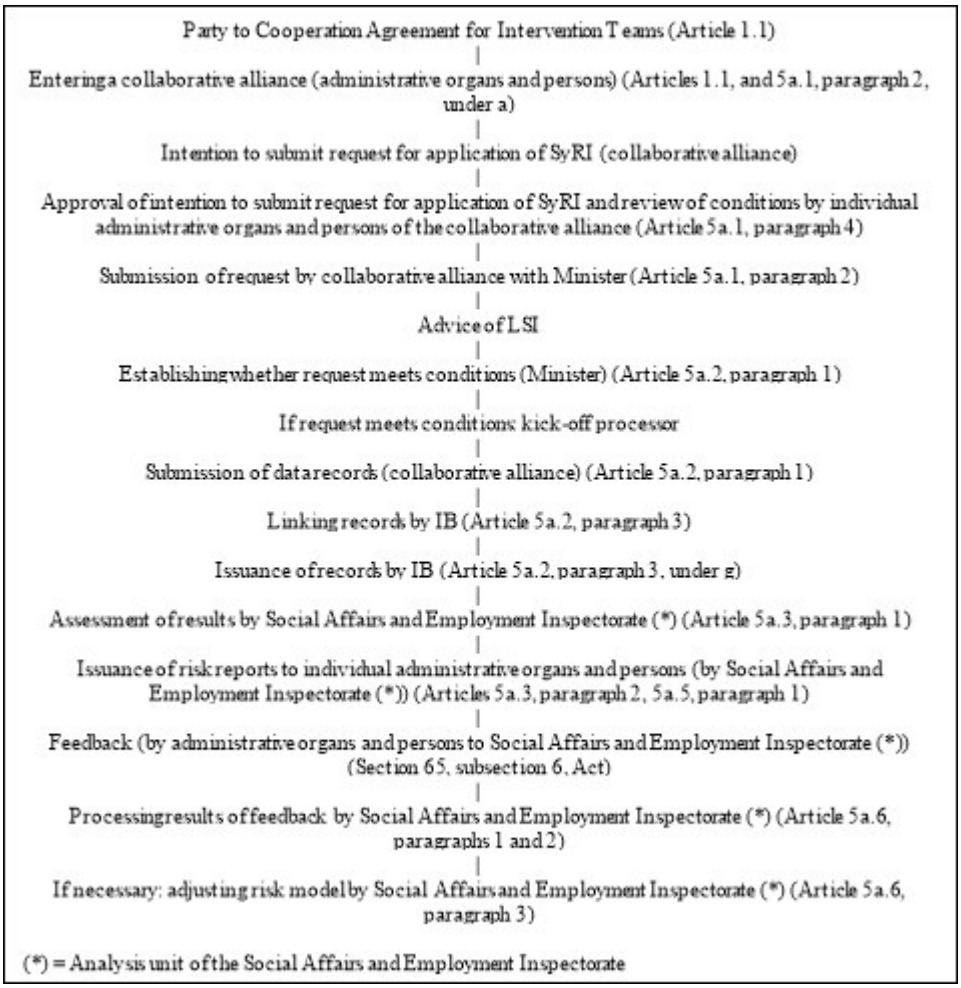
Data which may be processed in SyRI

4.17. One or more of the following categories qualify for processing in SyRI (Article 5a.1 paragraph 3 SUWI Decree):

a. work data, being data with which the work performed by a person can be established;
b. data on administrative measures and sanctions, being data proving that an administrative fine has been imposed on a natural or legal person, or that another administrative measure has been taken;
c. tax data, being data with which the tax obligations of a natural or legal person can be established;
d. data on movable and immovable property, being data with which the possession and use of certain property by a natural or legal person can be established;
e. data on grounds for exclusion from social assistance benefit or other benefits, being data proving that a person is not eligible for a benefit;
f. trade data, being data with which the nature and activities of a legal person can be established;
g. housing data, being data with which the actual or other place of residence or place of business of a natural or legal person can be established;
h. identifying data, being for a natural person: name, address, city, postal address, date of birth, gender and administrative characteristics, and for a legal person: name, address, postal address, legal form, place of business and administrative characteristics;
i. civic integration data, being data with which it can be established if an obligation to participate in a civic integration programme has been imposed on a person;
j. compliance data, being data with which the compliance history with legislation and regulations of a natural and legal person can be established;
k. education data, being data with which the financial support for the funding of education can be established;
l. pension data, being data with which pension entitlements can be established;
m. reintegration data, being exclusively the data with which it can be established if reintegration obligations have been imposed on a person and whether or not they are or are being met;
n. debt burden data, being data with which any debts of a natural or legal person can be established;
o. social benefit, allowances and subsidy data, being data with which the financial support of a natural or legal person can be established;
p. permits and exemptions, being data with which it may be established for which activities a natural or legal person has requested or has obtained permission;
q. health care insurance data, being exclusively the data with which it can be established if a person is insured for the Healthcare Insurance Act.

SyRI application flowchart

4.18. In the explanatory memorandum to the SUWI Decree the procedural steps for the application of SyRI are depicted in a flowchart – see below – with references to the relevant provisions in the SyRI legislation:



The request for application of SyRI, advice of LSI and duration of SyRI project

4.19. The Minister processes the data, referred to in Section 64 subsection 2 SUWI Act, if i) the request of the collaborative alliance within the meaning of the SUWI Decree meets the conditions in the SUWI Decree and ii) the prioritisation shows that there is sufficient capacity available for linking the records in SyRI and for the analysis of the ensuing results (Article 5a.1 paragraph 1 in conjunction with Articles 5a.2 and 5a.3 SUWI Decree).

4.20. A request to apply SyRI must meet the following conditions. The request must in any event show which designated government or other bodies work together on a concrete project (the SyRI project), what the concrete objective of this collaboration is, and how the collaboration is organised and structured. The intended start date and duration of the SyRI project must also be stated in the request (Article 5a.1 paragraph 2 under a SUWI Decree).

4.21. According to the SUWI Decree, a SyRI project is a project that gathers information with the aid of SyRI for the objective of that project and which is in line with the purpose as stated in Section 64 subsection 1 SUWI Act (Article 1.1 under dd SUWI Decree).

4.22. The request must also determine which concrete data will be provided by the participating government or other bodies, the intended manner of feedback on the risk reports by the Minister, and to which indicators and which risk model the request pertains (Article 5a.1 paragraph 2 under b-d SUWI Decree).

4.23. According to the explanatory memorandum to the SUWI Decree, the indicators and the risk model to be applied must be identified clearly and without this specification linking data records could lead to a "fishing expedition" and even arbitrariness. According to the Minister, this method does justice to the principle of "select before you collect". According to the SUWI Decree, an indicator is any information that makes the presence of a particular circumstance plausible. Risk

model is taken to mean a model consisting of predetermined indicators and which indicates whether there is an increased risk of unlawful use of government funds and government schemes in the area of social security and income-dependent schemes, taxes and social security fraud or non-compliance with labour laws (Article 1.1. under y, Article 1.1. under aa SUWI Decree, respectively).

4.24. Up till now the Social Affairs and Employment Inspectorate has had at its disposal one risk model that it has validated, namely the neighbourhood-oriented approach (*wijkgerichte aanpak* – WGA).[10] At the hearing the State explained that it has been working on the development of a risk model for certain companies and an address-related risk model. According to the explanatory memorandum to the SUWI Decree, in due course the intention is to create the opportunity for the application of a risk model specifically designed for a particular SyRI project.

4.25. The government or other bodies participating in the collaborative alliance assess individually whether there is a need for data supply. To this end, the participants in the collaborative alliance must demonstrate that within their respective organisations approval has been obtained to participate in the SyRI project. Insofar as a participant in the collaborative alliance has at its disposal the necessary data within the meaning of Section 64 subsection 2 SUWI Act it must also be proved that it has been assessed beforehand which data are necessary for the risk analyses in relation to the specific purpose of the SyRI project. The participants must also have substantiated separately that potential harm to the interests of natural or legal persons to whom or which the processing of data pertains is not disproportionate and is in proportion to the purpose of the application of SyRI. Only data that are necessary for the performance of risk analyses may be issued, where a less invasive manner cannot reasonably be applied to serve the purpose of the application of SyRI. All of this must also be made clear in the request (Article 5a.1 paragraph 4 SUWI Decree).

4.26. The LSI advises the Minister about the application of SyRI in the SyRI project in question. He determines the start date of the SyRI project if the request meets the conditions. He gives notice of this in the Government Gazette (Article 5a.4 paragraph 1 SUWI Decree). A model information letter has been drafted which municipal authorities can use to inform the residents of a neighbourhood beforehand. According to this model, residents are informed which bodies cooperate in the investigation and that only these bodies have access to the residents' data. The model also contains a notification that the team compares information already known to the various bodies. It is also stated how the verification with the help of SyRI is carried out and how a risk report is followed up. A SyRI projects ends as soon as the feedback from the government or other bodies participating in the collaborative alliance has been submitted, or when the Minister decides to terminate the project (Article 5a.4 SUWI Decree).

Data processing

4.27. After the Minister has established that the request to apply SyRI meets the conditions, a so-named kick-off meeting between collaborative alliance and the processor is held before the start of the SyRI project. At that meeting the collaborative alliance receives information and instructions about, among other things, the manner in which the records have to be submitted and the security level to be applied.

4.28. The Benefits Intelligence Agency Foundation (*Stichting Inlichtingenbureau*, hereinafter: IB) has been designated as processor and for linking the records in SyRI (Article 5a.2 SUWI Decree in conjunction with Article 5.24 SUWI Decree). Pursuant to Section 63 SUWI Act, the IB has been designated as the organ that is responsible for the coordination and service provision for municipal authorities in the area of exchanging data between the UWV, the Centre for Work and Income (*Centrum voor Werk en Inkomen* – CWI) and municipal authorities and the use, structure and maintenance of the required electronic infrastructure, Suwinet.[11] As processor, the IB is charged with, among other things, the collation, pseudonymisation (meaning: data encryption in a dataset

so that the data are no longer directly traceable to an individual), checking the encrypted records against the risk model and decryption after the assessment.

4.29. Data processing takes place in two phases: processing (phase 1) and analysis (phase 2). In the first phase the IB collates the records and pseudonymises them. Personal names and company names, citizen service numbers and addresses are among the data that are replaced with a code (a pseudonym). The processor then applies the first step in the risk selection to the encrypted data: the source file is checked against the risk model with all indicators in an automated manner. This generates potential hits. A potential hit is a hit that indicates an increased risk of fraud. The IB also creates a key file specifying which personal name or company name, citizen service number or address belongs to which pseudonym. When based on the risk model certain natural persons, legal persons or addresses are flagged as an increased risk, they are decrypted with the key file. All data related to these increased risks, except for the key file, are then forwarded to the Minister for the second phase of risk analysis by the analysis unit of the Social Affairs and Employment Inspectorate. The IB destroys any SyRI project files still in its possession within four weeks from forwarding the data to the Minister. The destruction is laid down in an official report.

4.30. In the second phase the decrypted data are analysed more closely by the analysis unit of the Social Affairs and Employment Inspectorate. The data are assessed on their worthiness of investigation. This results in a definitive risk selection. The Minister submits the risk reports on the basis of the definitive risk selection.

4.31. If a natural or legal person with an increased risk does not form the subject of a risk report, his or her data are destroyed within four weeks from completion of the analysis. The Minister destroys any remaining data following feedback from the participants in the collaborative alliance no later than two years following the start of the SyRI project. The destruction of the data is laid down in an official report. This order for destruction does not cover data in the risk reports register, to which a retention period of two years following the registration of the risk report applies (Section 65 subsection 5 SUWI Act).

Feedback on results of risk reports

4.32. The use of risk reports must be communicated to the Minister with the intention of increasing the effectiveness of the risk model. The feedback must in any event consist of the outcome of the risk reports, a substantiation if risk reports have not been followed up on and feedback on the usability of the risk reports. Pursuant to Article 5a.6 SUWI Decree, the Minister is obliged to evaluate the risk model based on the feedback received. Based on the feedback the risk model that is applied to the record linkage and analysis phase may, if required, be adjusted by the analysis unit of the Social Affairs and Employment Inspectorate.

Supervision

4.33. The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, hereinafter: AP, previously Cbp) has been designated as the supervisory body in the Netherlands within the meaning of the GDPR and as an external privacy authority monitors compliance with the SyRI legislation.[12]

5 The dispute

5.1. NJCM et al. claims that the court – in a judgment that is provisionally enforceable as far as possible:

I. rule that applying Sections 64 and 65 SUWI Act and Chapter 5a SUWI Decree is incompatible with higher-order law, in particular with Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter: ECHR), Article 7 and 8 of the Charter of Fundamental Rights of the European Union (hereinafter: Charter) and/or Article 17 of the International Covenant on Civil and Political Rights (hereinafter: ICCPR); and/or Article 6 and/or Article 13 ECHR; and/or Article 5, 6, 13, 14, 22 and/or 28 GDPR, or at least the corresponding

sections in the Wbp Act, or alternatively,

II. rule that applying the following parts of the SUWI Act and SUWI Decree is incompatible with higher-order law, in particular with Article 8 ECHR, Article 7 and 8 Charter and/or Article 17 ICCPR; and/or Article 6 and/or Article 13 ECHR; and/or Article 5, 6, 13, 14, 22 and/or 28 GDPR, or at least the corresponding sections in the Wbp Act:

a. a) the purpose clause as contained in Section 64 subsection 1 SUWI Act; and/or

b) the formulation of authorities for data processing and the application of SyRI as contained in Section 64 subsection 3 and Section 64 subsection 4 SUWI Act; and/or

c) the enumeration of categories of personal data as contained in Article 5a.1. paragraph 3 SUWI Decree; and/or

d) the practice of confidentiality of risk models used in the application of SyRI; and/or

e) the regulations pertaining to the risk reports register as contained in Article 5a.5 SUWI Decree); and/or

f) the State's substantiation of the necessity of SyRI; and/or

g) the regulations under which individual administrative organs are ordered to substantiate that the data supply in the context of a SyRI project is proportional and proportionate as contained in Article 5a.1 paragraph 4 SUWI Decree, and thereby failing to ensure that a sufficient, overarching review of these requirements takes place; and/or

h) the regulations under which parties involved are only informed about the processing of their personal data in SyRI if they are the subject of a risk report, and only upon request, as contained in Article 5a.5 SUWI Decree; and/or

i. i) the regulations pertaining to the monitoring of the application of SyRI, in particular the fact that the Minister is the only party monitoring the application of SyRI;

III. rule that processing personal data in the context of, with the use of and/or for the benefit of the application of SyRI, in particular the mutual exchange of personal data by administrative organs (including the Tax and Customs Administration), the issuance of personal data to the Minister (including by the Tax and Customs Administration), the provision of personal data to the IB, the processing of personal data by the IB, including profiling, the provision of personal data by the IB to the Minister, submitting risk reports and/or including report and information on such reports in the risk reports register, is unlawful because such processing constitutes a violation of Article 8 ECHR, Article 7 and 8 Charter and/or Article 17 ICCPR; and/or Article 6 and/or Article 13 ECHR; and/or Article 5, 6, 13, 14, 22 and/or 28 GDPR and/or the corresponding sections in the Wbp Act;

IV. render inoperative Articles 64 and 65 SUWI Act and Chapter 5a SUWI Decree, or at least the parts thereof the court deems incompatible with higher-order law pursuant to claim I and/or II, or at least the parts thereof the court reasonably deems incompatible with higher-order law in the proper administration of justice, or at least declare that they have no binding effect, or declare that these must not be applied, subject to the possible imposition of a condition if required;

V. rule that the State is acting contrary to the duties of confidentiality to which the Tax and Customs Administration is subject, because the Tax and Customs Administration provides personal data to other parties in collaborative alliances pursuant to Section 64 SUWI Act and to the Minister in the context of SyRI;

VI. order the State to disclose the risk models and risk indicators used in the projects G.A.LO.P. II and Capelle;

VII. rule that the processing of personal data by the IB is unlawful due to the absence of a

processing agreement within the meaning of Article 28 paragraph3 GDPR and/or Section 14 subsection 2 Wbp Act;

VIII. prohibit the State to process personal data, or at least personal data of [claimant sub 6] and [claimant sub 7] in the context of, with the use of and/or for the benefit of the application of SyRI;

IX. to order the State to irreversibly destroy all personal data collected in the context of, with the use of and/or for the benefit of the application of SyRI and to furnish proof of this destruction to NJCM et al.;

ordering the State to pay the costs of these proceedings, plus statutory interest from 14 days following the date of the judgment.

5.2. NJCM et al. bases its claims on unlawful acts of the State. According to NJCM et al. Sections 64 and 65 SUWI Act and Chapter 5a SUWI Decree, or at least their application, are contrary to provisions of international treaties binding on all persons. Moreover, the State (the Tax and Customs Administration) acts contrary to its statutory duties of confidentiality under national law by providing personal data pursuant to SyRI legislation to the third parties identified above by NJCM et al., and contrary to the GDPR because the IB processes data in SyRI without a processing agreement.

5.3. The State opposes the claims.

5.4. The arguments of the parties are discussed in more detail below, insofar as relevant.

6 The assessment

Introduction

6.1. With these proceedings, NJCM et al. aims to call a 'halt' to the use of SyRI. NJCM et al. believes that SyRI constitutes a breach of human rights. At the hearing NJCM et al. explained that its main aim is for the SyRI legislation to be declared as having no binding effect. According to NJCM et al. the SyRI legislation constitutes an invasion of a person's privacy, in particular the right to respect for private life. NJCM et al. deems the SyRI legislation as not having sufficient safeguards.

The State contests this. It puts forward that the SyRI legislation is based on objective criteria and contains procedural and substantive safeguards which, or so the State argues, prevents abuse and limits the invasion of private life caused by the application of SyRI to the minimum necessary.

6.2. The court must review whether or not the SyRI legislation is in breach of provisions of international and European law binding on all persons. In this context NJCM et al. has first and foremost argued a violation of Article 8 ECHR, Articles 7 and 8 Charter and Article 17 ICCPR and also a violation of Articles 5, 6, 13, 14, 22 and/or 28 GDPR.

6.3. The starting point is that social security is one of the pillars of Dutch society and contributes to a considerable extent to prosperity in the Netherlands. This is also endorsed by NJCM et al. The social security system can only function if citizens in the Netherlands who are not eligible for such facilities do not make use of them. The system is financed with public money and fraud affects the solidarity underlying the system. Combating fraud is therefore key to maintain citizen support for the system, as argued by the State and as is intended with the SyRI legislation.

6.4. New technologies – including digital options to link files and analyse data with the help of algorithms – offer (more) possibilities for the government to exchange data among its authorities

in the context of their statutory duty to prevent and combat fraud. The court shares the position of the State that those new technological possibilities to prevent and combat fraud should be used. The court is of the opinion that the SyRI legislation is in the interest of economic wellbeing and thereby serves a legitimate purpose as adequate verification as regards the accuracy and completeness of data based on which citizens are awarded entitlements is vitally important.

6.5. However, the development of new technologies also means that the right to the protection of personal data increasingly gains in significance. The existence of adequate statutory privacy protection in the exchange of personal data by government or other bodies contributes to citizens' trust in the government, as much as preventing and combating fraud do. As NJCM et al. correctly observes, it is plausible that a 'chilling effect' occurs in the absence of sufficient and transparent protection of the right to respect for private life. Without trust in sufficient privacy protection, citizens will be less likely to be willing to provide data or there will be less support for doing so.

6.6. Pursuant to Article 8 ECHR the Netherlands as a party to the ECHR has 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. From the viewpoint of protection of the right to respect for private life, which includes the protection of personal data, legislation must offer a sufficiently effective framework which allows the weighing of all interests in question in a transparent and verifiable manner. Under the legislation all persons should be able to have the reasonable expectation that their private life is sufficiently respected when SyRI is applied. The court holds that the SyRI legislation does not meet this requirement.

6.7. The SyRI legislation does not meet the requirement laid down in Article 8 paragraph 2 ECHR that interference with the exercise of the right to respect for private life is necessary in a democratic society, meaning that it should be necessary, proportionate and subsidiary in relation to the intended purpose. The court weighs the substance of the SyRI legislation in light of the aims the legislation pursues against the violation of private life by the SyRI legislation. The court is of the opinion that the legislation does not strike the 'fair balance' required under the ECHR between the social interest the legislation serves and the violation of private life to which the legislation gives rise to qualify as a sufficiently justifiable violation of private life. The court takes into consideration the fundamental principles underlying the protection of data under Union law (the Charter and the GDPR), specifically the principles of transparency, purpose limitation and data minimisation. The court holds that the legislation pertaining to the application of SyRI is insufficiently transparent and verifiable. For this reason, the court declares in this judgment that Section 65 SUWI Act and Chapter 5a SUWI Decree have no binding effect, being contrary to Article 8 paragraph 2 ECHR.

6.8. The court will explain below on which grounds it has arrived at its opinion.

Admissibility and procedural status of FNV

6.9. First of all, the court must review of its own motion whether or not the claims of each of the claimants are admissible. The State has taken the position that the claims of Koepel van DBC-Vrije Praktijken, [claimant sub 6] and [claimant sub 7] are inadmissible.

6.10. It is not in dispute that the NJCM, Platform Bescherming Burgerrechten, Privacy First and Koepel van DBC-Vrije Praktijken are civil society interest groups within the meaning of Book 3 Section 305a of the Dutch Civil Code. According to their articles these parties to the proceedings are authorised to promote the interests of their support base at law. In the case of the NJCM that support base consists of persons or groups whose fundamental human rights have been violated. The support base of Platform Bescherming Burgerrechten consists of a network of organisations, groups and persons that converge on, among other things, striving for an improved safeguarding and strengthening of civil rights in the Netherlands, in particular the right to privacy

and, in the case of Privacy First, all citizens of the Netherlands. The support base of Koepel van DBC-Vrije Praktijken consists of psychotherapists and psychiatrists of DTC-free practices and their patients/clients. These claimants also effectively promote the interests of this support base.

6.11. The court also holds that the legal claims in these proceedings seek to protect the interests of the support base of these four claimants. All identified civil society interest groups promote the protection of fundamental human rights in general, or the right to privacy in particular.

6.12. Since the NJCM, Platform Bescherming Burgerrechten and Privacy First promote the general interest, the court deems that the claims of these organisations are admissible.

6.13. Koepel van DBC-Vrije Praktijken promotes the interest of a group of persons who interests can be individualised, namely the interest of patients/clients of psychotherapists, psychiatrists and psychologists. The court rejects the defence of the State that the claims of Koepel van DBC-Vrije Praktijken are inadmissible. The court deems the concrete interest of Koepel van DBC-Vrije Praktijken in its claims as sufficiently factually explained. The data that can be processed in SyRI, such as reintegration data with a view to establishing an entitlement, may pertain to the group of patients/clients whose interests Koepel van DBC-Vrije Praktijken seeks to defend. In the context of admissibility the court does not deem it of decisive importance, as argued by the State, that no medical data may be processed in SyRI. Such a concrete interest is not required for establishing admissibility in this case. The claims of Koepel van DBC-Vrije Praktijken are therefore also admissible.

6.14. The State has not challenged the admissibility of the claims of Landelijke Cliëntenraad. The court acknowledges that considering the interests it promotes, as evidenced by the SUWI Act and its standing orders, Landelijke Cliëntenraad has an interest in the outcome of these proceedings. However, Landelijke Cliëntenraad is a consultative body without legal personality. No authorised natural persons appear in these proceedings on its behalf. Nor is it evident that there is another legal basis conferring capacity to bring legal proceedings on Landelijke Cliëntenraad. Neither the SUWI Act nor regulations based on this act show that Landelijke Cliëntenraad has a legal status comparable to that of representative bodies, such as a works council pursuant to the Works Councils Act, or a client council pursuant to the Participation (Clients of Care Institutions) Act. These are organs that, given their tasks, have the capacity to bring legal proceedings based on specific legal grounds. The standing orders also do not furnish evidence for this. Unlike NJCM et al. argues, the court therefore sees no basis for an analogous application of that legislation. In light of this the court declares the claims of Landelijke Cliëntenraad inadmissible.

6.15. The court also holds that the claims of [claimant sub 6] and [claimant sub 7] are inadmissible. NJCM et al. has not factually explained that in the case of these claimants there are concrete reference points from which it may follow that data pertaining to them form part of processing in SyRI. [claimant sub 6] and [claimant sub 7] are, among other things, authors and columnists and citizens of the Netherlands. They have serious concerns about the application of SyRI by the government. In these proceedings they have not furnished facts proving or making a plausible case for the existence of a possible concrete connection between their private lives, including possibly their professional activities, and data processing in SyRI. For a sufficiently concrete and personal interest within the meaning of Book 3 Section 303 Dutch Civil Code the court deems insufficient the mere possibility of an abstract review whether the SyRI legislation violates Article 8 ECHR and the circumstance that pursuant to the SyRI legislation the personal data of 'all persons' – insofar as they belong to one of the categories of Article 5a.1 paragraph 3 SUWI Decree – could potentially form part of a SyRI project.

6.16. The foregoing means that the court declares that the claims of Landelijke Cliëntenraad, [claimant sub 6] and [claimant sub 7] inadmissible. The claims of the other claimants, namely the NJCM, Platform Bescherming Burgerrechten, Privacy First and Koepel van DBC-Vrije Praktijken are admissible.

6.17. As regards the procedural status of FNV, the court would like to note that FNV has intervened to join the claimants' proceedings. FNV has not submitted claims against the State on or of its own. The decisions of the court in the operative part therefore do not pertain to any legal claim of FNV.

6.18. In view of the above insofar as the court refers to NJCM et al. below, it only refers to the four claimants whose claims have been declared admissible, and FNV.

General assessment framework

6.19. The subject under discussion is whether the SyRI legislation unlawfully violates the right that protects privacy. In this context the court will first discuss the general assessment framework it uses, followed by the protection of human rights under the ECHR, the Union law protection offered by, among other things, the Charter and the GDPR, and finally the interrelationship of the ECHR and Union law and the arguments between the parties to these proceedings.

Protection of human rights

6.20. The right to respect for privacy is a fundamental human right protected in international law in Article 8 ECHR and Article 17 ICCPR. These are provisions that are binding on all persons and which the court must apply pursuant to Articles 93 and 94 of the Constitution.

6.21. Article 8 paragraph 1 ECHR stipulates that everyone has the right to respect for his private and family life, his home and his correspondence. Interference of the government with the exercise of this right is only permitted, according to Article 8 paragraph 2 ECHR, in accordance with the law and when necessary in a democratic society in the interests of national security, public safety or the economic wellbeing 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. Seeing as Article 17 ICCPR, which offers the same protection of private life as Article 8 ECHR, has no independent significance in this case, the court will not discuss it further.

6.22. Considering that the Netherlands, as a party to the ECHR, is also bound to the jurisdiction of the European Court of Human Rights (hereinafter: ECtHR; see Article 32 ECHR), the court must proceed from the ECtHR's interpretation of Article 8 ECHR, or independently interpret this provision with the application of the interpretation criteria of the ECtHR.

6.23. Over time the ECtHR has brought various interests under the umbrella of private life, thereby bringing them under the protection of Article 8 ECHR. The right to respect for private life also protects the right to personal autonomy, personal development and self-determination and the right to establish relations with other human beings and the outside world. According to the ECtHR the principles of human dignity and human freedom constitute 'the very essence of the Convention'.[13] Together with the notion of personal autonomy, they play an important role in determining the scope of the right to respect for private life.

6.24. The right to a personal identity and the right to personal development have also been identified by the ECtHR as aspects of the right to respect for private life. Furthermore the right to a personal identity is closely related to the right of protection of personal data. Finally, the right to respect for private life in the context of data processing concerns the right to equal treatment in equal cases, and the right to protection against discrimination, stereotyping and stigmatisation.

6.25. The right to protection of personal data has not been laid down as a distinct right in the ECHR. According to the case law of the ECtHR the right to protection of personal data does in general terms have fundamental significance for the right to respect for private life.[14]

6.26. The court follows the parties to these proceedings in taking as a starting point that the SyRI legislation impacts private life and consequently falls within the scope of the protection of Article 8

ECHR. The legislator also takes as a starting point that data supply for the benefit of a collaborative alliance and the application of SyRI as stipulated in Sections 64 and 65 SUWI Act constitute an interference with the exercise of the right to respect for private life. The legislator expressly reviewed the legislative proposal against the requirements of Article 8 ECHR, Article 10 of the Constitution and the then applicable Wbp Act, and did not regard it as violating them.

Protection under Union law

6.27. Under Union law the right to protection of personal data as a distinct right is primarily laid down in the Charter and in the Treaty on the Functioning of the European Union (TFEU). Under Article 7 Charter everyone has the right to respect for his or her private and family life, home and communications. Article 8 Charter and Article 16 TFEU stipulate that everyone has the right to protection of personal data. Article 8 Charter also contains a further explanation of this right, namely that such data must be processed fairly, for specified purposes and on the basis of the consent of the data subject or some other legitimate basis laid down by law. It also specifies that everyone has the right of access to collected data concerning them, and the right to rectification and that an independent authority monitors compliance with these rules.

6.28. Before 25 May 2018 the protection of data was generally laid down in European secondary legislation in Directive 95/46[15], which at the national level was implemented in the Wbp Act. The GDPR applies as of 25 May 2018, after the summons was issued. As an EU regulation, the GDPR is binding in its entirety and directly applicable. The European legislator did not provide for transitory provisions in the GDPR. The court must assess the claims of NJCM et al. under the law as it currently stands. Considering the nature of the GDPR – as an EU regulation with precedence and direct effect – and the review the court must carry out, this is not altered by the fact that in Section 48 subsection 10 General Data Protection Regulation (Implementation) Act (hereinafter: UAVG) the Dutch legislator has stipulated that claims submitted to the court at the time the UAVG entered into force are subject to the law in force before said act entered into force. This provision must not be applied in this case.

6.29. By using a Regulation as the legal instrument of choice, the European legislator underlined the relevance that at the European level importance is attached to a careful handling of personal and other data. The protection of data in the Netherlands under the GDPR is therefore in principle exhaustive. At the same time the GDPR leaves room in parts for national legislation. Insofar as that is the case, the UAVG applies. The GDPR has strengthened existing rights of individuals whose data are processed (hereinafter also: the data subject), such as the requirement of consent of the data subject as a basis for processing data (Articles 6, 7 and 8 GDPR). New rights have been laid down in law, such as the right to be forgotten, the right to data portability and the right not to be subject to profiling (Articles 17, 20 and 22 GDPR). Unlike Directive 95/45, the GDPR also contains the obligation for the controller to take account of the risks of varying likelihood and severity for the rights and freedoms of natural persons when processing data (Article 24 GDPR). Using a data protection impact assessment it must be demonstrated that the regulation's requirements have been met by implementing measures, safeguards and mechanisms to limit that risk (Article 35 GDPR).

6.30. The GDPR has established several principles as regards the processing of personal data (see the recitals in conjunction with Article 5 GDPR). These are the principle of transparency, the principle of purpose limitation, the principle of data minimisation, the principle of accuracy and the principle of integrity and confidentiality and finally, as a corollary of these principles, the principle of accountability. These principles are explained in more detail in the other provisions of the GDPR.

6.31. The principle of transparency requires easily accessible and easy to understand information, communication and clear and plain language, and the provision of information to the data subject about the identity of the controller and the purposes of the data processing. Aside from this, under this principle, further information must actively be provided to ensure a sound and transparent data processing, and natural persons must be made aware of the risks, rules, safeguards and

rights in relation to the processing of personal data and also of how they may exercise their rights with respect to the processing.

6.32. The principle of purpose limitation means that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

6.33. The principle of data minimisation requires personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. As also follows from the principle of storage limitation laid down in the GDPR, not more personal data may be kept for longer than is necessary for the purpose for which the personal data are processed.

6.34. Pursuant to the principle of accuracy, the controller must take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay. The principle of integrity and confidentiality means that personal data are processed in a manner that ensures appropriate security of the personal data by using appropriate technical or organisational measures. Finally, the GDPR obliges the controller is responsible to comply with the above principles. This principle is known as the principle of accountability.

6.35. The GDPR also contains provisions on profiling and a ban on automated individual decision-making, including profiling. Article 4 point 4 GDPR defines profiling 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. Pursuant to Article 22 GDPR there is a general ban on fully automated individual decision-making, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her. Exceptions may apply and if one of them does apply, measures must be taken to safeguard the rights and freedoms and legitimate interests of the data subject.

6.36. The guidelines of the Article 29 Data Protection Working Party[16] state that the threshold for "significance" must be similar to that of a decision producing a legal effect for the data subject. According to the guidelines, for data processing to significantly affect someone the effects of the processing must be sufficiently great or important to be worthy of attention. The decision must have the potential to significantly affect the circumstances, behaviour or choices of the data subjects; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals.

Interrelationship ECHR and Union law and the arguments between the parties

6.37. The ECHR provides for a minimum level of protection of the fundamental right to respect for private life. The substance and scope of the EU fundamental rights in the Charter are the same as those of the ECHR rights, insofar as the Charter contains rights that correspond with the ECHR (Article 52 paragraph 3 Charter). The rights safeguarded by the ECHR also form part of Union law as general principles (Article 6 paragraph 3 TFEU). Therefore, as regards Union law, there is at least the same minimum level of protection as in the ECHR. However, Union law may provide more extensive protection (Article 52 paragraph 3 Charter). Under the Charter and the GDPR, the protection of EU citizens' right to protection of personal data is specified in more detail and in some instances extends beyond the protection under the ECHR.

6.38. The focal point of the arguments of NJCM et al. is the alleged violation of Article 8 ECHR, as confirmed by NJCM et al. at the hearing and as understood by the State. The debate between the parties therefore focuses on the questions whether the SyRI legislation meets the conditions Article 8 paragraph 2 ECHR lays down for restrictions of the right to respect for private life.

6.39. As follows from its arguments NJCM et al., and from the defence of the State, that Articles 7 and 8 Charter provide the same minimum protection as Article 8 ECHR in terms of their substance and scope.

6.40. The arguments of NJCM et al. and the defence of the State also imply, conversely, that the minimum protection of Article 8 ECHR also entails 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. The State has not taken the position – and in the opinion of the court correctly so – that the court is only able to review the SyRI legislation against these principles if and insofar as this legislation meets the conditions the ECHR lays down for restrictions of the right to respect for private life.

6.41. The court will take into account the aforementioned general principles of data protection from the Charter and the GDPR in its review of whether the SyRI legislation meets the requirements of Article 8 ECHR. In other words: the court will also interpret Article 8 paragraph 2 ECHR on the basis of these principles. There are no indications to assume that the minimum level of protection of the right to respect for private life, including the protection of personal data under the ECHR, is less extensive than the data protection offered by the Charter and the GDPR under the general principles laid down in these instruments.

The alleged violation of Article 8 ECHR

6.42. As has been stated before, it is not in dispute that collaboration for the benefit of data exchange and the application of SyRI, as laid down in the SyRI legislation, constitute an interference with the exercise of the right to respect for private life. The court must review, considering the debate between the parties, whether or not the SyRI legislation meets the requirements of Article 8 paragraph 2 ECHR to justify that interference.

6.43. Before commencing its assessment, the court would like to note that its duty is not to establish as it sees fit the value or social significance that should be attached to the interests in question. Moreover, considering the nature of the legislative function and the position of the court, the court must show restraint during the assessment.[17] However, this does not mean that the SyRI legislation must be assessed marginally. As has also been argued by NJCM et al., the court will not assess the amended legislation marginally, but fully against Article 8 paragraph 2 ECHR.

6.44. The court will first discuss the extent and seriousness of the interference with the right to respect for private life, which occurs or may occur when SyRI is applied. This interference is coloured by the answer to the question what precisely SyRI is. The positions of the parties on this point are widely divergent. It is also in dispute between the parties how to legally interpret the submission of a risk report, namely whether this constitutes profiling and automated individual decision-making within the meaning of the GDPR. The answer to this question also determines the extent and seriousness of the interference with private life when SyRI is applied. In summary, the court has arrived at a number of starting points for its further assessment. The court subsequently discusses whether or not SyRI legislation meets the requirement that interference must be 'in accordance with the law' and necessary in a democratic society in relation to the intended aims of the legislation.

Extent and seriousness of the interference: what is SyRI? Dragnet, untargeted approach, data mining, 'deep learning', 'big data'?

6.45. According to NJCM et al. the application of SyRI constitutes a dragnet, untargeted approach in which personal data are collected for investigation purposes. It argues that SyRI is a digital tracking system with which citizens are categorised in risk profiles and in the context of which the State uses 'deep learning' and data mining. According to NJCM et al., SyRI is a proactive system with a large-scale, unstructured and random automated linking of files of large groups of citizens

and secret processing of personal data. NJCM et al. also argues that the application of SyRI falls under what is referred to in literature, legal literature and in practice as 'big data'.

6.46. To substantiate its position, NJCM et al. has relied on, inter alia, an "Independent advisory opinion on the effects of digitisation on constitutional relations", as submitted by the Advisory Division of the Council of State (hereinafter: the Advisory Division) to the cabinet.[18] In the advisory opinion, the Advisory Division notes that in actual practice 'big data' generally refers to large amounts of data sets that are so large or complex that they cannot be processed by customary systems, and at the same time are derived from various sources. The Advisory Division noted the following in its opinion on SyRI by way of example:

"**Profiling as example**
The potential hazards in using large data sets are best illustrated with profiling to identify persons posing an increased risk. After all, this could lead to the situation where general characteristics are attributed to an individual.

(…)

In 2014 the Division issued an advisory opinion on the introduction of the *Systeem Risico Indicatie* [SyRI]. That system enabled the Ministry of Social Affairs to run different types of files containing data of citizens against each other in order to detect taxes or social benefits fraud. This is in line with the use of deep learning and self-learning systems, which after all are focused on investigating as many links as possible without preconceived notions. The downside is that such data may constitute a serious interference with a person's privacy. The enumeration of data is so wide that it is difficult to think of personal data that would not fall under it. The list appears not to seek limitation, but rather to create the widest possible reach."

And:

"**Deep learning – self-learning systems**
The Tax and Customs Administration is at the forefront of the application of deep learning techniques: it has huge amounts of data on persons in the Netherlands and plays a pivotal role in many collaborative alliances, such as those of the *Systeem Risico Indicatie* [SyRI]. In addition, some municipalities use algorithms to select possible cases of social assistance benefit fraud. The algorithm reads all sorts of data, such as dates of birth, family composition, benefit history and data of the Tax and Customs Administration, the Land Registry and the National Vehicle and Driving Licence Registration Authority. (…)

The term "self-learning" is confusing and misleading: an algorithm does not know and understand reality. There are predictive algorithms which are fairly accurate in predicting the outcome of a court case. However, they do not do so on the basis of the substantive merits of the case. They can therefore not substantiate their predictions in a legally sound manner, while that is required for all legal proceedings for each individual case. (…)

The reverse also applies: the human user of such a self-learning system does not understand why the system concludes that there is a link. An administrative organ that partially bases its actions on such a system is unable to properly justify its actions and to properly substantiate its decisions."

6.47. In its defence, the State has argued that when using SyRI, only data from existing data sets of designated government or other bodies are compared in order to identify discrepancies with a view to checking the entitlements of the data subject. With reference to statements made by the Minister[19] the State argues that files of existing, factual data are compared. The factual data are compared to each other with the aid of a simple decision tree.

6.48. Responding to reliance of NJCM et al. on the aforementioned independent advisory opinion of the Advisory Division, the State has referred to the reaction of the cabinet to this opinion. The State Secretary for the Interior and Kingdom Relations stated the following in that reaction:

"The Division has also described risks regarding the digital linking of data in various contexts. One example of data linking is SyRI (*Systeem Risico Indicatie*). Contrary to what the Division assumes SyRI is not a deep learning application nor is it a self-learning system. SyRI is emphatically not a tool to predict whether or not an individual could commit an offence. SyRI compares files containing existing, factual data of the parties designated under Section 64 of the Work and Income (Implementation Organisation Structure) Act (SUWI), such as the UWV, the SVB, the Municipal Executives, the Tax and Customs Administration and the Social Affairs and Employment Inspectorate in order to assess whether there are discrepancies in the data. If the mutual comparison following assessment against the risk model shows a discrepancy, this discrepancy must be examined by one or more of said parties before a decision may be taken that may have legal consequences for the data subject."[20]

6.49. The court finds that it is unable to assess the correctness of the position of the State of the precise nature of SyRI because the State has not disclosed the risk model and the indicators of which the risk model is composed or may be composed. In these proceedings the State has also not provided the court with objectively verifiable information to enable the court to assess the viewpoint of the State on the nature of SyRI. The reason the State gives for this is that citizens could then adjust their conduct accordingly. This is a deliberate choice of the State. That choice also coincides with the starting point of the legislator regarding the provision of information on SyRI. The SyRI legislation does not show how the decision model of SyRI functions and which indicators are or can be used in a SyRI project (see 4.23 above for the terms decision model and indicators), i.e. which factual data make or can make the presence of a certain situation plausible.

6.50. The court also finds that, unlike NJCM et al. argues, the SyRI legislation does not provide room for unstructured ('ad random') data collection with the use of SyRI. The number of data categories that can be used is extensive, but still enumerated exhaustively. On the other hand, the amount of data that can be used in the application of SyRI is substantial. A total of 17 data categories of various types qualify. Each separate category can be deemed to encompass a large amount of data. Depending on the specific SyRI project, there may be large amounts of structured data sets from various sources.

6.51. It is also found that in the application of SyRI links between data are established. This is because existing and new files are compared to each other with a view to producing potential hits, which are indicative of an increased risk. The SyRI legislation furthermore leaves the option open that in the application of SyRI use is made of predictive analyses, 'deep learning' and data mining. The definition of risk model in the SUWI Decree does not preclude this. The SyRI legislation furthermore expressly provides for the option to adjust a risk model based on an evaluation, while new risk models with new indicators can also be developed (see also 4.24). Therefore the court is of the opinion (concurring with the Advisory Division, see above in 6.46) that the application of SyRI "is in line" with 'deep learning' and self-learning systems. To this extent the court endorses NJCM et al. This does not alter the fact that the court, considering the communications of the government members to the House of Representatives, accepts as a factual assumption that *in the implementation* of the SyRI legislation no use is made at this point in time of 'deep learning' and data mining in the application of SyRI, as argued by NJCM et al.

6.52. The court also concurs with NJCM et al. to the extent that when SyRI is applied, use is made of 'big data' within the meaning of the opinion of the Advisory Division. However, there is no clear-cut definition of that term. The court deems it irrelevant to its further assessment whether or not the processing of data in SyRI should be qualified as a form of 'big data'.

6.53. As regards the use of risk profiles, a distinction must be made between *the development* of risk profiles on the one hand, and *their use* on the other. The court assumes that in the implementation of the SyRI legislation no risk profiles based on file linkages are currently being developed. This, as put forward by the State, in response to the references of NJCM et al. to the aforementioned Waterproof and 'black box' projects. The court is unable to find whether risk profiles are truly not

being developed with the aid of file linkage (see, for comparison, 6.49). However, the court deems it to be inherent in SyRI as an instrument, considering the purposes for which data are processed in SyRI and in light of the definitions of the terms risk model and risk indicator, that use is made of risk profiles based on existing factual data when SyRI is used.

6.54. Finally, there is the situation that the SyRI legislation does not provide for a duty of disclosure to those whose data are processed in SyRI so that these data subjects can be reasonably assumed to know that their data are or have been used for that processing. The SyRI legislation also does not provide for an obligation to notify the data subjects individually, as appropriate, that a risk report has been submitted. There is only a statutory obligation to announce the start of a SyRI project beforehand by way of publication in the Government Gazette and after the processing access to the register of risk reports upon request. The model letter which can be used in practice – as was the case in the Rotterdam Bloemhof & Hillesluis project – is not founded on a statutory obligation to inform the data subjects 'door-to-door', while the court is unable to find based on the available information whether municipalities have a standard practice in the implementation of the act. Data subjects are also not informed automatically afterwards. This only occurs if there is a control and investigation in response to a risk report. This does not happen as a matter of course.

Extent and seriousness of the interference: profiling and automated individual decision-making?

6.55. Now the court arrives at the assessment, in view of the debate between the parties on the extent to which submitting a risk report affects private life, whether or not profiling and automated individual decision-making occur when SyRI is applied.

6.56. It is not in dispute that the file linkage used in a SyRI project meets the definition of profiling within the meaning of Article 4 paragraph 4 GDPR. However, this does not mean that automated individual decision-making within the meaning of the GDPR occurs.

6.57. NJCM et al. argues, and FNV emphatically endorses, that the submission of a risk report by the Social Affairs and Employment Inspectorate can be considered a decision with legal effect, or at least a decision that affects the data subjects significantly in another way, and that this decision is taken on the basis of automated individual decision-making within the meaning of Article 22 GDPR, which is prohibited. According to NJCM et al. there is no meaningful human intervention prior to the submission of a risk report; the mere removal of 'false positives' cannot qualify as such nor can the assessment of the participating parties after receipt of a risk report.

6.58. The State contests that automated individual decision-making occurs and puts forward that in any event no prohibited form of it occurs. The State argues that all exceptions to the prohibition stipulated in the GDPR are met and that the amended legislation contains sufficient safeguards to protect privacy.

6.59. Although the court holds that, contrary to what NJCM et al. argues, the use of SyRI in and of itself is not aimed at having legal effect – whether in private law, administrative or criminal law – a risk report does have a similarly significant effect on the private life of the person to whom the risk report pertains. The court derives that conclusion partially from the guidelines of the Article 29 Data Protection Working Party (see 6.36). A risk report can be stored for two years and can be used by the participants in the SyRI project in question for a maximum of 20 months. In addition, the Public Prosecution Service and the police may be notified of the risk report upon request. The fact that a risk report does not necessarily always lead to further investigation, or to an administrative or criminal-law sanction, and may also not be used as the sole basis for an enforcement decision does not alter the significant effect on the private life of the data subject.

6.60. The court does not give an opinion on whether the exact definition of automated individual decision-making in the GDPR and, insofar as this is the case, one or more of the exceptions to the prohibition in the GDPR have been met. That is irrelevant in the context of the review by the court

whether the SyRI legislation meets the requirements of Article 8 ECHR. However, the court does consider the aforementioned significant effect of the submission of a risk report and its inclusion in the risk reports register on the private life of the data subject a significant factor in its assessment whether the SyRI legislation meets the requirements of Article 8 paragraph 2 ECHR. This effect, too, determines in part the extent to which the SyRI legislation interferes with the right to respect for private life. The court takes into account that part of the right to protection of personal data is the right of everyone to be reasonably able to follow up on their personal data and be informed about the processing of their data. Although the start of a SyRI project is published in the Government Gazette, a risk report may be retained in the register for two years, without this being known to the data subject.

Abstract

6.61. In summary, the court will take the following starting points into consideration in its further assessment. These starting points are relevant to the extent and seriousness of the interference with the private life of the data subjects by the SyRI legislation and are therefore included in the court's review whether this interference is permissible under Article 8 paragraph 2 ECHR.

6.62. The linking of files when SyRI is applied relates to the processing of the data categories as exhaustively listed in the SUWI Decree. The data can be found in files with factual data (personal or other data) which are available to the statutorily designated government or other bodies on the basis of their statutory duty. It involves structured data processing based on existing, available files. Depending on the SyRI project, there may be a set of a large amount of data derived from various sources. During the data processing a risk model is used, which consists of predetermined risk indicators and which gives an indication of whether there is an increased risk of unlawful use of government funds and government schemes in the area of social security and income-dependent schemes, taxes and social security fraud or non-compliance with labour laws.

6.63. There currently are no indications of 'deep learning' or data mining or the development of risk profiles in the implementation of the SyRI legislation. However, the SyRI legislation does provide scope for the development and application of a risk model using 'deep learning' and data mining, and for the development of risk profiles.

6.64. The court does not deem it relevant for its further assessment whether 'big data' plays a role in the processing of data in SyRI, as NJCM et al. argues and the State contests. This term has no clear-cut definition. In any event, a substantial amount of data qualifies for processing in SyRI.

6.65. Moreover, the risk model that is currently being used and the risk indicators constituting this risk model are 'secret'. This also applies to the data used in a concrete SyRI project (which data have been processed in SyRI). The risk model, the indicators and the data that have been concretely processed are not public nor are they known to the data subjects. The SyRI legislation does not provide for an obligation to inform the persons that their data have been processed in SyRI. Nor is there a legal obligation to inform the data subjects individually, as appropriate, that a risk report has been submitted. The court furthermore assumes that a risk report has a significant effect on the private life of the person to whom the report pertains.

In accordance with the law

6.66. The interference with private life in the application of SyRI must be in accordance with the law. According to the case law of the ECtHR this does not need to be an Act of Parliament: this requirement can also be met with any generally binding regulation or even judge-made law. "Some basis in domestic law" is sufficient.[21] The legal basis on which the interference is predicated must, however, be sufficiently accessible and foreseeable. This means that the legal basis must be sufficiently clear so as to enable an individual to regulate their conduct accordingly.[22]

6.67. In support of its argument that the SyRI legislation is unlawful, NJCM et al. mainly relies on the

case law of the ECtHR in matters pertaining to untargeted bulk interception (mass surveillance) or targeted interception of data in a criminal-law or national security context.[23] As follows from the foregoing, this is not the case with the application of SyRI. Therefore, this case law cannot be considered as a one-to-one guidance for the court's assessment.

6.68. The case of *S. and Marper versus the United Kingdom* revolved around the lawfulness of the British Data Protection Act (1998), implementing Directive 95/45 and the guidelines for the use of the Police National Computer on the basis of said act in connection with the retention of fingerprints, cellular samples and DNA profiles. Although the factual context of this case, too, is not comparable with the current proceedings, the judgment contains considerations of the ECtHR on data protection of a more general nature. That makes this judgment relevant to the assessment of the lawfulness or unlawfulness of the SyRI legislation.

6.69. The judgment of the ECtHR in that case proves that domestic law must afford adequate protection against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise in order to meet the requirements of accessibility and foreseeability. According to the ECtHR, the level of precision required of domestic legislation depends to a considerable degree 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"[24] The ECtHR then considers as follows:

"It reiterates that it is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness."[25]

6.70. To what extent the legal safeguards are sufficient depends, according to the ECtHR, on the concrete circumstances and comes down to weighing all of the legal safeguards combined. The extent to which and the level of detail with which safeguards must be laid down in law depends on the seriousness of the interference.

6.71. This judgment also shows that the assessment 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. The safeguards must be laid down in law but at the same time also be adequate to prevent abuse and thereby proportionate to the aims pursued. In light of its considerations regarding the latter assessment, the ECtHR therefore did not deem it necessary to review whether the quality of the act met the requirements of Article 8 paragraph 2 ECHR. In this context the court considered as follows:

"The Court notes, however, that these questions are in this case closely related to the broader issue of whether the interference was necessary in a democratic society. In view of its analysis in paragraphs 105–126 below, the Court does not find it necessary to decide whether the wording of section 64 meets the 'quality of law' requirements within the meaning of Article 8 § 2 of the Convention."[26]

6.72. Like the ECtHR in that case, the court leaves undiscussed in its review whether the SyRI legislation is sufficiently accessible and foreseeable and as such affords an adequate legal basis as required under Article 8 paragraph 2 ECHR for a justified restriction of the right to protection of private life. The court holds that the SyRI legislation in any case contains insufficient safeguards for the conclusion that it is necessary in a democratic society in light of the purposes of the legislation, as Article 8 paragraph 2 ECHR also requires. As a result, in its current form this legislation does not pass the test of Article 8 paragraph 2 ECHR and is therefore unlawful. The court deems what follows as substantiation of its opinion.

Necessary in a democratic society: general

6.73. What must be assessed is whether there is an interference that is necessary in a democratic society in the interest of, in this case, the economic wellbeing of the country. The court states first observes that the ECtHR in principle affords the authorities of a Member State a 'margin of appreciation' to determine whether a measure is necessary in a democratic society in the interest of one of the purposes listed in Article 8 paragraph 2 ECHR. As regards the scope of that margin of appreciation, the court settles on 'a certain' margin of appreciation. This margin (see also above in 6.43) calls for restraint on the part of the court in its assessment whether the SyRI legislation violates Article 8 paragraph 2 ECHR, as the State correctly argues.

6.74. It is not in dispute that the SyRI legislation serves a legitimate purpose (see above in 6.4). The supply of data for the benefit of a collaborative alliance and the application of SyRI as provided for in the SyRI legislation thereby meet the so-named 'general interest' test, namely that it occurred in the interest of one of the purposes as identified in Article 8 paragraph 2 ECHR.

6.75. It is in dispute between the parties whether there is a 'pressing social need', or in other words, whether the interference meets a pressing social need. NJCM et al. argues that this is not the case, in support of which it considers relevant that there is a very serious interference in the private lives of citizens. NJCM et al. also argues that the State has failed to show that it is necessary to deploy an instrument as severe as SyRI to maintain the social security system. It points out that the wider social attitude towards SyRI is negative, or at least reserved and that the SyRI projects have not borne fruit and are therefore not effective as a means for combating fraud.

6.76. The court rejects this argument of NJCM et al. The SyRI legislation in itself seeks to fulfil a sufficiently compelling purpose to justify an interference with private life. In doing so, the court takes into account the starting points mentioned above on what SyRI is and the effect on private life in case data processing in SyRI results in a risk report, which determine the extent and seriousness of the interference (see above in 6.44 - 6.60). Fraud in the area of social security and welfare is significant: the State has mentioned – uncontested – sums of 153 million Euros in social security fraud and half a billion to one billion Euros in welfare fraud as well as 135 million Euros in social damage as a result of social security fraud.[27] Combating fraud also has indirect effects, including on the integrity of the economic system and confidence in the financial institutions.[28] Also taking into account the margin of appreciation which the national authorities have, the direct and indirect damage of fraud in this area justifies the conclusion of the legislator that there is a pressing social need to take measures provided for by the SyRI legislation in the interest of the economic wellbeing of the Netherlands.

6.77. In this respect, NJCM et al. refers to what it calls the real problem, namely 'access at the gate'. NJCM et al. believes that this problem can only be solved by setting more stringent requirements on the obligation to provide proof for applications so as to prevent investigation afterwards. Leaving aside the usefulness and necessity of improving checks of applications, the court is of the opinion that NJCM et al. has furnished insufficient facts which can demonstrate that these checks cover the aim pursued by the SyRI legislation to such an extent that there no longer is a 'pressing social need' for the SyRI legislation and that for this reason alone this legislation has no binding effect. Nor does the case law of the ECtHR show that the actual effectiveness of the instrument of SyRI in the interest of the economic wellbeing of the Netherlands, in accordance with the standards of Article 8 paragraph 2 ECHR, must be determined beforehand in order to meet the requirement of a 'pressing social need', contrary to what is suggested by NJCM et al. In light of the purposes the legislation serves, SyRI is not an unsuitable instrument or an a priori disproportionate instrument.

6.78. In light of the foregoing, the court is of the opinion that the choice of the legislator to create a

legal basis for data processing for the benefit of a collaborative alliance aimed at the purposes as formulated in Section 64 SUWI Act *and* the choice of the legislator for data processing in an instrument such as SyRI therefore meet the general necessity requirement of Article 8 ECHR. The latter concerns the technical infrastructure chosen to link, or have the ability to link, data files in a secured environment in order to carry out analyses, so that risk reports can be generated.

6.79. But this does not mean that the functioning of the instrument of choice, or the instrument itself, in this case SyRI, and the associated procedures and safeguards created for its application by the legislator in the SyRI legislation, sufficiently respects privacy in light of Article 8 paragraph 2 ECHR. The SyRI legislation does not pass this concrete test, as the court will explain below.

Necessary in a democratic society: proportionality and subsidiarity

6.80. The court must assess whether the SyRI legislation meets the requirements of necessity, proportionality and subsidiarity pursuant to Article 8 paragraph 2 ECHR in light of the aims it pursues. There has to be a 'fair balance' between the purposes of the SyRI legislation and the invasion of private life the legislation causes.

6.81. The substance of the SyRI legislation is the starting point for this assessment (see Chapter 4 of this judgment). From that substance it follows, as has been argued by the State, that the SyRI legislation restricts the circle of designated government or other bodies, exhaustively lists the number of data categories that qualifies for data processing, and obliges the participating designated government or other bodies to verify the necessity of a SyRI project and the data to be processed in that project. Moreover, the IB has been designated as processor, which pseudonymises said data, while the separate analysis unit of the Social Affairs and Employment Inspectorate carries out the analyses. The SyRI legislation also contains retention periods and limitations as regards access to and use of risk reports as well as obligations to maintain confidentiality and perform evaluations.

6.82. For this assessment, the court also takes into consideration the starting points as summed up in 6.61-6.65. These starting points are of interest to the extent and seriousness of the interference of the SyRI legislation with the private lives of the data subjects. A great amount of data qualifies for processing in SyRI. The risk model and indicators that make up the model and the data which are used in a particular SyRI project are not public nor are they known to the data subjects. Furthermore, there is room in the legal framework to adjust the risk model based on the feedback outcome. Finally, there is the fact that the data subject is unaware of the existence of a risk report, while the submission of a risk report has a significant effect on them.

6.83. The court weighs the substance of the SyRI legislation in light of the aims it pursues against the violation of private life the SyRI legislation brings about. The court is of the opinion that the SyRI legislation, insofar as it concerns the application of SyRI, does not strike the 'fair balance' required for the conclusion that there is a justified interference within the meaning of Article 8 paragraph 2 ECHR. The court points out the following.

6.84. In the aforementioned judgment of the ECtHR in the matter of *S. and Marper versus the United Kingdom,* the ECtHR considered as follows: *"The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard".*[29]The Dutch legislator does not claim to be a pioneer in the application of the instrument of SyRI in this case, while that matter also concerned the retention of DNA profiles for an indefinite term. Both the intrusiveness of the interference with private life and the safeguards to protect privacy of the British legislation reviewed in that matter differ from those in the current proceedings. Nevertheless, the court holds that in this case, too, the State bears a special responsibility, as expressed by the ECtHR.

6.85. The development of new technologies gives the government, among other things, opportunities

to link files and analyse data with the aid of algorithms in order to exercise supervision more effectively. Partly due to the speed of said development, the right to data protection is becoming increasingly important. Collecting and analysing data with the help of those new technologies can interfere extensively with the private lives of those to whom the data pertain. Therefore the legislator bears a special responsibility when applying an instrument such as SyRI: for a data subject it is difficult to gauge the effect of the instrument on their private life while the ECHR requires that the legislation that provides a basis for such an interference provides sufficient safeguards to protect against abuse and arbitrariness.

6.86. When drafting the SyRI legislation, the legislator paid heed to Article 8 ECHR and the right to respect for private life, as protected by the ECHR. Unlike the State, the court is of the opinion that the safeguards laid down in the legislation for the protection of the private life of those whose data can be processed in SyRI are insufficient. Considering the principle of transparency, the principle of purpose limitation and the principle of data minimisation – fundamental principles of data protection – the court holds that the SyRI legislation is insufficiently transparent and verifiable to conclude that the interference with the right to respect for private life which the use of SyRI may entail is necessary, proportional and proportionate in relation to the aims the legislation pursues. The court is of the opinion that the following circumstances, viewed in conjunction, are relevant.

6.87. The principle of transparency is the leading main principle of data protection that underlies and is laid down in the Charter and the GDPR (see 6.27- 6.34 for the principles of data protection). The court is of the opinion that in view of Article 8 paragraph 2 ECHR this principle is insufficiently observed in the SyRI legislation. The court finds that the SyRI legislation in no way provides information on the factual data that can demonstrate the presence of a certain circumstance, in other words which objective factual data can justifiably lead to the conclusion that there is an increased risk. The legislative history only provides a few examples of indicators that can indicate an increased risk and a potential hit:

"For instance, there may be cohabitation fraud if persons who receive a social benefit and/or an allowance and who, according to the municipal personal records database (*Gemeentelijke Basisadministratie* – GBA) are registered at different addresses while in fact they are living at the same address. An example of undeclared assets is someone whose bank balance has grown exponentially in one year. Other examples include a person who has several lock-up garages in a particular neighbourhood and has multiple vehicles registered in his name in a short period of time, or a recipient of social assistance under the WWB who has registered a bank account number with the Tax and Customs Administration with assets, while this is not known to the Municipal Social Services."[30]

6.88. The State has provided several other examples that could indicate discrepancies, including the example of a person who receives social assistance as a single householder, healthcare allowance for married couples and where multiple occupants of the same address receive housing allowance for a different address, while only one occupant is eligible to receive housing allowance at one address. The State has failed to explain on which objectively verifiable information these examples are based.

6.89. What is more, the SyRI legislation does not provide information on the functioning of the risk model, for instance the type of algorithms used in the model, nor does it provide information on the risk analysis method as applied by the Social Affairs and Employment Inspectorate. In these proceedings, the State has explained in more detail that the risk model consists of i) risk indicators, ii) links and iii) a so-named cut-off point.

Depending on the purpose of the investigations, points are awarded per risk indicator. The score depends on, inter alia, the probability of the risk indicator occurring. The more improbable it is that the specific risk indicator occurs, the higher the score. The cut-off point, which is predetermined, constitutes a threshold value. Instances with a score below the threshold value will not result in a

potential hit.

The State argues that risk models are used which have been validated by the Social Affairs and Employment Inspectorate and for which use is made of verified risk indicators which have shown in practice that they can indicate an increased risk of abuse or fraud. However, the SyRI legislation does not afford insight into the validation of the risk model and the verification of the risk indicators; the court consequently lacks such insight in these proceedings.

6.90. The foregoing results in the inability to verify how the simple decision tree, to which the State refers, is generated and of which steps it is comprised. Consequently, it is difficult to comprehend how a data subject could be able to defend themselves against the fact that a risk report has been submitted about him or her. It is just as difficult to see how a data subject whose data were processed in SyRI but which did not result in a risk report, can be aware that their data were processed on correct grounds. The fact that in the latter situation the data did not result in a risk report and furthermore must be destroyed no later than four weeks following the analysis does not alter the requirement of transparency in respect of that processing. The right to respect for private life also means that a data subject must reasonably be able to track their personal data.

6.91. The importance of transparency, in the interest of verifiability, is also compelling, because using the risk model and the analysis that is carried out in that context carries the risk that discriminatory effects – unintentional or otherwise – occur. The Advisory Division stated in its opinion – see 6.46 – that analysing large data sets, with or without deep learning/self-learning systems is undeniably useful, but may also yield undesirable results, including unjustified exclusion or discrimination. The Minister for Legal Protection acknowledged in his letter on Information and Communications (ICT)[31] of 8 October 2019 to the House of Representatives that on account of the risk of discriminatory effects, at least in profiling-based data analyses, certain characteristics may be incorrectly attributed to people (false positive), or the other way around, characteristics may incorrectly not be attributed (false negative).

6.92. NJCM et al., in these proceedings also supported by FNV and the UN Special Rapporteur on extreme poverty and human rights, has explained extensively that it believes that the use of SyRI has a discriminatory and stigmatising effect. NJCM et al. notes that SyRI is used to further investigate neighbourhoods that are known as problem areas. This increases the chances of discovering irregularities in such areas as compared to other neighbourhoods, which in turn confirms the image of a neighbourhood as a problem area, contributes to stereotyping and reinforces a negative image of the occupants of such neighbourhoods, even if no risk reports have been generated about them.

6.93. It is correct that to date SyRI has only been applied to so-labelled ‘problem districts’, as confirmed by the State at the hearing. This in and of itself need not imply that such use is disproportionate or otherwise contrary to Article 8 paragraph 2 ECHR in all cases. However, given the large amounts of data that qualify for processing in SyRI, including special personal data, and the circumstance that risk profiles are used, there is in fact a risk that SyRI inadvertently creates links based on bias, such as a lower socio-economic status or an immigration background, as NJCM et al. argue.

6.94. Based on the SyRI legislation, it cannot be assessed whether this risk is sufficiently neutralised due to the absence of a verifiable insight into the risk indicators and the risk model as well as the functioning of the risk model, including the analysis method applied by the Social Affairs and Employment Inspectorate. The circumstance that the process of data processing consists of two phases and that the analysis unit of the Social Affairs and Employment Inspectorate, following a link of the files by the IB, assesses the decrypted data on their worthiness of investigation, which includes a human check for false positives and false negatives, is deemed insufficient by the court. After all, the manner in which the definitive risk selection takes place is not public. Nor are the data subjects informed about how the definitive risk selection is effectuated or about the associated

conclusion whether or not a risk report is submitted, while the SyRI legislation only provides for a general monitoring by the AP afterwards.

6.95. In view of the foregoing, the court is of the opinion that the SyRI legislation contains insufficient safeguards to protect the right to respect for private life in relation to the risk indicators and the risk model which can be used in a concrete SyRI project. Without insight into the risk indicators and the risk model, or at least without further legal safeguards to compensate for this lack of insight, the SyRI legislation provides insufficient points of reference for the conclusion that by using SyRI the interference with the right to respect for private life is always proportionate and therefore necessary, as required by Article 8 paragraph 2 ECHR, in light of its purpose of combating abuse and fraud.

6.96. The court also holds that the SyRI legislation, as assessed against Article 8 paragraph 2 ECHR, pays insufficient attention to the principle of purpose limitation and the principle of data minimisation. The court emphasises that the purpose clause in Section 64 subsections 1 and 2 SUWI Act in itself is sufficiently specific. It is clear in advance in connection with which purposes data must be provided for the benefit of a collaborative alliance. The choice of the legislator for a large number of areas of potential cooperation and for which data must be provided can also be considered as being justified, in the sense of necessary, proportionate and subsidiary. Here the court has also taken into consideration the importance of fighting abuse and fraud and the margin of appreciation which the State, as the national authority, has. The court rejects the argument of NJCM et al. and accepts the defence of the State on this point. The court considers the SyRI legislation as not in violation of the principle of purpose limitation in that respect.

6.97. However, the situation changes if and insofar as those purposes are viewed in conjunction with the large amounts of data that qualify for processing in SyRI pursuant to Section 65 SUWI Act and the SUWI Decree, the circumstance that the test of necessity is carried out, as required, by the designated government or other bodies and there is no comprehensive review beforehand by an independent third party. The test of necessity which the designated government or other bodies must perform is relates to both the principle of purpose limitation and the principle of data minimisation.

6.98. The statutory restriction of the data set can be found in the eventually exhaustive enumeration of the data categories that qualify for processing, and the necessity of the data in terms of the purposes the specific SyRI project serves (Section 64 subsection 2 SUWI Act in conjunction with Article 5a.1 SUWI Decree). However, even if the exhaustive list of data categories is accepted as a given, it is hard to imagine any type of personal data that is not eligible for processing in SyRI.

6.99. Furthermore, the necessity of the test whether the data provision is needed for the benefit of a particular project has been left to each of the designated government or other bodies participating in the collaborative alliance. That test of necessity can and must only be carried out with respect to the data sets which the relevant government or other body has at its disposal. The SyRI legislation does not provide for a comprehensive review beforehand nor for a review by an independent third party, that is to say, a review prior to the data processing in SyRI by the Minister at the request of a collaborative alliance for the purpose of assessing whether or not the interference with private life is necessary, proportionate and subsidiary in light of all the files that are linked in a project considering the specific purpose of that project.

6.100. Unlike the State has argued, the sum total of the separate reviews carried out the participants involved in the SyRI project cannot be definitively considered as a comprehensive review in advance. In this respect, too, the court also considers it relevant that the SyRI legislation does not provide insight into the functioning and validation of the risk indicators and the risk model. The risk model and the risk indicators are, after all, also of importance for the assessment whether, and if so, to what extent the data provision is necessary and thereby also for the overall effect on the private life of the comparison of the various data sets in SyRI. The court holds that

against this backdrop, too, a data subject has insufficient certainty that their privacy is safeguarded when SyRI is used.

6.101. Moreover, the LSI is merely an advisory organ. Its advice is non-binding and lacks an explicit legal basis. What is more, the LSI is comprised of representatives of organs which also have an interest in combating and preventing abuse and fraud in the areas specified in Section 64 subsection 1 SUWI Act. Furthermore, the Social Affairs and Employment Inspectorate is not only represented in the LSI, but can itself also be a participant in a collaborative alliance for the benefit of a SyRI project, and is charged with analysing data for the definitive risk selection based on which a risk report is submitted. The court is unable to assess if and to what extent the internal functional division between the various units of the Social Affairs and Employment Inspectorate (the investigation unit, the analysis unit and possibly other units) is sufficiently safeguarded. The State has failed to provide further explanation about this in its response to the defence of NJCM et al.

6.102. Citing judgments of the Central Appeals Tribunal, among other things, the State has pointed out that case law accepts file linkage with a view to selecting inspection cases.[32] The judgments on which the State relies do not move the court to draw a different conclusion. As is apparent from the foregoing, the court deems the use of risk profiles in connection with the exercise of their regulatory duty not to be contrary to Article 8 paragraph 2 ECHR per se. The judgments on which the State relies do not pertain to the use of SyRI, but in each case to the exchange of a limited set of data, for which use was made of risk profiles justified by objective criteria. Where SyRI is applied, the SyRI legislation provides insufficient safeguards due to the large amount of data – of various types and from a large number of different sources – that can be processed. Moreover, there is no insight into the risk indicators and risk model nor into the objective criteria underlying the validity of the risk indicators and risk model. In this sense, the cases resulting in the judgments cited by the State differ fundamentally from the legislation to be assessed in these proceedings.

6.103. The State has also put forward that a data privacy impact assessment (DPIA) has been carried out in the context of the act and that therefore a DPIA neither is nor need be carried out for each SyRI project.

6.104. The court considers that pursuant to Article 35 paragraph 1 GDPR a DPIA must be carried out when a type of processing, considering its nature, the scope, the context and purposes, probably entails a high risk for the rights and freedoms of natural persons. As the State has correctly observed, this provision does not apply pursuant to Article 35 paragraph 10 GDPR if, put briefly, the specific processing or all relevant processing activities are regulated by law, and a DPIA has already been carried out in that context, unless the Member States deem it necessary to carry out such an assessment prior to the processing. The State has pointed out that since the entry into force of the SyRI legislation a new data protection model of the civil service is being used, geared towards the privacy rules of the GDPR.

6.105. Without further explanation, which is lacking, the court cannot accept the defence of the State why a DPIA is not carried out for each individual SyRI project. After all, the DPIA that has been carried out occurred before the entry into force of the GDPR. Whether this assessment meets the requirements set by the GDPR cannot be assessed by the court on the basis of the available information. The State has also failed to elucidate why, considering the extent and seriousness of the invasion of private life, occasioned by the processing of data in SyRI, such an assessment is not carried out for each individual project. In this regard it should be noted that insofar as the court is aware a limited number of SyRI projects (five) have been carried out since the entry into force of the SyRI legislation.

6.106. In view of the large amount of data that qualify for processing in SyRI and the circumstance that in a concrete SyRI project the test of necessity is carried out by the separate participants in

the project, that is to say, with no comprehensive and furthermore no independent assessment prior to the approval by the Minister, the SyRI legislation therefore contains insufficient safeguards for the conclusion that, in light of the principles of purpose limitation and data minimisation, Article 8 paragraph 2 ECHR has been complied with.

6.107. In view of all of the above, the court will not assess whether the SyRI legislation is contrary to one or more specific provisions of the GDPR on which NJCM et al. relies and whether the SyRI legislation is in violation of Articles 6 and 13 ECHR. The court therefore leaves undiscussed the other arguments and defences of the parties.

The claims of NJCM et al.
6.108. The question that remains is what the foregoing means for the claims of NJCM et al.

6.109. As has been considered above, the court will declare the claims of Landelijke Cliëntenraad, [claimant sub 6] and [claimant sub 7] inadmissible. The court refrains from assessing claim VIII, which only pertains to [claimant sub 6] and [claimant sub 7] .

6.110. As regards the claims of Platform Bescherming Burgerrechten, Privacy First and Stichting Koepel voor DBC-Vrije Praktijken the court considers as follows. The court considers the SyRI legislation to be contrary to Article 8 paragraph 2 ECHR insofar as this legislation pertains to the use of SyRI. Only Section 65 SUWI Act and Chapter 5a SUWI Decree specifically relate to SyRI and its application. Section 64 SUWI Act provides for the exchange of data for the benefit of a collaborative alliance with a view to prevent and combat the unlawful use of social security schemes, income-dependent schemes, taxes and social security fraud and non-compliance with labour laws in general. From the foregoing it follows that the court considers Section 64 SUWI Act, viewed separately, not to be contrary to Article 8 paragraph 2 ECHR.

6.111. Also, the court arrives at the opinion on fundamental grounds that the SyRI legislation, insofar as it concerns SyRI and its application, is contrary to Article 8 paragraph 2 ECHR. These grounds pertain to both Section 65 SUWI Act and Chapter 5a SUWI Decree. The combined statutory basis of SyRI in Section 65 SUWI Act and the more detailed elaboration in Chapter 5a SUWI Decree contains, considering the corpus of legislation, insufficient safeguards to constitute a sufficiently justified interference with private life when SyRI is. This is not altered by the fact that the court considers certain choices and starting points of the legislator, as formulated in Section 65 SUWI Act and Chapter 5a SUWI Decree, compatible with Article 8 ECHR.

6.112. In light of the foregoing the court will rule that Section 65 SUWI Act and Chapter 5a SUWI Decree have no binding effect with respect to NJCM, Platform voor Burgerrechten, Privacy First and Koepel van DBC-Vrije Praktijken and on the individuals whose interests these parties promote for being contrary to Article 8 paragraph 2 ECHR. In this respect claim IV is allowed. The claim is dismissed in all other respects.

6.113. The court will dismiss all other claims. As regards the declaratory decisions claimed under claims I-III, considering the partial allowance of claim IV, the claimants have no independent interest in these claims.

6.114. Insofar as claim V pertains to the provision of data by the Tax and Customs Administration to other collaborative alliances pursuant to Section 64 SUWI Act the claimant have failed to sufficiently substantiate their assertions. Insofar as this claim is connected to the provision of data to the Minister in respect of the use of SyRI pursuant to Section 65 SUWI Act in conjunction with Section 64 SUWI Act, the claimants have no independent interest in this claim.

6.115. As regards the order claimed under claim VI to disclose the risk models used in the specific SyRI project, an administrative-law court procedure with sufficient safeguards is available. Nor does it follow from the assessment of the court regarding the unlawfulness of the SyRI legislation,

insofar as it pertains to the use of SyRI, that the State is under the obligation to disclose this model to the claimants.

6.116. Claim VII fails, too, due to the lack of a sufficiently independent interest in the claim, and also because, regardless of the use of SyRI, it has been insufficiently explained to be allowable.

6.117. Finally, the court considers claim IX to be too generally worded to be allowable. The fact that Section 65 SUWI Act and Chapter 5a SUWI Decree do not have binding effect does not inevitably lead to the conclusion that the State has an obligation to the collective interest organisation whose claims have been declared admissible in these proceedings to destroy all personal data collected in the context of, with the use of or for the benefit of the application of SyRI and to furnish proof of this destruction to them. Nor is this claim suitable for assessment in the context of a class action, considering its close connection with the individual circumstances of the support base of the collective interest organisations.

The costs of the proceedings

6.118. As the more unsuccessful party the State will be ordered to pay the costs of the proceedings on the part of NJCM, Platform voor Burgerrechten, Privacy First and Koepel van DBC-Vrije Praktijken and FNV. The costs on the part of these parties to date are estimated at:

- summons € 98.01
- court fees € 1,252.00
- lawyer's fees € 1,900.50 (3.5 points x rate II of € 543)

Total € 3,250.51

6.119. The claimed statutory interest on the costs of the proceedings, which is undisputed, is allowable.

7 The decision

The court

7.1. declares that the claims of Landelijke Cliëntenraad, [claimant sub 6] and [claimant sub 7] are inadmissible,

7.2. rules that Section 65 SUWI Act and Chapter 5a SUWI Decree have no binding effect with respect to NJCM, Platform voor Burgerrechten, Privacy First and Koepel van DBC-Vrije Praktijken and on those whose interests these parties represent for being contrary to Article 8 paragraph 2 ECHR,

7.3. orders the State to pay the costs of the proceedings, on the part of NJCM, Platform voor Burgerrechten, Privacy First and Koepel van DBC-Vrije Praktijken and FNV to date assessed at € 3,250.51 plus statutory interest as of 14 days from today until the day of full payment,

7.4. declares this judgment provisionally enforceable as far as possible,

7.5. dismisses all other claims.

This judgment was rendered by *mr.* M.C. Ritsema van Eck-van Drempt, *mr.* J.S. Honée and *mr.* H.J. van Harten and pronounced in open court on 5 February 2020.

[1] Section 8 SUWI Act.

[2] *Parliamentary Papers II* 2012/13, 33579, 3.

[3] Government Gazette 2017, 20624.

[4] Act of 9 October 2003, establishing an act for support with integration into the workforce and the provision of social assistance by municipal authorities (Work and Social Assistance Act), Bulletin of Acts and Decrees 2003, 375.

[5] *Parliamentary Papers II* 2014/15, 17050, 508.

[6] Respectively: Government Gazette 2015, 34927 and Government Gazette 2015, 34927 (https://zoek.officielebekendmakingen.nl/stcrt-2015-34927.html) (rectification); Government Gazette 2016, 3826; Government Gazette 2016, 19457; Government Gazette 2018, 12083; Government Gazette 2018, 12088. 'WGA' stands for *wijkgerichte aanpak* (neighbourhood-oriented approach), see also 4.24 below.

[7] Act of 9 October 2013 to amend the Work and Income (Implementation Organisation Structure) Act and any other acts pertaining to tackling fraud by exchanging data and the effective use of data known within the government, Bulletin of Acts and Decrees 2013, 405.

[8] Decree of 1 September 2014 to amend the SUWI Decree in connection with rules for tackling fraud by exchanging data and the effective use of data known within the government with the use of SyRI, Bulletin of Acts and Decrees 2014, 320.

[9] Regulation (EU) 2016/679 of the European Parliament and the Council 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), Official Journal L 119/1, p. 1.

[10] State's statement of defence, under 5.8 with reference to footnote 20 there. According to the explanatory memorandum to the SUWI Decree there are two standard risk models.

[11] Decree of 13 December 2001, containing further rules on the coordination and service provision by the Benefits Intelligence Agency for the benefit of municipal authorities as regards the data supply under both the SUWI Act and the Social Assistance Act (*Algemene bijstandswet* – Awb), the Older and Partially Disabled Unemployed Workers Income Scheme Act (*Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers* – IOAW) and the Older and Partially Disabled Former Self-Employed Persons Income Scheme Act (*Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen* – IOAZ) as well as regarding the financing of the Benefits Intelligence Agency (Benefits Intelligence Agency (Municipalities) Decree), Bulletin of Acts and Decrees 2001, 686.

[12] Section 6 General Data Protection Regulation (Implementation) Act.

[13] See ECtHR 27 October 1995, no. 20190/92 (C.R. versus the United Kingdom), para. 42 and ECtHR 29 April 2002, no. 2346/02 (Pretty versus the United Kingdom), para. 65.

[14] See, inter alia, ECtHR 4 December 2008, nos. 30562/04 and 30566/04 (S. and Marper versus the United Kingdom), para. 66.

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal 1995, L 281, p. 31.

[16] Claimants' Exhibit 22, Guidelines on Automatic individual decision making and Profiling for the purposes of Regulation 2016/679, 3 October 2017; last amended on 6 February 2018.

[17] Cf. HR (Supreme Court) 16 May 1986, NJ (Dutch Law Reports) 1987/251 (*Landbouwvliegers*), para. 6.1.

[18] *Parliamentary Papers II* 2017/18, 26643, 557.

[19] *Parliamentary Papers II* 2018/19, Appendix to the Proceedings, 1037.

[20] *Parliamentary Papers II* 2018/19, 26643, 578.

[21] ECtHR 2 August 1984, no. 8691/79 (Malone versus the United Kingdom).

[22] ECtHR 26 April 1979, no. 6538/74, (Sunday Times versus the United Kingdom), para. 48.

[23] See, inter alia, ECtHR 29 June 2006, no. 54934/00 (Weber and Saravia versus Germany) and the case law cited there, and ECtHR 12 January 2016, no. 31718/14 (Szabó and Vissy versus Hungary).

[24] ECtHR 4 December 2008, nos. 30562/04 and 30566/04 (S. and Marper versus the United Kingdom), para. 96.

[25] ECtHR 4 December 2008, nos. 30562/04 and 30566/04 (S. and Marper versus the United Kingdom), para. 99.

[26] ECtHR 4 December 2008, nos. 30562/04 and 30566/04 (S. and Marper versus the United Kingdom), para. 112.

[27] See statement of defence 5.63, with reference to the explanatory memorandum to the legislative proposal to amend the SUWI Act, P. Olsthoorn, 'Big data for combating fraud' ('*Big data voor fraudebestrijding*'), WRR (Scientific Council for Government Policy) working paper number 21 and a PWC report, "On the road to an overview of fraud in the Netherlands" ("*Naar een fraudebeeld Nederland*"), Amsterdam, 19 December 2013.

[28] For these indirect effects, see for instance *Parliamentary Papers II* 2013/14, 17050, 450 and *Parliamentary Papers II* 2013/14, 17050, 439, to which the State refers (statement of defence, 6.51)

[29] ECtHR 4 December 2008, nos. 30562/04 and 30566/04 (S. and Marper versus the United Kingdom), para. 112.

[30] *Parliamentary Papers II* 2012/13, 33579, 3, p. 5.

[31] *Parliamentary Papers II*, 2019/20, 26643, 641.

[32] See, inter alia, CRvB (Central Appeals Tribunal) 15 December 2009, ECLI:NL:CRVB:2009:BK8311 and CRvB (Central Appeals Tribunal) 27 April 2010, ECLI:NL:CRVB:2010:BM:3881.