

Artificial Intelligence, Big Data and Fundamental Rights

Country Research Netherlands

2020

Report provided to FRA
under contract D-SE-19-T02¹

DISCLAIMER: This document was commissioned under contract as background material for comparative analysis by the European Union Agency for Fundamental Rights (FRA) for the project [Artificial Intelligence, Big Data and Fundamental Rights](#). The information and views contained in the document do not necessarily reflect the views or the official position of the FRA. The document is made publicly available for transparency and information purposes only and does not constitute legal advice or legal opinion.

¹ Report prepared by Ecorys and the University of Utrecht. While every effort has been made by the FRA contractor to refer to relevant national institutions, policy developments and law relating to the field of AI and fundamental rights, given the wide reach of AI developments and the quickly evolving nature of the field there may be omissions or recent developments at national level that are not referred to in this country research.

Table of contents

1	Constitutional and institutional context	6
1.1	Map of the major stakeholders	6
1.1.1	Parliament and government	6
1.1.2	Decentralised bodies	6
1.1.3	Public bodies and agencies	7
1.1.4	Advisory councils and bodies	8
1.1.5	Research institutions	9
1.1.6	Judiciary	10
1.1.7	Public-private partnerships and relations between the private and public sector	11
1.1.8	Civil society	12
1.2	International relations	13
1.2.1	General strategy	13
1.2.2	European linkages – Council of Europe and OECD	15
1.2.3	International linkages – G20	16
1.3	National strategies and guidelines	17
1.3.1	Strategic Action Plan AI (SAPAI)	17
1.3.2	Digital Government Agenda 2019	21
1.3.3	Other policy briefs relevant for AI and fundamental rights	23
1.4	Standards and voluntary guidelines; the role of the private sector	25
1.4.1	Government standards and guidelines	25
1.4.2	Self-regulation in the private sector	27
1.5	Sample recent cases	28
1.5.1	System for Risk indication (SyRI)	28
1.5.2	Facebook’s algorithms	31
1.5.3	AERIUS calculator	32
1.5.4	Discrimination and AI	32
2	Laws and regulations applicable to AI and big data	34
2.1	General	34
2.2	Application of fundamental rights laws to AI	34
2.2.1	Privacy related rights, personal autonomy and data protection	35
2.2.2	Freedom rights (e.g. freedom of information and freedom of expression)	35
2.2.3	Non-discrimination and equality rights	36
2.2.4	Procedural rights	37
2.3	Overview of laws applicable to AI and big data	39
3	Future development	78
4	References	80

Abbreviations

ACM	Dutch Authority for Consumers and Markets (<i>Autoriteit Consument en Markt</i>)
AI	Artificial Intelligence
AIC	Dutch Artificial Intelligence Coalition (<i>Nederlandse AI Coalitie</i>)
AIV	Advisory Council for International Affairs (<i>Adviesraad Internationale Vraagstukken</i>)
ALLAI	Alliance for Artificial Intelligence
AP	Data Protection Authority (<i>Autoriteit Persoonsgegevens</i>)
AVG	General Data Protection Regulation (<i>Algemene Verordening Gegevensbescherming</i>)
AWGB	Dutch General Equal Treatment Act (<i>Algemene Wet Gelijke Behandeling</i>)
BEREC	Body of European Regulators for Electronic Communications
BHOS	Foreign Trade and Development Co-operation (<i>Buitenlandse Handel en Ontwikkelingssamenwerking</i>)
BNVKI/AIABN	Benelux Association for Artificial Intelligence
BZ	Foreign Affairs (<i>Buitenlandse Zaken</i>)
CAHAI	Ad Hoc Committee on Artificial Intelligence
CBP	College for the Protection of Personal Data (<i>College Bescherming Persoonsgegevens</i>)
CBS	Central Bureau of Statistics
CEDAW	Convention on the Elimination of All Forms of Discrimination Against Women
CERD	Committee on the Elimination of Racial Discrimination
CETS	Council of Europe Treaty Series
CFR	Charter of Fundamental Rights
CIP	Centre for Information Security and Privacy Protection (<i>Centrum voor Informatiebeveiliging en Privacybescherming</i>)
CJEU	Court of Justice of the European Union
CTIVD	Committee for the Supervision of Intelligence and Security Services (<i>Commissie van toezicht op de inlichtingen- en veiligheidsdiensten</i>)
ECHR	European Convention on Human Rights
ECP	Platform for the Information Society
ESC	Economic, Social and Cultural
FRA	European Union Agency for Fundamental Rights
FSA	Financial Supervision Act (<i>Wet op het financieel toezicht</i>)
GDPR	General Data Protection Regulation
HR	Human Rights

ICAI	Innovation Centre for Artificial Intelligence
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology
IND	Immigration and Naturalisation Service (<i>Immigratie- en Naturalisatiedienst</i>)
ISO	International Organization for Standardization
IVD	In Vitro Diagnostic
MSI-AUT	Committee of experts on Human Rights Dimensions of automated data processing and different forms of artificial intelligence
NEN	Royal Netherlands Standardization Institute (<i>Nederlands Normalisatie-Instituut</i>)
NGO	Non-Governmental Organization
NHRI	National Human Rights Institute
NJCM	Netherlands Committee of Jurists (<i>Nederlands Juristencomité voor de Mensenrechten</i>)
NRC	Norwegian Refugee Council
OECD	Organization for Economic Co-operation and Development
OM	Netherlands Public Prosecution Service (<i>Openbaar Ministerie</i>)
PACE	Parliamentary Assembly of the Council of Europe
PAS	Programmatic Approach to Nitrogen (<i>Programmatiese Aanpak Stikstof</i>)
PBL	Netherlands Environmental Assessment Agency (<i>Planbureau voor de Leefomgeving</i>)
ROB	Council for Public Administration (<i>Raad voor het Openbaar Bestuur</i>)
SAPAI	Strategic Action Plan for Artificial Intelligence
SDG	Sustainable Development Goals
SER	Social and Economic Council of the Netherlands
SVB	Sociale Verzekeringsbank
TFEU	Treaty on the Functioning of the European Union
TNO	Netherlands Organization for Applied Scientific Research (<i>Toegepast Natuurwetenschappelijk Onderzoek</i>)
UAVG	GDPR Execution Act (<i>Uitvoeringswet Algemene Verordening Gegevensbescherming – UAVG</i>)
UN	United Nations
UNECE	United Nations Economic Commission for Europe
UNESCO	United Nations Educational, Scientific and Cultural Organization
VNO-NCW	Confederation of Netherlands Industry and Employers
VSNU	Association of Universities in the Netherlands (<i>Vereniging Samenwerkende Nederlandse Universiteiten</i>)
WGB	World Bank Group

WRR Dutch Scientific Council for Government Policy
(*Wetenschappelijke Raad voor het Regeringsbeleid*)

WTO World Trade Organization

1 Constitutional and institutional context

1.1 Map of the major stakeholders

1.1.1 Parliament and government

The Netherlands has a unitary, yet decentralised constitutional system. Legislation is made on the central level (statutory acts or Acts of Parliament) are made in a collaboration between the [Parliament](#) (*parlement*) and the [Government](#) (*regering*). The Government is mostly responsible for the preparation and execution of statutory acts as well as for setting out major policy lines; this happens in the various ministries or departments. Another important power of the Government is to draft further legislation and regulations (government decrees, ministerial decrees) to refine and execute statutory legislation.

Parliament itself (consisting of the Lower House (*Tweede Kamer*) and the Senate (*Eerste Kamer* or *Senaat*) may also initiate legislation and make policy proposals and, in addition, it may amend bills proposed by the Government. For example, in the field of AI, an [‘initiative policy brief’ was presented by a Member of Parliament on human-centric AI](#) in May 2015. After such a brief has been presented and debated, it is the Government’s task to respond and act on requests (*moties*) made by Parliament. Furthermore, an important task for the Parliament is to deliberate with the Government’s Ministers about the various policies adopted and to supervise and check on the quality and political acceptability of legislative and policy proposals. On 2 July 2019, the Lower House has established a [temporary commission on the digital future](#) (*Tijdelijke commissie digitale toekomst*) in order to enable it to exercise its role in this field as effectively as possible.

In practice, major policy lines and strategies regarding technological development, responsible AI, open data etc. are set out by the Government (see also below, [section I.3](#)), under close parliamentary supervision and control. Together, the Parliament and the Government also decide whether such policies ought to be transformed to statutory legislation or whether other regulatory methods are to be preferred.

1.1.2 Decentralised bodies

On a decentralised level, the [12 Provinces](#) (*provincies*), [355 Municipalities](#) (*gemeenten*) and [21 Water authorities](#) (*waterschappen*) execute the legislation and policies drafted on the central level. The decentralised bodies often have significant discretionary powers, which include legislative, extensive policy-making and decision-making

competences. Their discretion is particularly wide in relation to policy fields like infrastructure, agriculture and nature (for the Provinces) and social benefits, primary and secondary education, housing and safety (for the Municipalities). In addition, decentralised bodies have certain autonomous powers regarding the governance of their own territories, but these are rather limited.

Within the boundaries set by central policies and legislation, all decentralised bodies may experiment with AI in exercising their own discretionary and autonomous powers and they may develop it. In practice, they often do so. A recent quick scan of [AI applications in the public sector](#) has shown considerable efforts by many decentralised bodies to make use of the possibilities offered by big data analyses and algorithms in their policy activities and decision-making.

1.1.3 Public bodies and agencies

Many regulatory, executive and supervisory powers are exercised by about 200 public bodies and [agencies](#) (*zelfstandige bestuursorganen*). There are many public bodies and agencies which have special competences in functional policy fields, such as social security (e.g. [Uitvoeringsinstituut Werknemersverzekeringen](#) – UWV and [Sociale Verzekeringsbank](#) – SVB), or health care ([Zorginstituut Nederland](#)). While the agencies mainly execute policies and legislation set on the central level, they are functionally and personally independent (although Ministers are responsible for their policies and may set certain policy guidelines, and Parliament may hold them Ministers accountable for the acts and omissions of agencies). Some agencies have particular supervisory or investigative tasks, they may be competent to impose (or propose) fines to companies or persons who are considered to have violated legislation, and/or they may have semi-judicial tasks. Examples of agencies having such competences are the Data Protection Authority ([Autoriteit Persoonsgegevens](#)), the Authority for Consumers and Markets ([Autoriteit Consument en Markt](#) – ACM), the Immigration and Naturalisation Service ([Immigratie- en Naturalisatiedienst](#) – IND), the Commissariat for the Media ([Commissariaat voor de Media](#)) and the Netherlands Institute for Human Rights ([College voor de Rechten van de Mens](#)).

Even though there is no specific agency for AI, innovation or (emerging) technologies,² many agencies may experiment with the development and use of AI and big data in their own work and/or are involved in policy-making, regulation and supervision in this regard.³ Many agencies also actively participate in various 'labs' and public-private partnerships working in the field of AI. For example, the national police ([Politie](#)) and

² Although the Dutch Organization for Applied Technological Science (TNO) seems a relevant agency in the field. As its tasks are mainly in the field of research, it is addressed under that heading.

³ Autoriteit Persoonsgegevens, 'AP doet onderzoek naar verwerking nationaliteit bij Belastingdienst', 20 May 2019, <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-doet-onderzoek-naar-verwerking-nationaliteit-bij-belastingdienst>.

the Netherlands Public Prosecution Service ([Openbaar Ministerie](#) – OM) have started a [Police Lab AI](#) together with Utrecht University and the University of Amsterdam. The Police Lab AI is part of a collaboration between academia, industry and government: the [Innovation Centre for Artificial Intelligence](#) (ICAI). Another example of cooperation between different government agencies are the [Living Labs Big Data](#). They are developed by various ministries and agencies working in child protection, justice, security and migration in order to obtain insights regarding data quality and offer reliable data analyses in the field of child protection or migration routes. This type of public-private partnerships is further addressed [below](#).

A recent [report by the Central Bureau of Statistics](#) (CBS) has shown that 47% of all ministries, government agencies and decentralised bodies make use of (mainly rule-based, but also case-based, machine learning) algorithms and deep learning algorithms in their primary processes.

1.1.4 Advisory councils and bodies

The Netherlands has an extensive number of advisory councils and bodies. Some of these are High Advisory Councils which are established by law, based on the Dutch Constitution, and are fully independent of the Government.⁴ An important example is the Council of State ([Raad van State](#)). In its advisory function the Council of State advises Parliament and the government on the compatibility of draft legislation (and its underlying policies) with the Constitution, European and international law and, in particular, fundamental rights. The Council of State may also give unsolicited advice, as it did in 2018 in relation to [digitalisation and the use of algorithms by the government](#). Another example of a High Advisory Council is the National Ombudsman ([Nationale Ombudsman](#)) who is competent to deal with complaints regarding unfair treatment by the government and who may advise the government on matters of good governance. Furthermore, the Ombudsman may advise on the fair use of technology by government bodies which it did in 2019 when defining risk profiling by algorithms as a [priority](#). In particular, the aim is to identify citizens' perspectives on risk profiling and develop a point of view on which requirements need to be set taking into account citizens' interests.

The Dutch Scientific Council for Government Policy ([Wetenschappelijke Raad voor het Regeringsbeleid](#) – WRR) advises the government, upon request or from its own accord, on strategic issues with important political and societal consequences. The WRR is particularly active in advising the government on technology-related matters like [internet governance](#), [iGovernment](#), [big data](#), [digital disruption](#) and [robotics](#). It is currently preparing an [advisory report on the opportunities and consequences of AI for \(Dutch\) society](#).

⁴ See Articles 73 and 75 of the Dutch Constitution.

Other relevant advisory councils are the Advisory Council for International Affairs ([Adviesraad Internationale Vraagstukken](#) – AIV), which has previously advised on [internet freedom](#) and is currently preparing another report on the topic, and the Council for Public Administration ([Raad voor het Openbaar Bestuur](#) – ROB), which recently advised the government on the use and risks of new technologies in relation to the rule of law and democracy.

1.1.5 Research institutions

In the academic field, all universities have specialists working in the field of AI (its development as well as research into its applications and their consequences).⁵ Many scientists and scholars are involved in research-for-society or conduct research projects commissioned by the government or by private actors. For example, upon the request of the government or one of the ministries, university researchers may be asked to advise on the opportunities and risks of AI for fundamental rights, either in general or in specific fields.⁶ In particular, the Research and Documentation Centre ([Wetenschappelijk Onderzoek- en Documentatiecentrum](#) – WODC) of the Ministry of Justice and Security has commissioned important research projects on the legal and societal impact of AI. An example is the (still running) project on the impact of algorithm-driven decision-making on fundamental rights conducted by Utrecht University.⁷ In addition, the WODC may conduct research projects itself, which usually focus on legal and societal consequences of policies in the field of crime control, policing, judicial administration and migration issues.

Science funding organisations such as the Dutch Organisation for Scientific Research ([Nederlandse Organisatie voor Wetenschappelijk Onderzoek](#) – NWO) run specific funding schemes to stimulate AI development as well as AI-in-context research.⁸ NWO is currently

⁵ To mention just a few examples: see European Association for Artificial Intelligence (EURAI), 'BNVKI/AIABN', accessed 20 March 2020, <https://www.eurai.org/node/4> and Benelux Association for Artificial Intelligence, 'About BNVKI', <http://ii.tudelft.nl/Bnvki/> (blog), accessed 20 March 2020, <https://ii.tudelft.nl/bnvki/>.

⁶ For a recent example, see M.J. Vetzo, J.H. Gerards, and R. Nehmelman, 'Algoritmes En Grondrechten' (Montaigne Centrum voor Rechtstaat en Rechtspleging, 2018), which was written upon the request of the Ministry of the Interior and Kingdom Relations; for the report, see https://www.uu.nl/sites/default/files/rebo-montaigne-algoritmes_en_grondrechten.pdf; for the response the government sent to parliament, see Digitale Overheid, 'Kamerbrief met reactie op UU-rapport Algoritmes en grondrechten', webpagina, 28 March 2019, <https://www.digitaleoverheid.nl/gebeurtenis/kamerbrief-met-reactie-op-uu-rapport-algoritmes-en-grondrechten/>.

⁷ See generally: Digitale Overheid, 'Planning Agenda Digitale Overheid', webpagina, 2019, <https://www.digitaleoverheid.nl/nl-digibeter2019/planning-agenda-digitale-overheid/>.

⁸ See, for example, its call on projects regarding Responsible Use of AI of July 2019: NWO, 'Responsible Use of Artificial Intelligence: Call for Proposals', 2020, <https://www.nwo.nl/en/documents/enw/responsible-use-of-artificial-intelligence---call-for-proposals>.

engaged in drafting a policy agenda for AI research in the Netherlands, which focuses on a wide variety of AI related issues, including the impact of AI on fundamental rights.⁹

The universities themselves co-operate in the framework of the Association of Universities in the Netherlands ([Vereniging Samenwerkende Nederlandse Universiteiten](#) – VSNU), which launched a [Digital Society Research Agenda](#) in 2017. The aim of this agenda is to secure a leading role for the Netherlands in the field of human-centred information technology. Furthermore, it focuses on issues such as citizenship and democracy in relation to responsible data science.

Besides universities, the Netherlands has several public research institutes that specialise in new technologies and fundamental rights. An important example is the Netherlands Organization for applied technological science ([TNO](#)), an institute that often conducts government-commissioned research and actively contributes to many public-private partnerships in innovation and new technologies. It works [in almost all AI related areas](#), aiming to form a bridge between the academic world and the business sector, and it has published [many reports and studies on AI in relation to public values](#). The same is true for the [Rathenau Institute](#), which focuses on the societal aspects related to science, innovation and technology. As part of their research focus ‘[Digital Society](#)’, the Rathenau Institute has published numerous reports analysing technological developments and advising the government about its implications.

Other important public research institutes are the Central Bureau of Statistics ([Centraal Bureau voor de Statistiek](#) – CBS) as well as specialised planning bodies (such as the Netherlands Institute for Social Research ([Sociaal en Cultureel Planbureau](#) – SCP) and the Netherlands Environmental Assessment Agency ([Planbureau voor de Leefomgeving](#) – PBL). They have important roles in, *inter alia*, collecting and analysing (big) data as a basis for policy-making and legislation.

[1.1.6 Judiciary](#)

Another relevant stakeholder is the [judiciary](#) which deals with concrete cases on the use of AI and algorithmic decision-making. Several cases reviewing the compatibility of algorithm-based decision-making with the right to a fair trial and principles of transparency have appeared before administrative and civil courts.¹⁰ Furthermore, specific AI-related cases have appeared before civil courts, for instance, dealing with the

⁹ See also already the [AI for the Netherlands strategy](#) presented in 2018.

¹⁰ For the most important examples, see ABRvS (Judicial Division of the Council of State) 17 May 2017, ECLI:NL:RVS:2017:1259 (Aerius I); ABRvS 18 July 2018, ECLI:NL:RVS:2018:2454 (Aerius II); HR (Supreme Court) 17 August 2018, ECLI:NL:HR:2018:1316; Rb (District Court) Amsterdam 4 July 2019, ECLI:NL:RBAMS:2019:4799 (system for placement of children in schools).

recognition of decisions rendered by '[e-Court](#)' which is an AI-driven alternative dispute resolution body that deals with complaints about debt recovery.¹¹ Furthermore, in February 2020, the civil court found that legislation allowing for algorithm-driven fraud detection in the field of social security (the so-called 'SyRI' system) was incompatible with data protection and non-discrimination rules.¹²

1.1.7 Public-private partnerships and relations between the private and public sector

Many private companies in the Netherlands increasingly use and invest in development of AI. This is certainly true for large technology companies such as Philips which invested in [new applications of AI in healthcare](#). In the retail sector, Albert Heijn (Ahold-Delhaize) is using [AI to prevent food waste](#) by means of dynamic discounting of fresh products.¹³ In the insurance sector, AI is being applied at such a broad scale that [the sector is now closely looking into various ethical issues](#).

The private sector is also involved in AI-policy making and (self-) regulation. In particular, their efforts relate to the collection and processing of personal data. For example, the Dutch Association of Insurers ([Verbond van Verzekeraars](#)) has introduced an [ethical code on the processing of personal data by insurers](#). More related to AI, several technology companies have joined forces in the [ECP \(the Platform for the Information Society\)](#) to develop a Dutch AI impact assessment for the private sector together with a code of behaviour. In addition, ICT companies can become a member of [NL Digital](#). More information about the activities of these platforms and associations can be found in [Section I.4](#).

The various public bodies and agencies often work together with universities and private organisations, either informally or through public-private partnerships. Such partnerships oftentimes conduct experiments and pilots or run 'living labs' to develop and test new technologies that could have a public function. An example is the '[Stratumseind](#)' living lab which is part of the [Smart Cities Programme of Eindhoven University of Technology](#). This living lab investigates how crowds can be controlled and crime can be prevented by collecting data using smart sensors and smart interfaces in a lively part of the city

¹¹ For some examples, see Regional Court Overijssel 15 juni 2018, ECLI:NL:RBOVE:2018:2037; Regional Court Amsterdam 30 January 2018, ECLI:NL:RBAMS:2018:419; Regional Court Amsterdam 27 March 2017, ECLI:NL:RBAMS:2017:2424; Regional Court Almelo 28 October 2011, ECLI:NL:RBALM:2011:BU2930.

¹² Rb (District Court) Den Haag 5 February 2020, ECLI:NL:RBDHA:2020:865. For more information on the SyRI case, please see section I.5.1 below.

¹³ For another example, also of collaboration between large companies, see 'Kickstart AI: Five Dutch Companies to Further Boost Artificial Intelligence in the Netherlands', 2019: <https://www.aholddelhaize.com/media/9892/191010-final-press-release-kickstart-ai-eng.pdf>.

centre of Eindhoven.¹⁴ There is close cooperation between Eindhoven University, Philips, the municipality of Eindhoven, Brainport Eindhoven and several other parties. Similarly, Delft University collaborates with [Logius](#) (part of the Ministry for Internal Affairs), [ICTU](#) and [NL Digital](#) to create a 'Digicampus'. The Digicampus is meant to be a meeting place for academia, industry, government and citizens who are looking to innovate and collaborate in order to improve public services. The [abovementioned Police Lab AI](#) (a collaboration between the national police, the prosecutor's office, Utrecht University and the University of Amsterdam) also forms part of a broader collaboration between academia, the industry and government: the [Innovation Centre for Artificial Intelligence](#) (ICAI).

In October 2019, a new public-private partnership was launched: the Dutch AI Coalition ([Nederlandse AI Coalitie](#) – NL AIC).¹⁵ The initiative arose from representatives of the private sector (the Confederation of Netherlands Industry and Employers ([VNO-NCW](#)), entrepreneurs-organisation [MKB-Nederland](#) and tech industry employer's organisation [FME](#)), technology companies and other large private companies ([IBM](#), [Seedlink](#), [Philips](#), [Ahold Delhaize](#), FME), existing public-private networks ([Topteam Dutch Digital Delta](#))), the Ministry of Economic Affairs and Climate Policy, and TNO. It is a public-private partnership which aims to stimulate, support and – if necessary - organise Dutch activities in the field of AI with the objective of making the Netherlands a frontrunner when it comes to the know-how of utilizing AI for welfare and a better society. The aim is to stimulate as many public bodies and private actors to work together in this coalition. In its AI Strategy (see [below](#)), the government mentions NL AIC as an important player for achieving its objectives in the field of AI.

Another platform in the field of AI is the [Alliance for Artificial Intelligence](#) (ALLAI), which aims to be a platform for active involvement of stakeholders in achieving responsible AI.

1.1.8 Civil society

Civil society is well-organised in the Netherlands and often engages in public consultations on new policies and regulation (including technological policies) or in strategic litigation. Examples of non-governmental organisations who are particularly active in the field of AI, big data and fundamental rights are [Bits of Freedom](#), [Amnesty International](#) (which is active, for example, in the field of [ethnic](#)

¹⁴ See also: Saskia Naafs, "Living Laboratories": The Dutch Cities Amassing Data on Oblivious Residents', *The Guardian*, 1 March 2018, sec. Cities, <https://www.theguardian.com/cities/2018/mar/01/smart-cities-data-privacy-eindhoven-utrecht>.

¹⁵ For its action plan, see VNO-NCW, 'Algoritmen Die Werken Voor Iedereen Samen Bouwen Aan Onze (Digitale) Toekomst Met Artificiële Intelligentie: Position Paper - Taskforce A', 18 July 2019: https://www.vno-ncw.nl/sites/default/files/position_paper_algoritmen_die_werken_voor_iedereen.pdf.

[profiling](#)), [Privacy First](#), the Netherlands Committee of Jurists ([Nederlands Juristencomité voor de Mensenrechten](#) – NJCM) and the Civil Rights Platform ([Platform Burgerrechten](#)).

1.2 International relations

1.2.1 General strategy

Most provisions of international law as well as decisions of international organisations have direct effect on as well as priority over Dutch law (including over acts of parliament and even the constitution).¹⁶ Thus, the legal status of international law is – in fact – similar to the status of EU primary and secondary law. In line with this special status of international law and the intertwinement of the Dutch, European and global economies, the Netherlands is traditionally very active in international and European policy-making. Stimulating respect for fundamental rights and a human rights inclusive policy is recognised to be a core aspect of the Dutch contribution to international policy debates as was recently emphasised in a [policy brief on AI, fundamental rights and public values](#) (see also below, [section I.3.3](#)).¹⁷ In particular, many Dutch policy efforts are geared towards internet freedom and open internet governance.¹⁸

In keeping with this overall approach, the Netherlands is active in promoting responsible AI on the international and European level. [Several members of parliament have requested the government](#) to emphasise the ethical aspects of AI, to respect fundamental rights in the development and application of AI, and, more generally, for the government to strive for human-centric and responsible AI. This should not only be prioritized in national policies, but [also in European and international cooperation](#). In its recent Strategic Action Plan AI (see

¹⁶ See Articles 93 and 94 of the Dutch Constitution. For a further discussion of the interpretation of these provisions in English, see e.g. the chapter on The Netherlands in Fleuren and Gerards 2014 and see Gerards, Van Ommeren and Wolswinkel 2020 (forthcoming).

¹⁷ See generally the annual reports of the Ministry of Foreign Affairs on human rights policy; the 2018 annual report: Ministerie van Buitenlandse Zaken, 'Mensenrechtenrapportage 2018 - Inzet en resultaten buitenlands mensenrechtenbeleid', rapport, 29 May 2019, <https://www.rijksoverheid.nl/documenten/rapporten/2019/05/29/bijlage-kamerbrief-mensenrechtenrapportage-2018>. Freedom of expression and internet freedom are, for example, important priorities for Dutch foreign policy; see e.g. Ministerie van Buitenlandse Zaken, 'Vrijheid van meningsuiting, internetvrijheid en onafhankelijke journalistiek - Mensenrechten - Rijksoverheid.nl', onderwerp, 23 October 2012, <https://www.rijksoverheid.nl/onderwerpen/mensenrechten/mensenrechten-wereldwijd/vrijheid-van-meningsuiting-en-internetvrijheid>.

¹⁸ See for the Dutch activities in 2018 e.g.: Ministerie van Buitenlandse Zaken, 'Mensenrechtenrapportage 2018 - Inzet en resultaten buitenlands mensenrechtenbeleid'.

below, [section I.3](#)) the government has embraced this position. Additionally, in documents related to its foreign policy, the government has acknowledged that a human-centric, ethical and fundamental rights compatible AI has the full attention of the government. This can be seen, for example, in a [policy document preparing for its contribution to the Finnish chairmanship of the EU](#) in July 2019, where the Dutch government emphasised that it embraces the human-centric AI approach laid down in the European coordinated action plan AI.¹⁹ The government also emphasised in this document that strong legal protections are important when AI is used in policy affairs, and it stressed the importance of striking a careful balance between all legal, ethical and security interests involved in the design and application of AI. In addition, it mentioned the importance for the Netherlands of being able to conduct experiments and invest in AI innovation. In this respect, the government pointed to living labs such as the Police Lab AI where opportunities for the deployment of AI are investigated alongside the different aspects of legal protection and safeguards like explainable AI and transparency.

In accordance with this general approach, the Minister of Foreign Affairs announced in the [Explanatory Memorandum for the budget for the Ministry of Foreign Affairs for 2020](#) that – grounded in the ‘Digitalisation Vision for Foreign Affairs 2019-2022’ (*Digitaliseringsvisie voor BZ 2019–2022*)²⁰ – in 2020, the ministry will focus ‘on necessary innovations such as big data analyses and artificial intelligence, with attention for both the opportunities and the risks offered by digitalisation’. The Minister of Interior has emphasised in her [policy brief on AI, fundamental rights and public values](#) that the Netherlands in all its international relations should propagate the importance of respecting fundamental rights and public values in developing and using AI. The country should aim to do so by offering ‘best practices’ and allow human centric AI to become an essential export product.

The Digital Agenda for Foreign Trade and Development Co-operation ([Digitale Agenda voor Buitenlandse Handel en Ontwikkelingssamenwerking](#) – Digital Agenda BHOS), which the ministry of Foreign Affairs presented to Parliament in June 2019, reflects a similar stance. Though the Digital Agenda BHOS mentions several opportunities of AI and new technologies, such as realising the SDGs through improved food production, increased productivity and allowing for more inclusiveness and freedom as well as emancipation, it also mentions risks for these same rights (in particular inclusiveness and social and economic rights) as well as for security, privacy and data protection. It is mentioned in the Agenda that Dutch foreign trade policy should show awareness of both opportunities and risks. In this respect, the ministry proposes that the Netherlands forms new, or joins existing, international

¹⁹ See further the EU Communication [Building Trust in Human-Centric Artificial Intelligence](#).

²⁰ This document is not to be found in open sources, but it is likely that this concerns the Digital Agenda for Foreign Trade and Development Co-operation (see below).

coalitions and networks (e.g. the [Digital4Development Coalition](#), the [International Development Innovation Alliance](#), the [eTrade for Women Network](#)) and uses its position in the G20, OECD, WTO and other international bodies to increase knowledge and explore possible action lines. It is further emphasised in the Agenda that in its international trade policy, the Netherlands always wants to propagate the need to respect European values and ethical norms. Special international policy efforts should be made in relation to freedom of expression as well as the protection of persons and NGOs who aim to contribute to fundamental rights protection in the digital world. In this respect, strong support is expressed for the [Digital Defenders Partnership](#) and the need to build international coalitions to protect personal data and respect for privacy rights.

In its Strategic Action Plan AI (SAPAI, see [section I.3](#)) the government mentioned its strong support for several European initiatives regarding AI, in particular the [Ethical Guidelines of the High-Level Expert Group for trustworthy AI](#). Together with the Dutch AI Coalition (see [above](#)), the government will actively stimulate private companies and public bodies and agencies to take part in the pilots for these guidelines. In addition, the SAPAI notes that the Netherlands is chairing a European Commission working group that will present an opinion on AI and gender in 2020 and that the Ministry of Foreign Affairs will investigate what has so-far been laid down about AI in international trade agreements and what changes might be required to bring these in line with European public values. The Minister of Interior further noted in her recent [policy brief on AI, fundamental rights and public values](#) that the Netherlands actively takes part in EU activities giving shape to the AI strategy contained in the European Commission's [Coordinated Action Plan](#).

1.2.2 European linkages – Council of Europe and OECD

In her recent [policy brief on AI, fundamental rights and public values](#), the Minister of Interior emphasised that the Netherlands is active in the Council of Europe stimulating the development of policy instruments intended to safeguard fundamental rights in the era of digitisation. In the Council of Europe framework, the Dutch Rathenau Institute (see [above](#)) has presented a [research report on human rights in the robotic age](#) reporting on challenges to fundamental rights arising from the use of robotics, AI and virtual and augmented reality. This report was commissioned by the Parliamentary Assembly of the Council of Europe (PACE) in preparation of the [PACE report on technological convergence, artificial intelligence and human rights](#) which was adopted on 28 April 2017.

The Dutch expert Prof. Frederik Zuiderveen Borgesius prepared a study on [discrimination, artificial intelligence and algorithmic decision-making](#) for the Council of Europe's [European Commission against Racism and Intolerance](#).

Another Dutch expert, Prof. Natali Helberger was elected in 2018 as a member of the Council of Europe's Committee of Experts on Human Rights Dimensions of Automated Data Processing and Different Forms of Artificial Intelligence ([MSI-AUT](#)). The task of the MSI-AUT is to prepare standard-setting instruments (in form of Committee of Ministers recommendations or declarations) on the basis of a study on the human rights dimensions of automated data processing techniques (in particular algorithms and possible regulatory implications).²¹ MSI-AUT studies the development and use of new digital technologies and services, including different forms of artificial intelligence.²² MSI-AUT forms part of the Council of Europe's [Steering Committee on Media and Information Society](#).

In terms of policy contributions, it is notable that on 11 September 2019 the Council of Europe established an [Ad Hoc Committee on Artificial Intelligence \(CAHAI\)](#), inviting Council of Europe member states to appoint one or more representatives of the highest possible rank with recognized expertise in the field of digital governance and the legal implications of the functioning of different forms of AI relevant to the Council of Europe mandate. In 2019, the Netherlands was represented at the first CAHAI meeting.

Furthermore, the Netherlands has signed the [Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data](#) ('Convention 108+', CETS no. 223) in [October 2018](#).

In respect to the OECD, the Netherlands has announced in the aforementioned [2019 policy agenda for digitalisation in international trade and development co-operation](#) that it will urge the OECD – as the main forum for business and human rights – to take steps to clarify the OECD guidelines on the digital economy. In particular it should be explained how private companies may map the risks of misuse and avoid such risks, with a focus on companies responsible for maintaining and removing online content.

1.2.3 International linkages – G20

As member of the G20, the Netherlands has supported the 'Society 5.0' agenda Japan presented at the Osaka G20 meeting in June 2019, which contains an inclusive and human-centric approach to technology. In a [report presenting the outcomes of the G20 meeting](#), the government explained to parliament that Japan strived to connect AI and sustainability goals and it connected trade and the digital economy in a

²¹ IVIR, 'Prof. Dr. Natali Helberger Elected Member of a Council of Europe Expert Committee on Human Rights Dimensions of Automated Data Processing and Artificial Intelligence', 2019 2018, <https://www.ivir.nl/helberger-elected-to-council-of-europe-expert-committee/>.

²² Idem.

'useful manner'. In addition, the government reported that it had supported the joint [Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism](#) initiated by Australia. In its report, the government further mentioned that it would be important for the Netherlands to find a balance, on the one hand, the need to combat terrorist propaganda and, on the other hand, respect human rights and fundamental freedoms such as the freedom of expression on the internet. According to the government, this balance was well-reflected in the statement.

1.3 National strategies and guidelines

1.3.1 Strategic Action Plan AI (SAPAI)

On 8 October 2019, the government presented its [Strategic Action Plan AI \(Strategisch Actieplan AI – SAPAI\)](#) under the responsibility of the Ministry of Economic Affairs and Climate Policy. SAPAI contains various strategies and policy plans to ensure that AI is optimally and sustainably used in the Netherlands, that the Netherlands plays a central role in innovation and technology, and that public values are guaranteed and protected. SAPAI is intended to be a 'rolling agenda' that will be updated on a yearly basis. It builds off the Digital Government Agenda 2019 (see [below](#)) and is meant to be read in close connection to that Agenda. In addition to a description of actions that are already taken and priorities to be set, SAPAI contains a list of action points as well as a concrete budget proposal to invest in research and innovation into AI and AI applications.

SAPAI proceeds along three tracks with the third track being most relevant to fundamental rights. For each track, several core objectives have been formulated that are to be realised in the upcoming years:

Track 1: Using societal and economic opportunities

- AI is used to respond to societal challenges.
- All public bodies make optimal use of AI in exercising their tasks.
- AI entrepreneurship is stimulated.

Track 2: Creating the right conditions

- AI research and innovation must be of high quality and must be leading in Europe.
- Excellent education possibilities are realised that allow the Netherlands to 'live together with AI' and boost talent to work with AI.
- More useable data are made available for AI applications to realise better AI developments.

- The Netherlands has a prime position in Europe regarding high-quality digital and intelligent connectivity for effective AI-applications.

Track 3: Strengthening the foundations

- Public values and fundamental rights are protected.
- AI is used in a manner that can be trusted by all.
- Markets are open and competitive and offer sound consumer protection.
- The safety and security of citizens, companies and public bodies in the Netherlands are protected.

In relation to these tracks and objectives, some specific plans and strategies can be highlighted:

Using societal and economic opportunities

SAPAI emphasises the value of AI in responding to numerous societal challenges in specific domains or sectors, such as security and judicial administration, health and healthcare, agriculture and food production, energy transition and sustainability. The strategy emphasises that the potential of AI can be realised in particular by means of a Dutch strength: public-private partnerships and creating a fruitful environment for experiments, pilots and living labs. The Dutch AI coalition (see [above](#)) is to play a special role in realising this potential. The strategy will accommodate and facilitate such public-private partnerships and experiments in a variety of ways. In particular, start-ups and scale-ups will be stimulated (in particular if they work with human-centric AI) by, for example, creating a favourable financial and economic climate and involving them in projects conducted by large companies and public-private partnerships.

Creating the right conditions

SAPAI mentions a variety of actions to be taken to stimulate research and innovation regarding AI, including a number of financial injections and investments. The government wants to continue its participation in European programmes such as Horizon Europe, Digital Europe and Eureka, and it aims to strengthen its co-operation with other EU member states by means of, for example, the Holland Innovation Network. SAPAI also emphasises the importance of participation in CLAIRE, the Confederation of Laboratories for AI in Europe, which is based in The Hague. In addition, the government strives to co-operate bilaterally with specific states (e.g. Germany, France, Singapore, the US and Belgium).

Besides this, the government mentions that changes need to be made in educational programmes, both in primary and secondary schools, and in professional training in order to ensure that sufficient workers are available who can develop and use AI (applications). In addition to this, strong investments need to be made in promoting digital skills on all levels of education.

The government's aim is to have sufficient data made available for AI development and applications, in particular by creating systems that allow for secure data sharing between companies. In addition, the Netherlands will invest in high-quality digital connectivity, for instance, by collaborating with other EU member states in the field of research and innovation of High Performance Computing. Further actions are to be announced.

Strengthening the foundations

SAPAI pays considerable attention to the need to protect public values and fundamental rights. It specifically mentions five categories of rights for which AI is considered to be a particular risk:

- The prohibition of discrimination (caused by, for instance, biased data, biases in the algorithms or biases in classifications made by algorithms).
- The protection of privacy (in particular in the context of the processing of personal data in technologies such as facial recognition and big data analyses).
- The freedom of expression and information (in particular in the context of personalisation and ordering of search results, as well as automated content removal).
- The right to human dignity and personal autonomy (in particular because of the risk for dehumanisation and the influence of AI on human decision-making).
- The right to a fair trial (which could be at risk if it is not clear which algorithms are used to make a decision or which assumptions and data have influenced decisions, and because of threats to the principle of equality of arms).

The baseline of SAPAI is that protection of fundamental rights and public values is just as important in the digital age as it was before. According to the government, a strong legal basis for protection of these fundamental rights is provided in existing legislation (see [hereafter](#)). Nevertheless, specific actions will be taken in this regard:

- The Ministry of Social Affairs and Employment will create an action plan to prevent and reduce discrimination in the employment market; part of this will be the creation of algorithms to trace specific forms of discrimination in the texts of job advertisements.
- Several further studies into the impact of AI on public values have been commissioned (see [below](#); this is also part of the Digital Government Agenda 2019, also discussed [below](#)).
- The Ministry for Legal Protection will explore the desirability of a system of certification for AI applications in the field of administration of justice; accreditation of the competent certification institutes should take place on the European level.

- The Ministry of Interior will establish a transparency lab for government bodies, allowing for knowledge exchange and support in relation to transparency, explainability and accountability.
- Further studies will be conducted into how public bodies decide whether or not to publish information on the working of the algorithms they use.

In addition, SAPAI emphasises the crucial need for AI to be trustworthy and human-centric. The government regard this as a unique proposition for Europe's international position and for its profile in e.g. the Council of Europe, OESO, G20, UNECE and UNESCO. On the national level, trustworthy and human-centric AI requires that AI is applied within appropriate ethical and legal frameworks and that it is transparent how the different stakeholders utilise AI. It is also considered important that there is adequate oversight and monitoring regarding compliance with the legal framework and the principle of proportionality, and that it is clear who can be held responsible for possible damage done by AI applications. The government points out that the most important relevant legal framework is constituted by the GDPR and the equal treatment legislation (see hereafter, [section II](#)) as well as by ethical codes such as that developed by the European AI High-Level Expert Group. It is emphasised that private parties have to comply with such standards and should be involved in taking further steps to translate these rules and standards to everyday practice. The government, together with the AI Coalition (see [above](#)) aims to involve as many companies and public bodies/agencies as possible in the pilots run by the European AI High-Level Expert Group to develop and test its ethical code. In addition, a 'mission-driven', pilot- and experiment-based approach will be taken to develop ethically responsible AI applications in public-private partnerships and investments will be made in innovation and research into explainable and responsible AI. Similarly, the government wants to stimulate research into the question how to deal with AI that has been developed outside the European Union which may be based on different value systems.

According to SAPAI, it is further important to ensure that AI applications are controllable, in particular if they have legal effects, if they have considerable impact on human beings or society, or if there are limited possibilities for human intervention and control. This is further explained in a government brief to parliament that was published in October 2019 containing a set of guidelines for application of algorithms in data-drive applications by public bodies which will be discussed in detail [below](#). To address these potential risks, stakeholders may be required to inform people that AI is used and they may be asked to give insight in the way the AI system has been developed and in matters of responsibility and accountability. The government emphasises that this requirement follows from the GDPR which contains transparency and information obligations for those agents that collect, process and use personal data,

as well as from consumer legislation that requires that individuals must be able to make an informed choice between different services or goods. For public bodies and agencies, information obligations may also follow from the unwritten general principles of good administration and good governance and from the legislation on open government. It is up to the Authority for Consumers and Markets and the Data Protection Authority (see [above](#)) to check if these legal obligations are met. In addition, investments should be directed at possibilities for offering technical transparency as well as explainable AI. Support will be given to initiatives such as trusted third parties that can carry out audits on algorithms, the use of the AI Impact Assessment (see below, section I.4), and the introduction of certificates for responsible AI. To avoid uncertainty and increase consistency, the government will support internationally harmonised general standards that do justice to European public values and it will invite the [NEN-norm Commission AI](#) to share good practices and develop a framework for reliable and ethically responsible AI applications to contribute to the development of global AI norms by the [International Organisation for Standardisation](#). To the extent that it turns out that companies do too little to protect these values, the government will consider introducing further legislation to protect these values, for example regarding specific sectors. As an example, the government mentioned the requirements introduced by [MiFID II](#) for transparency and explainability that have to be met by companies using trading algorithms.²³

Finally, being aware of the role played by big tech companies in this particular field, the government proposes as part of SAPAI that a European authority is introduced that is competent to impose ex-ante obligations on big gatekeeping platforms that have an impact on consumers and entrepreneurs. It also embraces the [European Commission proposal to modernise consumer protection](#) in order to allow individuals to make well-informed, conscious choices without being unduly guided by information asymmetries, and it supports the European initiatives in protecting [intellectual property rights in the digital single market](#) and in [modernising patent law](#).

1.3.2 Digital Government Agenda 2019

Before the Government published its Strategic Action Plan AI (SAPAI), it already presented an overall strategy on 'digitalisation' in 2019, the Digital Government Agenda 2019 ([Agenda Digitale Overheid 2019](#)). This agenda addresses the development and application of AI, big data analysis, algorithms and related technologies. It focuses on a wide range of policies and measures, ranging from legislation to education and from stimulating further research to government participation in 'living labs'. Similar to SAPAI, a core element of the Digital Government Agenda is

²³ Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, OJ L12 June 2014 p. 349-496.

the awareness that the opportunities offered by the digital society should be grasped, yet the autonomy and rights of individual citizens should be respected.²⁴

The Digital Government Agenda rests on five pillars:

- [*Investing in innovation*](#), for instance by means of supporting the AI research agendas of NWO (see above) and the Digital Society agenda of the VSNU (see above); supporting public-private partnerships working in the field of AI (see above); promoting skills and knowledge within the government (including algorithms, ethics and application of new technologies); and supporting knowledge exchange between universities and the government in relation to the Innovation Centre for AI (see above) ([*ICAI*](#), see above).
- [*Protecting fundamental rights and public values*](#), for instance by stimulating a societal debate on the effects of new technologies; creating a toolbox on responsible entrepreneurship ('ethics by design' for the private sector); drafting guidelines and guarantees for responsible use of algorithms by the government; drafting legislation regarding algorithmic profiling by the government; commissioning various research reports on the potential effects of AI for fundamental rights and rule of law values; providing strategic surveys to identify the legal, technological and ethical consequences of new developments at an early stage.
- [*Enhancing accessibility, understandability and inclusion*](#), for instance by investing in increasing digital competences and digital awareness within the entire population (in particular people with limited digital skills); creating new educational programmes for primary and secondary education; increasing accessibility of government websites; investing in a public-private partnership on a 'digi-competent' country ('Alliance Digital Living Together' – [*Alliantie Digitaal Samenleven*](#)); increasing data control for citizens and entrepreneurs; and investing in a Dutch version of the basic digital [*AI-course*](#).
- [*Personalising government services*](#), for instance by modernising government gateways to make them more accessible and allow citizens better access to their personal data, focussing on the quality of digital correspondence and guaranteeing secure information and services.
- [*Being ready for the future*](#), which means mainly that the Agenda is intended to be a 'rolling document' that will constantly be renewed and changed to reflect new developments.

To the extent that the Digital Government Agenda relates to fundamental rights and public values that are relevant for AI, further detail can be found in the Strategic Action Plan AI, which has been discussed [above](#).

²⁴Digital Government, 'Digital Government Agenda: NL DIGIbeter', accessed 20 March 2020, <https://www.nldigitalgovernment.nl/digital-government-agenda/>.

1.3.3 Other policy briefs relevant for AI and fundamental rights

As a basis for the Agenda and SAPAI and their follow-up, the government has invested in commissioning a number of research reports and follow-up reports.²⁵ To the extent that these reports have already been completed, they have been presented to parliament with an official response by the responsible minister(s) containing plans for follow-up measures and policies. Most of the findings of the reports and the government's responses have now been brought together in SAPAI, but it is worth mentioning some examples that have been particularly influential and relevant in drafting SAPAI. In addition, various ministries have been engaged in drafting policy briefs on specific topics setting out a variety of policy measures that can or will be taken:

- On the same day SAPAI was presented (8 October 2019), the Ministry of Interior presented a policy brief to parliament on [AI, public values and fundamental rights](#). The policy brief mentions that it should be read together with SAPAI and the brief on safeguards against the risk of data analysis conducted by public bodies (see below, next bullet). The brief further builds on the government's response to the report on algorithms and fundamental rights (see also below), it contains a response to another research report by the Rathenau Institute on [protecting public values in the digitised society](#) and it answers to requests for policy measures made by several members of parliament. It stresses that a human-centric approach must be chosen where AI-applications have a strong influence on human beings or on society as a whole. This means that respect for public values based on fundamental rights is essential, although this also might create dilemmas to the extent that fundamental rights or public values conflict; in that case, careful balancing is needed. The policy brief lists the most important risks of AI for fundamental rights (such as discrimination as a result of biased data, or reduction of interpersonal relations if AI takes over certain forms of interaction). Aware of all policy efforts in the field, the Minister of Interior mentions in the brief that these policies will be the more effective if they are conducted in a coherent fashion, if they are concretised as much as possible, if monitoring mechanisms are reinforced and if policy objectives are shared on the European and international level.
- To avoid fragmentation and undue overlap, the ministry will establish a collaboration platform for the government on the topic

²⁵ For a full list of all policy activities and commissioned projects in the field of AI and public values, see Digitale Overheid, 'Planning Agenda Digitale Overheid'. See also the narrative overview presented in the policy brief of the Minister of the Interior on AI, fundamental rights and public values: Tweede Kamer der Staten-Generaal, 'AI, publieke waarden en mensenrechten', Text, 8 October 2019, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail/2019Z19125/2019D39850.

of AI and public values which will enable knowledge exchanges, facilitate coherence and allow for connections to be made with researchers.

- To enhance concretisation, the ministry will develop 'concrete use' cases to see how public values and fundamental rights can be operationalised as system principles, which then will be presented to government bodies, agencies and private parties; this will start with non-discrimination.
- To reinforce monitoring mechanisms, the Ministry of Interior and the Minister for Legal Protection will assess whether the present monitoring bodies are sufficiently equipped to supervise the use of algorithms and whether any blind spots exist. In addition they will stimulate the already existing collaboration between the various supervisory and monitoring bodies.
- In its European and international policy efforts, the Netherlands will propagate the importance of human-centric AI and the need to respect for public values.

The policy brief contains an annex explaining the risks and opportunities of AI for various groups of fundamental rights (the prohibition of discrimination, privacy and data protection, freedom of expression, human dignity, personal autonomy and procedural rights) and listing the various policy initiatives and efforts that are already undertaken in relation to these groups of rights. In addition, the annex contains a list of general policies to protect public values and fundamental rights in relation to AI-developments, such as policies in the field of education and disinformation, self-regulation and ethical codes, and international co-operation.

- On the same day SAPAI was presented, the Ministry of Justice and Security presented a policy brief to parliament about guidelines offering [safeguards against the risks of data analyses conducted by public bodies](#). This is partly a follow-up to the policy brief on transparency (see below) and partly a response to a research report prepared by the WRR (see [above](#)) on [big data in a free and safe society](#). It explains the different types of algorithms that can be used by public bodies and agencies as well as a number of core requirements (such as explainability, auditability, responsibility and controllability) that have to be met if public bodies or agencies want to make use of AI.
- In response to a research report on [algorithms and fundamental rights](#), a [policy brief](#) has been presented by the Minister of Interior to parliament in March 2019 offering an overview of relevant policy measures and announcing a number of projected initiatives to deal with the risks identified in the report.
- A [policy brief on transparency](#) has been presented to parliament in October 2018 containing a framework and a set of relevant factors in determining the degree to which transparency can be offered in the use of algorithms by the public bodies and agencies.

- A [policy brief on AI and algorithms in judicial administration](#) has been sent to parliament in 2019, identifying relevant experiments and initiatives in relation to the use of AI in judicial administration (which is a broad notion that encompasses judicial decision-making, prosecution of crime and immigration matters). The brief also offers an overview of a variety of opportunities and risks as well as lists a number of policy measures and possibilities for taking concrete action (such as the introduction of an Innovation Team at the Ministry of Justice and Security).
- The Minister for Justice and Security sent a [policy brief on the use of AI by the police](#) to Parliament on 3 December 2019. This policy brief describes examples and opportunities of the use of AI for prevention and detection of crime, as well as explains how risks for interferences of fundamental rights should be dealt with. It is emphasised that it is always necessary to have a 'human in the loop', to safeguard algorithmic transparency and quality (e.g. by validation processes), and use the National Police Lab AI to stimulate further research and experiments into human centred and ethical AI. In addition, it is mentioned that the national police has developed an internal quality framework for big data that helps to safeguard the quality of the development and use of AI by the police. This is monitored by the Inspection for Justice and Security (*Inspectie JenV*) and the Data Protection Authority (*Autoriteit Persoonsgegevens* – AP) which also check compliance with legislation such as the GDPR.
- Separate policy briefs have been presented to parliament on [digital inclusion](#) (December 2018) and [protection of horizontal privacy](#) (June 2019). These mainly concern the collection and protection of personal data, but also, for example, a risk analysis concerning facial recognition technology.
- Several research reports on AI and public values have been commissioned of the WRR, WODC, and universities, which are still forthcoming; they are mentioned in the SAPAI (p. 42), which was discussed [above](#).

1.4 Standards and voluntary guidelines; the role of the private sector

Next to the relevant international and national binding norms and legislation that have been discussed above, various AI-related standards, soft law, ethical codes and voluntary guidelines are available in the Netherlands.

1.4.1 Government standards and guidelines

Some relevant standards and guidelines are provided by the government. Particularly worth mentioning are the following examples:

- The recent [policy brief on offering guarantees against the risks of data-analyses by public bodies](#) contains an annex setting out [Guidelines for the application of algorithms by public bodies](#). These guidelines concern issues such as awareness of the risks of using algorithms, explainability, data recognition, auditability, responsibility, accountability, validation, and controllability. It also contains a description of different types of algorithms (arranged according to their complexity and technical transparency), their different uses (descriptive, diagnostic, predictive and prescriptive), and their potential impact. Depending on the nature of the algorithms used, the purpose of their use and their impact, the document contains guidelines for public bodies as to how to guarantee, for example, explainability or accountability, as well as to how to inform the general public and offer transparency. It is also explained that the guidelines are particularly relevant to data-analyses that concern profiling (in the understanding given to that notion by the GDPR) and territory-based analyses (e.g. predictive policing in specific neighbourhoods) in relation to which also personal data are processed and which give rise to similar risks as profiling.
- The [Roadmap Digitally Safe Hard- and Software](#) contains minimum safety requirements for, amongst others, Internet of Things devices, which also include measures to prevent privacy interferences by e.g. voice recognition.
- Under development is a [toolbox for ethics by design](#) that will be developed as part of the Digital Government Agenda. It contains an impact assessment and a number of practical standards and guidelines to help government agencies and decentralised bodies to innovate in a responsible manner (i.e., with an eye to public values, transparency, democracy, rule of law values, data protection, fundamental rights and the like).
- Also under development is a *Manual Legislation and ICT*, which is to contain good practices on the use of ICT in legislation.²⁶ This manual may also trigger changes to be made to the important *General Guidelines on Legislation*, to which all legislation has to conform, and the *Integral Framework for Drafting Legislation and Policy-making* so as to raise awareness with policy-makers and lawyers involved in drafting legislation as regards the potential consequences of using new technologies (including AI and algorithms) by government bodies.
- The [Supervision Framework](#) of the Data Protection Authority contains some guidelines as to the use of personal data in AI driven technologies.
- The [Code for Good Public Administration](#) in the future will also include guidelines concerning privacy issues related to the further development of, for example, smart cities.²⁷

²⁶ Digitale Overheid, 'Kamerbrief met reactie op UU-rapport Algoritmes en grondrechten'.

²⁷ Digitale Overheid.

- The [Guidelines on transparency under Regulation 2016/679](#) of the Article 29 Data protection working party are specifically mentioned in the governments transparency policy brief as a relevant document that also should be taken into account in the Netherlands.²⁸

1.4.2 Self-regulation in the private sector

In addition to the government standards and guidelines there are several initiatives by private companies to engage in self-regulation and develop ethical codes.²⁹ An example is an initiative taken by the Dutch ICT sector to develop an [ethical code for Artificial Intelligence](#).³⁰ More than [600 member companies of NL Digital](#) support this ethical code, which, *inter alia*, means that they undertake to show awareness of the influence of AI on public values and the need to minimise undesired bias and promote inclusive representation.

Relatedly, the Platform for the Information Society (ECP) has developed an [AI impact assessment](#) and an [ethical code](#) that can be used both by government bodies and by private companies.³¹ About 130 companies and government bodies participate in the ECP, amongst which are major platforms and technology companies such as Facebook, eBay, Microsoft, bol.com and Google, the port of Rotterdam, large retailers like Albert Heijn, power companies like Tennet and associations such as the [Association for ICT organisations in the healthcare sector](#) and the [Association of health insurance companies in the Netherlands](#).

The Netherlands norm-drafting institute NEN has introduced a [norm commission in relation to AI and Big Data](#). Through this commission, NEN aims to influence [ISO standardisation norms in the field](#), amongst others with the aim of reducing bias in AI-systems, risk management in AI, trustworthiness and robustness of AI.³²

In her recent [policy brief on AI, fundamental rights and public values](#), the Minister of Interior emphasised that the Dutch government expects of companies in the Netherlands that they act in compliance with the [UN](#)

²⁸ Ministerie van Justitie en Veiligheid, 'Kamerbrief over motie transparantie van algoritmes in gebruik bij de overheid - Kamerstuk - Rijksoverheid.nl', kamerstuk, 9 October 2018, <https://www.rijksoverheid.nl/documenten/kamerstukken/2018/10/09/tk-transparantie-van-algoritmes-in-gebruik-bij-de-overheid>.

²⁹ A list of initiatives in the US and Europe can be found in a 2019 report by the Rathenau Institute containing an overview of ethics codes and principles of AI: Rathenau Instituut, 'Overview of ethics codes and principles for AI', 19 March 2019, <https://www.rathenau.nl/en/digital-society/overview-ethics-codes-and-principles-ai>.

³⁰ NLdigital, 'Nieuwe ethische gedragscode AI voor ICT-sector', 21 March 2019, <https://www.nldigital.nl/news/nieuwe-ethische-gedragscode-ai-voor-ict-sector/>. An English language version of the code is available at <https://www.nldigital.nl/wp-content/uploads/2019/04/NEDERLAND-ICT-ETHICAL-CODE-FOR-ARTIFICIAL-INTELLIGENCE.pdf>.

³¹ ECP, 'Artificial Intelligence: Whitepaper: Gespreksstof En Handvatten Voor Een Evenwichtige Inbedding in the Samenleving', 2018.

³² See the policy brief of the Minister of the Interior of 8 October 2019, p. 9-10: Tweede Kamer der Staten-Generaal, 'AI, publieke waarden en mensenrechten'.

[Guiding Principles on Business and Human Rights](#). Consequently, in designing or purchasing AI-applications, they should be aware of any potentially negative impact on fundamental rights and take measures to prevent or repair such interferences. Companies should bear their own responsibility in doing so.

Finally, some private initiatives have been taken to draft guidelines and standards for responsible AI and responsible data collection. An example is [RESPECT4U](#), which is a set of guidelines for privacy-by-design developed by TNO (see above, section *I.1*). Companies may download and use these guidelines for free without having to become a member of an association or a platform. Similarly, the [Guidelines Privacy by Design](#) have been developed by the Centre for Information Security and Privacy Protection ([Centrum voor Informatiebeveiliging en Privacybescherming](#) – CIP), which is a public-private partnership. These guidelines contain a step-by-step guide that can be used by companies who want to comply with privacy by design requirements.³³

1.5 Sample recent cases

It is clear from the above that there are many public and private initiatives to stimulate responsible AI and that show awareness of the positive effects as well as the risks of AI for public values such as fundamental rights. Dutch media often report on new technology and related human rights issues, and major newspapers all have knowledgeable technology journalists. The media are very active in reporting on related matters. A few recent examples are mentioned below.

1.5.1 System for Risk indication (SyRI)

Much media attention has been generated surrounding SyRI (System for Risk Indication, [Systeem Risico Indicatie](#)). SyRI is a system which allows a predictive algorithm to search the data of residents in certain municipalities for patterns that could indicate social security fraud. A number of civil society organisations and two well-known writers/columnists brought proceedings in the Dutch civil courts concerning data protection issues allegedly involved in the legislation that allowed for the development and use of SyRI, which generated quite some media attention at the time it was started in 2018.³⁴ The court

³³ The guidelines can be downloaded from the government's website; <https://www.rijksoverheid.nl/documenten/rapporten/2018/02/19/handleiding-privacy-by-design>.

³⁴ See e.g. Trouw, 'Tommy Wieringa wil niet dat de overheid zijn risico meet', 12 January 2018, <https://www.trouw.nl/gs-b58f21b5>; RTL Nieuws, 'Staat gedagvaard om "ondoorzichtige" risicoanalyses burgers', 27 March 2018,

hearing in October 2019 also attracted considerable attention.³⁵ SyRI further generated a lot of media coverage in the summer 2019 when it turned out that the programme could have the effect that persons living in 'poor' neighbourhoods were more likely to be monitored for fraud risks than persons living in richer neighbourhoods.³⁶ In relation to the findings of these risks of profiling, the municipality of Rotterdam stopped its experiments with SyRI in July 2019.³⁷

The district court of The Hague handed down its judgment on the SyRI legislation on 5 February 2020.³⁸ The parties had invoked Article 8 ECHR, Articles 7 and 8 EU Charter of Fundamental Rights and Articles 5, 6, 13, 14, 22 and 28 of the GDPR, but the district court decided to deal with the case under Article 8 (2) ECHR only, read in the light of the principles laid down in EU-law (in particular the Charter and the GDPR).³⁹ It held that it had few possibilities to really establish the correctness of the states' position on the legitimacy of SyRI because the state did not publish the risk model and risk indicators that were part of it. In the procedure before the court, the state further had not advanced any objectively verifiable information that would allow the court to assess the state's allegations regarding 'what SyRI is'.⁴⁰ Nevertheless, the district court considered it sufficiently established that SyRI allowed for the processing of large sets of structured data derived from different sources and that it aimed to search for correlations and patterns in these data. The SyRI legislation thereby enabled the use of predictive analyses, deep learning and datamining, although the court did not find it established that such use was currently made.⁴¹ The district court further found it clear that the legislation did not provide for any

<https://www.rtlnieuws.nl/tech/artikel/4128921/staat-gedagvaard-om-ondoorzichtige-risicoanalyses-burgers>.

³⁵ E.g. Charlotte Huisman, 'Rechter buigt zich over omstreden snuffelprogramma dat fraude via computers moet ontdekken', de Volkskrant, 29 October 2019, <https://www.volkskrant.nl/gs-ba4fb626>; Kristel van Teeffelen, 'Frauderisicosysteem SyRI schendt privacy niet, zegt de staat', Trouw, 29 October 2019, <https://www.trouw.nl/gs-be3f90e3>; Camil Driessen, "'Willen we dat de overheid zo met burgers omgaat?'", NRC, 28 October 2019, <https://www.nrc.nl/nieuws/2019/10/28/willen-we-dat-de-overheid-zo-met-burgers-omgaat-a3978217>; Joost Schellevis, 'Rechtszaak over fraudebestrijding overheid: "Burgers bij voorbaat verdacht"', 29 October 2019, <https://nos.nl/l/2308110>; FD.nl, 'Mag de Staat Gluren in de Watermeter?', accessed 21 March 2020, <https://fd.nl/economie-politiek/1322434/mag-de-staat-gluren-in-de-watermeter>; NOS, 'VN-rapporteur zeer bezorgd over Nederlands opsporingssysteem voor uitkeringsfraude', 21 October 2019, <https://nos.nl/l/2307132>.

³⁶ See e.g. Charlotte Huisman, 'SyRI, het fraudesysteem van de overheid, faalt: nog niet één fraudegeval opgespoord', de Volkskrant, 27 June 2019, <https://www.volkskrant.nl/gs-b789bc3a>; Jochem van Staalduine, 'De Rotterdamse huishoudens die verdacht worden van fraude zijn diep beledigd: "Het lijkt wel '40-45"', Trouw, 20 June 2019, <https://www.trouw.nl/gs-be0bd77f>.

³⁷ Charlotte Huisman, 'Rotterdam stopt omstreden fraudeonderzoek met SyRI', de Volkskrant, 3 July 2019, <https://www.volkskrant.nl/gs-becb336a>.

³⁸ Rb (District Court) Den Haag 5 February 2020, ECLI:NL:RBDHA:2020:865.

³⁹ See paras. 6.37-6.41 of the judgment. See also para. 6.65.

⁴⁰ Para. 6.49.

⁴¹ Para. 6.63.

information obligations regarding the persons' whose data was processed in the system. The district court expressly mentioned that it did not want to answer the question whether the system involved automated decision-making. Based on these elements, the district court found that the system had significant impact on individuals' private lives and thus constituted an interference with Article 8 (1) ECHR.⁴²

Although the district court expressed its doubts regarding the accessibility and foreseeability required under Article 8 (2) ECHR, it did not want to fully decide this issue because it considered it more important to deal with the case under the requirement of Article 8 (2) ECHR that the interference be necessary in a democratic society.⁴³ In that respect, it emphasised that the aims pursued were of considerable weight and importance, since fighting social security fraud serves a weighty economic interest and also affects the integrity of the economic system as a whole as well as the public trust in financial institutions. This meant that, as such, there was a pressing social need to introduce a system such as SyRI. However, the chosen instrument to serve these objectives did not meet the requirements of necessity and proportionality. The district court emphasised the lack of transparency of the system and the difficulties involved in auditing its working and effects.⁴⁴ It also indicated that there might be a discriminatory and stigmatising effect to the extent that it had been convincingly shown by the plaintiffs that SyRI led to heightened supervision in certain problem neighbourhoods.⁴⁵ The district court further found that the principles of data minimalization and purpose limitation had not sufficiently been respected,⁴⁶ and that there had been no independent and integral assessment of the data protection risks before the use of SyRI in concrete situations.⁴⁷ For those reasons, it declared the relevant provisions of the SyRI legislation to be invalid because of their incompatibility with Article 8(2) ECHR.⁴⁸

The judgment generated significant media attention.⁴⁹ On 23 April 2020, the [state announced](#) that it would not make use of its right of appeal, which means that the judgment has become final. In its [press release](#) explaining its choice not to appeal, the state explained that it accepted that SyRI did not meet the requirements of respect for the privacy rights of individuals.⁵⁰ Because of the importance of fighting social security

⁴² Para. 6.65.

⁴³ Para. 6.72.

⁴⁴ Paras. 6.90 and 6.95.

⁴⁵ Para. 6.92.

⁴⁶ Paras. 6.95ff.

⁴⁷ Para. 6.106.

⁴⁸ Para. 7.2.

⁴⁹ To mention just a few examples: 'Rechter geeft staat een oordeel om gebruik SyRI', *Financieel Dagblad* 5 February 2020; 'Privacyvoorvechters krijgen SyRI via rechter verboden', *NRC Handelsblad* 5 February 2020; 'Overheid stopt met omstreeden computersysteem SyRI na uitspraak rechter', *Trouw* 5 February 2020.

⁵⁰ See also the letter of the Secretary of State to the Parliament of 23 April 2020, <https://www.rijksoverheid.nl/documenten/kamerstukken/2020/04/23/kamerbrief-naar-aanleiding-van-vonnis-rechter-inzake-syri>.

fraud, however, it announced that it would investigate new technological tools to do so in an effective manner while respecting individual privacy rights. It thereby mentioned that it aimed to learn from the experiences and problems involved with SyRI and involve both experts and stakeholders in the search for a new instrument. Again, this decision was widely reported in the media.⁵¹

More generally, responding to risks of profiling such as those related to SyRI, some members of parliament and political parties have proposed that the government should be obliged to report the use of algorithms in its policies and activities; significant media-attention was given to this proposal.⁵²

1.5.2 Facebook's algorithms

Much attention has been paid to freedom of information issues related to fake news and disinformation that can be the result of the use of personalisation algorithms, especially after the Facebook judgment of the European Court of Justice and after it turned out that Facebook is not fact checking posts by politicians.⁵³ In addition, a journalist has initiated court proceedings against the removal by Facebook of three his photographs of a half-naked young girl and the blocking of his Facebook account.⁵⁴ This, too, has been widely covered in the national media.⁵⁵

⁵¹ E.g. 'Geen hoger beroep tegen uitspraak over fraudebestrijdingssysteem SyRI', *NRC Handelsblad* 23 April 2020; 'Overheid stopt met controversieel frauderisicosysteem SyRI', www.tweakersnet.nl, 23 April 2020.

⁵² See e.g. NU.nl, 'Tweede Kamer wil een algoritmemeldplicht voor de overheid', 24 September 2019, <https://www.nu.nl/politiek/5997764/tweede-kamer-wil-een-algoritmemeldplicht-voor-de-overheid.html>; bnr.nl, 'Algoritme-Meldplicht En Grapheneos', 2 October 2019, <https://www.bnr.nl/podcast/digitaal/10391288/algoritme-meldplicht-en-grapheneos>; NOS, 'Overheid gebruikt op grote schaal algoritmes, "risico op discriminatie"', NPO Radio 1, 29 May 2019, <https://www.nporadio1.nl/binnenland/16765-overheid-gebruikt-op-grote-schaal-algoritmes-risico-op-discriminatie>; NOS, 'D66 en CDA willen richtlijn en toezichthouder voor overheidsalgoritmes', 18 June 2019, <https://nos.nl/l/2289495>; Jan Middendorp, 'Op naar een nieuwe balans tussen overheid, markt en algoritmen', *de Volkskrant*, 26 May 2019, <https://www.volkskrant.nl/gs-b378b396>.

⁵³ ECJ 3 October 2019, Case C-18/18, ECLI:EU:C:2019:821. See e.g. Rudy Bouma, "'Politici plaatsen steeds vaker desinformatie op sociale media'", 3 October 2019, <https://nos.nl/l/2304514>; RTL Nieuws, "'Facebook gaat satire en opinie niet factchecken'", 1 October 2019, <https://www.rtlnieuws.nl/tech/artikel/4867766/facebook-gaat-satire-en-opinie-niet-factchecken>.

⁵⁴ See his own Twitter account: <https://twitter.com/thijsheslenfeld>.

⁵⁵ See e.g. Thomas Borst, 'Fotograaf Thijs Heslenfeld doet aangifte tegen Facebook, nadat zijn foto's werden verwijderd: "Dit raakt aan onze vrijheid"', *de Volkskrant*, 8 August 2019, <https://www.volkskrant.nl/gs-bf496ad2>; Maarten Moll, 'Nederlandse fotograaf doet aangifte tegen Facebook na verwijderen "blootkiekjes" Namibische vrouwen', *AD.nl*, 8 August 2019, <https://www.ad.nl/binnenland/nederlandse-fotograaf-doet-aangifte-tegen-facebook-na-verwijderen-blootkiekjes-namibische-vrouwen~ac8543a8/>; NRC, 'Nederlandse fotograaf doet aangifte tegen Facebook voor verwijderen naaktfoto's', accessed 21 March 2020, <https://www.nrc.nl/nieuws/2019/08/08/nederlandse-fotograaf-doet-aangifte-tegen-facebook-voor-verwijderen-naaktfotos-a3969507>.

1.5.3 AERIUS calculator

Another important case that has drawn the attention of many legal scholars and the media related to the programmatic approach to nitrogen (*Programmatische Aanpak Stikstof – PAS*). To regulate the emission of nitrogen by, for example, farmers or building companies, an algorithm-driven AERIUS Calculator was used to calculate whether certain building or exploitation permits could be issued. Unsure about the working of AERIUS, court proceedings were brought, in which the highest administrative court, the Judicial Division of the Council of State, ruled that transparency requirements should also hold for this type of algorithm-driven decision-making programmes and the government was obliged to provide for a proper and understandable explanation of the type of data used and the choices that were made as part of the algorithm.⁵⁶ This judgment has been much commented on, in particular by legal bloggers.⁵⁷

1.5.4 Discrimination and AI

Finally, there is an extensive media debate on the risks of discrimination by the use of algorithms and AI. In this debate, both examples are provided of such discrimination (and the inherent risk of it in using algorithms),⁵⁸ and examples and arguments to show that there is no reason to fear for such discrimination⁵⁹. This debate does not only

⁵⁶ ABRvS (Judicial Division of the Council of State) 17 May 2017, ECLI:NL:RVS:2017:1259 (Aerius I); ABRvS 18 July 2018, ECLI:NL:RVS:2018:2454 (Aerius II).

⁵⁷ See e.g. Stibbeblog, 'Afdeling Bestuursrechtspraak Verfijnt Toetsingskader Voor Geautomatiseerde Besluitvormingsprocessen (AERIUS)', accessed 21 March 2020, <http://www.stibbeblog.nl/all-blog-posts/environment-and-planning/afdeling-bestuursrechtspraak-verfijnt-toetsingskader-voor-geautomatiseerde-besluitvormingsprocessen-aerius/>; Franca Damen, 'Blogserie uitspraken PAS (deel 3): toetsingskader en wijze van instemming', Franca Damen, 30 May 2017, <https://www.fracadamen.com/natuurbescherming/blogserie-uitspraken-pas-deel-3-toetsingskader-en-wijze-van-instemming/>; Ellen Timmer, 'Geautomatiseerde besluitvorming in het bestuursrecht | uitspraak ABRvS in zaak over AERIUS', *Ellen Timmer - juridische artikelen en berichten* (blog), 25 December 2017, <https://ellentimmer.com/2017/12/25/geautomatiseerde-besluitvorming-in-het-bestuursrecht-uitspraak-abrvs-in-zaak-over-aerius/>. On the follow-up, see e.g. Ralph Frins, 'PAS Een Jaar Later. Waar Staan We Nu? - VMR', 17 May 2018, <https://www.milieurecht.nl/nieuws/pas-een-jaar-later-waar-staan-we-nu>.

⁵⁸ E.g. Bright, 'Algoritmes Facebook zorgen voor discriminatie bij reclame', 5 April 2019, <https://www.bright.nl/nieuws/artikel/4667426/algoritmes-facebook-zorgen-voor-discriminatie-bij-reclame>; FD.nl, 'Discriminatie Door Algoritmes Wordt Subtieler, Waarschuwt Raad van Europa', accessed 21 March 2020, <https://fd.nl/ondernemen/1289056/raad-van-europa-algoritmes-discrimineren-nieuwe-klassen-van-mensen>; RTL Nieuws, "Algoritmes politie kunnen leiden tot discriminatie", 6 February 2019, <https://www.rtlnieuws.nl/tech/artikel/4599766/algoritmes-politie-kunnen-leiden-tot-discriminatie>.

⁵⁹ Christian Verhagen, 'Angst voor algoritmes is onterecht: "discriminerend" algoritme geeft slechts weer wat mensen denken', Trouw, 1 July 2019, <https://www.trouw.nl/gs-b3179e7b>; FD.nl, 'Algoritmes Kunnen Discriminatie Juist Beperken, Maar Alleen Met Goede Data', accessed 21 March 2020,

concern the use of AI in the public sector, but also in the private sector, such as in employment decisions.⁶⁰

<https://fd.nl/opinie/1277940/algorithmes-kunnen-discriminatie-juist-beperken-maar-alleen-met-goede-data>; NOS, 'Algorithmes moeten discriminatie in vacatureteksten opsporen', 10 August 2019, <https://nos.nl/l/2296998>.

⁶⁰ See e.g. Jochem van Staalduine, "'Algorithmes bedreigen solidariteitsbeginsel verzekeringen'", Trouw, 25 July 2019, <https://www.trouw.nl/gs-b65f2053>; NRC, 'Solliciteren bij een algoritme', accessed 21 March 2020, <https://www.nrc.nl/nieuws/2018/05/11/solliciteren-bij-een-algoritme-a1602656>; Stephan Vegelien, 'Voorspellende algoritmes duiken overal op, ook bij de boer in z'n stal', 28 June 2019, <https://nos.nl/l/2291044>.

2 Laws and regulations applicable to AI and big data

2.1 General

In the Netherlands, just like the provisions of the EU Charter of Fundamental Rights, all fundamental rights provisions contained in the European Convention on Human Rights (ECHR) and many provisions of other international human rights treaties have direct effect and priority over national acts of parliament (and even the Constitution).⁶¹ For various reasons, the fundamental rights as laid down in the Constitution have less practical impact than the rights contained in the ECHR and the EU Charter of Fundamental Rights. In most Dutch case-law, legislation and policy documents, extensive reference is made to the standards and principles defined in the judgments of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU).⁶² This can also be seen in the reports, policy documents and judgments listed in [section II.3](#) of this report. Although constitutional fundamental rights provisions are usually mentioned, the meaning of fundamental rights in the context of AI is generally clarified by referring to relevant judgments of one of the European Courts. However, since none of these courts have yet been given an opportunity to really express themselves directly on issues of AI and fundamental rights, few topical references can be found in this respect.

As for other general human rights laws, the most important are the laws on non-discrimination and equal treatment (which also serve to implement the relevant EU-directives) and the laws on data protection (the GDPR and the law implementing the Police data Protection Directive, and related rules). The impact of this legislation is briefly and generally described in [section II.2](#). An overview of the most relevant laws for AI and fundamental rights is provided in [section II.3](#), a list of standards and voluntary guidelines (provided by the government as well as in self-regulation) is provided in [section II.4](#).

2.2 Application of fundamental rights laws to AI

⁶¹ See Articles 93 and 94 of the Netherlands Constitution.

⁶² Fleuren and Gerards 2014; Gerards, Van Ommeren and Wolswinkel 2020 (forthcoming).

2.2.1 Privacy related rights, personal autonomy and data protection

For data protection rights it is obvious that the General Data Protection Regulation (GDPR) plays a key role. To the extent that the policy briefs, standards and legislation mentioned in [section I.2](#) and [section I.3](#) discuss issues of data collection and processing, they always refer to the relevant provisions of the GDPR and related legislation. The relevant guidelines, ethical codes and soft-law documents cited in [section II.4](#) also standardly refer to the GDPR and related data protection legislation as the relevant framework.

In relation to the use of AI for purposes of dataveillance (e.g. interception of data, facial recognition, preventive detection of fraud risks), reference is commonly made to the relevant case-law of the ECtHR on surveillance and interception. Article 8 ECHR and the relevant case-law of the ECtHR are referred to in relation to private companies using new technologies to monitor their employees or make employment decisions.⁶³

To the extent that AI can be used in robots, who for instance could take over various tasks in caring for the elderly or for ill persons, reference is usually made in general terms to notions of human dignity and personal autonomy as recognised in the case-law of the ECtHR.⁶⁴

2.2.2 Freedom rights (e.g. freedom of information and freedom of expression)

As for freedom rights, the general fundamental rights instrument that is most often referred to in both case-law and policy briefs and legislation is the ECHR as interpreted by the ECtHR, as well as the EU Charter and relevant CJEU and ECtHR judgments (especially where search engines and, to a lesser degree, social media are concerned).⁶⁵ In relation to algorithms used for personalisation, for instance, policy documents might emphasise the importance of the freedom of expression and of information as contained in Article 10 ECHR, as well as the need to avoid a 'chilling effect' as is often referred to in the ECtHR's judgments.⁶⁶ It is then usually mentioned that these freedoms might conflict with other rights and public values, such as protection of one's reputation, privacy rights, non-discrimination or security issues. In drafting policies and in (stimulating self-) regulation, emphasis is placed on the need to find a balance between such conflicting interests and to offer safeguards to ensure that this balance is, indeed, found.

⁶³ See further Vetzo, Gerards and Nehmelman 2018, p. 126; Van Est and Gerritsen 2017.

⁶⁴ Vetzo, Gerards and Nehmelman 2018, p. 133/4; Van Est and Gerritsen 2017.

⁶⁵ For the preferred use of the ECHR and ECtHR case-law as a legal source see Gerards and Fleuren 2014 and Gerards, Van Ommeren and Wolswinkel 2020 (forthcoming).

⁶⁶ Cf. Vetzo, Gerards and Nehmelman 2018, p. 159. For one example out of many of an ECtHR judgment mentioning the risk of a chilling effect, see *Magyar Jeti Zrt v Hungary*, ECtHR 4 December 2018, no 11257/16, ECLI:CE:ECHR:2018:1204JUD001125716, para. 83.

In supporting education programmes, reference is often made to the need to offer diverse and pluralist information and the need for both children and adults to be aware of the risks of AI in relation to the reliability of information presented through digital media.⁶⁷

2.2.3 Non-discrimination and equality rights

The Dutch General Equal Treatment Act (*Algemene Wet Gelijke Behandeling* – AWGB) covers non-discrimination in employment (in both the public and private sector) as well as in offering goods and services (also both in the public and private sector). This means that, for example, retail companies and insurers are bound to comply with the equality rules laid down in this legislation.⁶⁸ The AWGB is also the main implementation law for the relevant EU Directives (although it predates most EU legislation in the field) and it therefore contains the prohibited grounds as the EU Directives do as well as some additional ones (i.e., religion, belief, political conviction, sex/gender, nationality, hetero- or homosexual orientation, civil status). In addition to the AWGB, and also meant to transpose the relevant EU Directives and Framework Decisions, there is specific (yet similar) general equal treatment legislation for grounds that are not mentioned in the AWGB, such as handicap/chronic illness (*Wet gelijke behandeling handicap en chronische ziekte* – WGBH/CZ), age (*Wet gelijke behandeling op grond van leeftijd* – WGBL (limited to employment discrimination)), part-time/fulltime work (*Wet onderscheid arbeidsduur* – WOA) and temporary/permanent contracts (*Wet onderscheid bepaalde / onbepaalde tijd* – WOBOT). The AWGB is furthermore complemented by a specific statutory act on equal treatment of men and women (*Wet gelijke behandeling mannen en vrouwen* – WGB), which predates the AWGB and covers some aspects that are not regulated in that act.

If individuals fall victim to acts to which the abovementioned legislation does not apply (e.g. in relation to decisions by public bodies granting or refusing a permit or imposing a sanction, or in relation to age discrimination in service provision), they can invoke the prohibition of discrimination of Article 14 ECHR (taking account of its accessory character, which means that Article 14 always should be invoked together with one of the substantive provisions of the ECHR), or, alternatively, the relevant provisions of the EU Charter of Fundamental Rights (in cases where EU law is applicable). If none of these provisions

⁶⁷ See in particular Agenda Digital NL at: *Digitale Overheid*, 'Beschermen van grondrechten en publieke waarden', webpagina, accessed 21 March 2020, <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nldigibeter/beschermen-van-grondrechten-en-publieke-waarden/>. and the policy brief of the Minister of the Interior on AI, fundamental rights and public values at: Twede Kamer der Staten-Generaal, 'AI, publieke waarden en mensenrechten'.

⁶⁸ It is not yet fully clear if also digital platforms intermediating between service providers and users come within the scope of application; this would be important since such platforms commonly use algorithms and sometimes AI as part of their business models. On this, see Gerards 2019 (forthcoming).

apply, the equal treatment and non-discrimination clause of Article 1 of the Dutch Constitution can be invoked, just like Article 26 of the ICCPR or the equality principle as an unwritten principle of good administration.

Finally, the relevant legal framework on equal treatment is complemented by several prohibitions of discrimination contained in Dutch criminal law, in particular Articles 137g and 429quater of the Dutch Criminal Code ([Wetboek van Strafrecht](#)). For these provisions to apply, an intention to discriminate usually must be shown, which makes such provisions less relevant to AI related matters.⁶⁹

In relation to AI and AI applications, policy documents such as those discussed in [section I.3](#) usually refer to the AWGB and other general equal treatment legislation or to the ECHR and the Constitution to explain that algorithms may not cause direct or indirect discrimination on protected grounds. A difficult situation may arise in relation to algorithmic profiling when it is not easy to establish a discriminatory harm: profiling as such is not covered by any of the non-discrimination laws mentioned above. In that case, for example in the National AI Strategy, the GDPR is referred to instead, pointing at the restrictions regarding sensitive personal information.

2.2.4 Procedural rights

In relation to rights such as the right of access to an effective remedy and to a court, judicial independence and impartiality, good administration, fair trial and equality of arms, Dutch policy briefs and legislation tend to refer to the case law of the ECtHR under Articles 6 and 13 ECHR and the case-law of the CJEU under Articles 41 and 47 CFR. The main reason for this is that a fundamental right to a fair trial and to access to a remedy is currently missing from the Dutch Constitution, although there is a bill pending to fill this gap.⁷⁰ In other cases, especially court cases on transparency of algorithms, not so much these procedural provisions are referred to as well as unwritten principles of good administration such as the principle of giving reasons

⁶⁹ Cf. Vetzo, Gerards and Nehmelman 2018, p. 147.

⁷⁰ In the Netherlands, proposals to amend the Constitution have to be adopted in two so-called readings in Parliament. After the bill is adopted in the first reading, new elections must take place and the new Parliament (both the House of Parliament and the Senate) have to adopt the bill with a two-thirds majority (Article 137 of the Netherlands Constitution; see in more detail and in English on this procedure and its legal effects Gerards 2016). The proposal to add a provision to the Constitution on the right to a fair trial was adopted in 2018 (*Staatsblad* 2018, 88; see: *Parlementaire Monitor*, 'Wet van 21 Februari 2018, Houdende Verklaring Dat Er Grond Bestaat Een Voorstel in Overweging Te Nemen Tot Verandering van de Grondwet, Strekkende Tot Het Opnemen van Een Bepaling over Het Recht Op Een Eerlijk Proces - *Parlementaire Monitor*', 21 February 2018, <https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vkn2c4mspxy6> ; and is now awaiting its second reading. When this will take place depends on when Parliament is dissolved (normally this would happen in 2021, but this can be earlier after a government crisis) and on whether there is sufficient support in both Houses of Parliament after the elections.

for administrative law decisions. Examples of this can be found in the relevant policy briefs discussed in [section I.3](#).

2.3 Overview of laws applicable to AI and big data

Sector	Title of national law/provision	Fundamental rights addressed	EU law basis	Legal remedies	Description
Cross-sectoral	European Convention on Human Rights	Civil and political rights (but also socio-economic because of case-law); many positive obligations (substantive and procedural) based on case-law			Main fundamental rights treaty. Strong legal effect ensues from limited meaning of the Dutch Constitution (see below) in combination with Articles 93/94 Constitution (providing direct effect and priority to self-executing provisions of international law). In most judgments and policy documents/legislation, reference is made to the judgments of the ECtHR explaining the provisions of the ECHR.

	European Social Charter	Social and economic rights			Main fundamental rights treaty in the field of social and economic rights. In the Netherlands, some rights are considered to have direct effect and priority (a well-known example is Article 6 (4) on the right to take collective action), but most do not. Nevertheless, it is sometimes referred to in legislative texts, policy documents and case-law, mainly as source of inspiration or additional support for arguments; this includes decisions of the European Commission of Social Rights
	International Covenant on Civil and Political Rights	Civil and political rights			Civil and political fundamental rights treaty that has mostly direct effect and

					priority in the Netherlands; mainly of relevance where ECHR or EU Charter cannot be invoked; e.g. prohibition of discrimination (Article 26) and right to a fair trial (Article 14)
	International Covenant on Social, Economic and Cultural Rights	Social, economic and cultural rights			Fundamental rights treaty of which most provisions do not have direct effect and priority. Sometimes referred to in legislative texts, policy documents and case-law, mainly as source of inspiration or additional support for arguments; this includes views/general comments of the International Committee of ESC Rights.

	CERD / CEDAW / Children's rights Convention	Non-discrimination and group-related fundamental rights			Non-discrimination treaties of which some provisions have direct effect and priority. Sometimes they are referred to in legislative texts, policy documents and case-law, mainly as source of inspiration or additional support for arguments; this includes views/general comments of the relevant committees
	EU Charter of Fundamental Rights	Civil, political, social, economic and citizenship-based fundamental rights	Yes, same status as primary EU law		Fundamental rights document of which all provisions expressing rights have direct effect and priority. The provisions as explained by the CJEU are always taken into account in relevant policy fields; first source of reference where applicable (even if compared to ECHR) in



					case-law; many preliminary questions referred to ECJ to ask for further explanation. It is not yet clear to what extent provisions also have horizontal effect.
	Dutch Constitution	Several civil and political fundamental rights (but no right to life, prohibition of torture or right to a fair trial); several social and economic rights (but no direct effect).	No		Basic law for the Netherlands; contains both fundamental rights and basic norms for legislation, government, the judiciary, decentralization, agencies and the role of the monarch. Judicial review of Acts of Parliament against the Constitution is not allowed (Article 120 Constitution), so practical meaning is limited to review of lower legislation and administrative acts (but even there: not



					popular). Usually the Constitution is only invoked in relation to cases on prior restrictions of freedom of expression (fully prohibited by Article 7) and right to education (Constitution offers specific protection).
	Equal treatment legislation (<i>AWGB, WGBH/CZ, WGBL, WGB, WOA, WOBOT</i>)	Prohibits direct and indirect discrimination based on religion, belief, political conviction, sex/gender, nationality, hetero- or homosexual orientation, civil status, handicap / chronic illness, age, part-time / fulltime contract, temporary / permanent contract	Yes, implements relevant EU-equality directives, in particular Directive 2000/43/EC (equal treatment based on race and ethnicity); Directive 2000/78/EC (framework directive on equal treatment in employment and occupation);	Protection and enforcement are laid down in Title 5 AWGB (and similar provisions in the other equal treatment laws). Most relevant provisions: Article 7: prohibition of victimisation Article 8: termination of employment contract by employer in breach with equal treatment legislation can be annulled (cf. Article 7:681 Dutch Civil Code). Article 9: contractual agreements in breach	This legislation prohibits unjustified differences in treatment in employment and, for the General Equal Treatment Act, in offering goods and services. Further interpretation usually by National Human Rights Institute (competent to deal with individual complaints about discrimination) and/or by the courts, taking into account relevant



			<p>Recast Directive 2006/54/EC.</p>	<p>with equal treatment legislation are void. Article 10(1): <i>prima facie</i> evidence suffices to show differential treatment; burden of proof of acting in conformity with the legislation lies with the defendant.</p> <p>Individual complaints about unequal treatment can be brought before the National Human Rights Institute (College voor de Rechten van de Mens; NHRI); see Act on the National Human Rights Institute (<i>Wet College voor de rechten van de mens</i>); this NHRI can give non-binding judgments in individual cases brought before it (Article 10) or can start an investigation from its own motion (Article 11); it can also start judicial</p>	<p>case-law of the CJEU. So far no specific application in cases on AI or big data.</p> <p><i>Examples</i> in 'main' General Equal Treatment Act (<i>Algemene Wet Gelijke Behandeling – AWGB</i>):</p> <p><i>Employment:</i> Article 5(1) (taken in conjunction with Articles 1 and 2) prohibits direct and indirect discrimination based on several grounds (mentioned in Article 1(a-c)), with some general and specific exceptions in Article 2 and 5 (2-5), e.g. for religious and political institutions with regard to</p>
--	--	--	-------------------------------------	---	--



				<p>proceedings claiming that an act is contrary to the equal treatment laws (Article 13).</p> <p>In addition, individual victims of unequal treatment can turn to the regular civil and administrative courts, e.g. based on a negligence/tort claim (Article 6:162 Dutch Civil Code).</p>	<p>religion, belief, political conviction.</p> <p><i>Providing goods and services:</i> Article 7(1) prohibits direct and indirect discrimination in both the public and private sector, with some general and specific exceptions in Article 2 and 7 (2-3).</p>
	<p>Criminal Code (<i>Wetboek van Strafrecht</i>)</p>	<p>Several provisions protecting against discrimination, incitement to hatred, unequal treatment etc.</p>	<p>No, but related to Directive 2000/43/EC (equal treatment based on race and ethnicity)</p>	<p>The third book of the Dutch Code of Criminal Procedure (<i>Wetboek van Strafvordering</i>) contains the legal remedies, such as appeal (Title II) and cassation (Title III). Section B provides for 'extraordinary legal remedies', including for example revision of court judgments with <i>res</i></p>	<p>Article 90quater defines 'discrimination' as 'any form of distinction, exclusion, restriction or preference, the purpose or effect of which is to nullify or impair the recognition, enjoyment or exercise on an equal footing of human rights and fundamental freedoms</p>



				<p><i>iudicata</i> by the Supreme Court (Title VIII).</p> <p>Suspects (as defined in Article 27 Code of Criminal Procedure) also enjoy the (procedural) safeguards as laid down in Article 6 / 13 ECHR and Article 47-40 CFR, such as the right to have access to a court, equality of arms, effective participation in the proceedings and the right to defend oneself in person or through legal assistance.</p>	<p>in the political, economic, social or cultural field or in other areas of social life’.</p> <p>This definition is relevant to the application of the following articles, containing definitions of criminal offences:</p> <p>Article 137c: prohibition of intentionally making insulting statements about a group of persons because of their race, religion etc.</p> <p>Article 137d: prohibition of inciting hatred against or discrimination of persons or violence against their person or property because</p>
--	--	--	--	--	--



					<p>of their race, religion etc.</p> <p>Article 137e: prohibition of making public statements likely to offend a group of people because of their race, religion etc., or to incite hatred or discrimination or violence against their person or property; prohibition of sending or distributing, without request, an object likely to contain such a statement.</p> <p>Article 137f : prohibition of taking part in, or providing financial or other material support to, activities aimed at discrimination of</p>
--	--	--	--	--	--



					<p>persons because of their race, religion etc.</p> <p>Article 137g: prohibition of intentionally discriminating people because of their race in the exercise of office, profession or business.</p> <p>Article 429quater (1): prohibition of discriminating people because of their race, religion etc. in the exercise of office, profession or business;</p> <p>Article 429quater (2): prohibition of undertaking or refraining from undertaking, for no reasonable grounds, certain acts in the exercise of office,</p>
--	--	--	--	--	---



					<p>profession or business which can have the purpose or effect in regard of persons which a physical, mental or intellectual disability of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental rights in the political, economic, social or cultural field or in other areas of social life.</p> <p><i>Other relevant articles related to fundamental rights (aimed at protecting e.g. private life):</i> Article 138c (in force since 1 March</p>
--	--	--	--	--	---



					<p>2019): prohibition of intentional and unlawful taking over of non-public data stored by means of an automated work, for himself or for another person.</p> <p>Article 139c: prohibition of intentional and unlawful interception of recording of data, which is not intended for him by means of a technical device.</p> <p>Article 139d: prohibition of installing technical devices with the intention of unlawfully using it to eavesdrop on, intercept or record a conversation, telecommunications</p>
--	--	--	--	--	--

					<p>or other type of data transfer or processing.</p> <p>Article 139e: prohibition of possessing, obtaining and disclosing or intentionally making available data that has been obtained by unlawful eavesdropping, interception or recording.</p> <p>Article 139f: prohibition of intentional and unlawful production of an image of a person who is present in a home or in another non-public place by means of a technical device which is not clearly visible or notified</p>
--	--	--	--	--	---



					<p>(covert camera surveillance); (paragraph 2) prohibition of having at his disposal an image which, as he knows or should reasonably suspect, has been obtained by means of or as a result of such covert camera surveillance.</p> <p>Article 139g: prohibition of making public an image as referred to in the previous Article.</p> <p>Article 441b: prohibition of unlawful production of an image of a person who is present at a place accessible to the public, by employing a specially installed</p>
--	--	--	--	--	---



					technical device which is not clearly visible (covert camera surveillance).
	General Data Protection Regulation (<i>Algemene Verordening Gegevensbescherming</i> – AVG)	Safeguards personal data (including sensitive data) against misuse in collecting and processing; contains ‘ethics-by-design’ principle; can offer additional protection against discrimination to the extent that processing of certain categories of personal data is in principle not allowed	Yes, Regulation 2016/679 with a basis in primary Union law in Article 16 TFEU.		Broad protection of personal data in both horizontal and vertical relations; directly applied by courts and administrative bodies/legislators, referring to relevant case-law of the ECJ.
	GDPR Execution Act (<i>Uitvoeringswet Algemene Verordening Gegevensbescherming</i>)	See above	Yes, GDPR	Supervisory authority is Data Protection Authority (<i>Autoriteit Persoonsgegevens</i>) (Chapter 2 UAVG):	Specific elaboration of GDPR to the extent needed to give effect to the GDPR.



	<p><i>herming – UAVG)</i></p>			<p>Article 14: tasks and competences Article 15: supervision and special powers (e.g. entering homes) Article 16: injunctions Article 17: fines Article 18: administrative fines for public authorities Article 19: collaboration with other supervisory bodies Article 20: competence in relation to data sharing with third countries</p> <p>Legal remedies are described in Title 3.3: Articles 34 + 35: when a written decision is given upon a request as meant in Articles 15-22 GDPR by an administrative body, this qualifies as an 'administrative decision', allowing for</p>	
--	-----------------------------------	--	--	--	--



				<p>legal proceedings to be brought in line with the General Administrative Law Act (<i>Algemene wet bestuursrecht</i>)</p> <p>Article 36: conflict resolution by Data Protection Authority</p>	
			Article 9(2) GDPR		<p>Article 23: general exceptions to the prohibition of processing of special categories of personal data</p> <p>Article 24: exceptions for archiving purposes</p>
			Article 9(2)(b), (g) and (h) GDPR		Articles 25-30: specific exceptions in relation to race / ethnic origin, political opinion, religious / philosophical beliefs, genetic data, biometric data, health data
			Article 22 GDPR		Article 30: specific provisions in relation to specific sectors, such as administrative



					bodies, child protection, insurance
			Article 36(5) GDPR		Article 40: concerns the exception to automated decision-making ('suitable measures' are considered to be taken if the right to obtain human intervention, the right of the data subject to express his or her point of view and the right to contest the decision, are safeguarded). No use is made of possibility of making prior authorization mandatory for controllers.
	General tort / negligence provisions in	Regulates liability if a private party (company,			Provide the most important legal basis in private law cases

	the Netherlands Civil Code (e.g. Article 6:162 Dutch Civil Code)	individual) has acted against general principles of law, which include all conceivable fundamental rights			where there is no specific legislation available that can be invoked
			Articles 12-14 of Directive 2000/31/EC (E-Commerce Directive) containing three liability safe harbours for information society service providers		Implemented in Article 6:169c Dutch Civil Code: the three safe harbours nonetheless leave the possibility for a court injunction to, for example, terminate or prevent a copyright infringement, possibly combined with a penalty payment (<i>dwangsom</i>).
	Media Act (<i>Mediawet</i>)	Safeguards media pluralism and access to the media (hence freedom of expression /information)	Yes, Audiovisual Media Services Directive 2010/13/EU as amended by Directive 2018/1808	The Commissariat for the Media is responsible for the administrative enforcement of the provisions of the Media Act, with certain exceptions (Article 7.11). Article 7.12 gives the Commissariat the power	Legislation regulating access to the media, distribution, advertisements, media pluralism etc. Some relevant provisions:



				<p>to, under certain conditions and for the violation of certain provisions in the Media Act:</p> <ul style="list-style-type: none"> ○ impose an administrative fine up to €225,000 per violation; ○ give an order for periodic penalty payments (<i>last onder dwangsom</i>). <p>The Dutch Journalism Fund (<i>Stimuleringsfonds voor de journalistiek</i>) encourages the quality, diversity and independence of journalism by using money, knowledge and research to promote the innovation of the infrastructure for journalism.</p> <p>The goal of this Fund, according to Article 8.3, is</p>	<p>Title 6.1.1: the Commissariat for the Media (<i>Commissariaat voor de media</i>) allocates a number of hours on the general programme channels of the national public media service to political parties in parliament.</p> <p>Title 6.1.2: the Commissariat allocates a number of hours for the purpose of public information programmes.</p> <p>Articles 3.5b and 3.7ff: advertisements shall be clearly distinguishable.</p> <p>Overall emphasis on the 'editorial autonomy'</p>
--	--	--	--	---	--



				to maintain and promote the pluralism of the press. The Fund is charged with, inter alia, giving out subsidies and conducting or commissioning research into the functioning of the press. The decisions made by the Fund are considered a subsidy under Dutch administrative law, so the legal protection mechanisms provided by the General Administrative Law Act apply.	(<i>redactionele autonomie</i>) of public and commercial channels, entailing their responsibility for the form and content of their programmes and limited governmental interference in this regard (for instance Article 1 (definition of 'media service') and Article 2.88).
	Act on the Security of Network and Information Systems (<i>Wet beveiliging netwerk- en informatiesystemen – Wbni</i>)	Applies to inter alia energy, transport, bank, health and digital infrastructure sectors.	Yes, implements EU Directive 2016/1148 concerning measures for a high common level of security network and information systems		



			across the Union.		
Public Administration	Act on Open Government (<i>Wet openbaarheid van bestuur – Wob</i>)	Safeguards open access to (government) information, also of a digital nature, and allows open exchange and re-use of such information; regulates intellectual property rights	Yes, implements e.g. Directive 2003/98 on the re-use of public sector information		Legislation on access to government information



<p>Law Enforcement</p>	<p>Act on Data Processed by the Police (<i>Wet Politiegegevens</i> - Wpg)</p>	<p>Contains specific safeguards to protect (sensitive and other) personal data that have been obtained or are used in relation to criminal prosecution and/or criminal trials</p>	<p>Yes, Directive 2016/680 (previously framework decision 2008/977)</p> <p>Supervisory authority is the Data Protection Authority (<i>Autoriteit Persoonsgegevens</i>) (same as GDPR).</p> <p>Title 4 Wpg (Article 24a onwards) provides for specific rights of data subjects, such as the right of access (Article 25) and right to rectification (Article 28).</p>	<p>Data protection regarding data collected, processed and used by the police in the exercise of its powers. Applies to i.a. National Police, special investigative services (<i>bijzondere opsporingsdiensten</i>), Royal Marechaussee, National Police Internal Investigations Department (<i>Rijksrecherche</i>).</p>	
------------------------	---	---	--	--	--



			<p>Article 29(1) Wpg: decisions upon request for these rights qualify as ‘administrative decisions’ within the meaning of the General Administrative Law Act (<i>Algemene wet bestuursrecht</i>, Article 1:3), allowing for legal proceedings to be brought in line with this Act (administrativ e appeal + access to an administrative court).</p>		
--	--	--	---	--	--



			Article 31a Wpg: data subject can file a complaint to the supervisory authority, which responds within three months (paragraph 5) and which response qualifies as an 'administrative decision' within the meaning of the General Administrative Law Act as well.		
	Act on Intelligence and Security Services (<i>Wet inlichtingen- en veiligheidsdiensten – Wiv</i>)	Contains specific safeguards to protect (sensitive and other) personal data that have been obtained or are used in relation to intelligence and security issues; sharing information etc.; contains	No	Article 23(1)(a) GDPR (in conjunction with Article 41(1)(a) GDPR Execution Act) holds that Union law or Member State law may restrict the scope of certain GDPR rights and obligations, provided that such a restriction is necessary and proportionate in a	Regulation of the powers of the intelligence and security services (e.g. interception, sharing of data with foreign services); supervision and safeguards against misuse.



		<p>specific safeguards related to supervision</p>		<p>democratic society and respects the essence of the fundamental rights and freedoms, to safeguard national security. Certain rights and remedies of the GDPR thus do not apply.</p> <p>Article 32: establishes a Committee for the review of the employment of competences by the intelligence and security services (<i>toetsingscommissie inzet bevoegdheden</i>). This independent Committee carries out an upfront assessment of the lawfulness of the use of specific special powers; its judgment is binding (Article 32(2)).</p> <p>Title 7: the Committee for the Supervision of Intelligence and Security Services</p>	<p>The Wiv gives certain competences to intelligence and security services, for example:</p> <p>Article 38: systematic collection of data concerning persons from public sources;</p> <p>Article 39: consultation of informants, such as administrative bodies (<i>bestuursorganen</i>) and civil servants;</p> <p>Articles 48-50: investigation-oriented interception of communication (<i>onderzoeksopdrachtgerichte interceptie</i>);</p> <p>Article 45: hacking</p>
--	--	---	--	---	---



				<p>(<i>Commissie van toezicht op de inlichtingen- en veiligheidsdiensten – CTIVD</i>) handles the complaints with regard to the intelligence and security services.</p> <p>Article 114: the right to file a complaint to the Committee for the Supervision.</p> <p>Article 124(4): the Committee may determine that, for instance, the employment of a power shall be terminated or that certain data processed by the intelligence and security services shall be erased.</p> <p>With regard to the use of special powers against lawyers (confidential communication) and</p>	
--	--	--	--	---	--



				journalists (source protection), judicial authorisation by The Hague Court is required – only in the case of important operational interests, such as the existence of one or more indications of an immediate threat to national security (Article 30(2-3)).	
	Act on Data Relevant to Criminal Prosecution and Criminal Procedure (<i>Wet justitiële en strafvorderlijke gegevens - Wjsg</i>)	Contains specific safeguards to protect (sensitive and other) personal data that have been obtained or are used in relation to criminal prosecution and/or criminal trials. Accordingly, the provisions mainly safeguard data protection and privacy rights.	Yes, Directive 2016/680/EU (previously framework decision 2008/977)	<p>The data subject enjoys the right to request information (Article 18 Wjsg) and rectification (Article 22 Wjsg)</p> <p>Article 25 Wjsg: the exercise of these rights is free of charge</p> <p>Article 23(1) Wjsg: a decision upon the request to exercise the right to information and rectification qualifies as an 'administrative decision' within the</p>	Data protection regarding data collected and processed in relation to judicial administration and criminal prosecution. Directly applied by prosecution bodies and courts, referring to relevant case-law of the CJEU and the ECtHR on data protection and privacy issues.



				<p>meaning of Article 1:3 General Administrative Law Act, allowing for legal proceedings to be brought before an administrative court in line with this Act.</p> <p>Article 26a(1) Wjsg: data subjects enjoy the right to file a complaint to the Data Protection Authority (Autoriteit Persoonsgegevens), without prejudice to other legal remedies; (5) the Data Protection Authority shall respond within five months. Such a decision qualifies as an 'administrative decision' within the meaning of the General Administrative Law Act.</p> <p>Articles 27(4)/39r(3)/51(3)/51(d)/51h(3) Wjsg list the</p>	
--	--	--	--	---	--



				<p>competences of the Data Protection Authority (<i>Autoriteit Persoonsgegevens</i>), namely: warning the data controller or processor (a), applying administrative coercion (<i>last onder bestuursdwang</i>), b), imposing an administrative fine (c), giving an advice to the data controller regarding prior consultation (d) and obliging the data controller to notify data subjects of a data breach (e).</p> <p>Article 27(7) (and other Articles mentioned above) Wjsg: the competences under (d) and (e) qualify as 'administrative decisions', allowing for legal proceedings to be</p>	
--	--	--	--	--	--



				<p>brought before an administrative court in line with the General Administrative Law Act (Articles 5:21 and Article 5:40; administrative coercion and administrative fines also qualify as 'administrative decisions').</p> <p>In line with Articles 53 Directive (right to an effective judicial remedy against a supervisory authority), Article 26b Wjsg states that a claim against the Data Protection Authority (<i>Autoriteit Persoonsgegevens</i>) can be submitted to a court as mentioned in Article 2 Law on the Organisation of the Judiciary (<i>Wet op de Rechterlijke</i></p>	
--	--	--	--	---	--



				<p><i>Organisatie</i>), without prejudice to any other administrative or non-judicial remedies.</p> <p>Article 7f Wjsg: compensation for damages caused by a breach of the legal provisions. Paragraph (4) contains an exception to this liability: no, or limited compensation for damages if the damage is not attributable to the data controller or processor (burden of proof lies with the data controller or processor).</p>	
Telecommunication	Telecommunications Act (<i>Telecommunicatiewet</i>)	Safeguards e.g. net neutrality (hence freedom of expression/information); confidentiality of communication	Yes, implements and executes various EU-directives relevant to telecommunication and e-communication/e-privacy (e.g. Directive	Title 11 contains provisions regarding the protection of personal data and privacy, without prejudice to the GDPR. Article 11.3, for instance, describes the obligation for public electronic communication network and service providers to take	Legislation regulating the telecommunication infrastructure and related rights.



			<p>2002/58/EC, Directive 2009/136/EC, Directive 2009/140/EC, BEREC-Resolution no. 1211/2009, Directive 2018/1972 EC)</p>	<p>appropriate technical and organizational measures for the safety and security of the networks and services.</p> <p>Article 11.6(4): the subscriber has the right to verify, to have corrected or to have erased, free of charge, personal data relating to him in a subscriber directory.</p> <p>Article 11.7a: provisions on cookies (requiring consent and the provision of clear and complete information in line with the GDPR). The general system of legal protection applies, but no specific judicial remedy is available.</p>	
Health	The Medical Treatment Agreement Act (<i>Wet Geneeskundig</i>	Individual private rights, fundamental rights of life/safety, data rights. Ensures that			One of the main legal frameworks for patient information in the Netherlands. Outlines the responsibility that

	e <i>Behandelovereenkomst, WGBO</i>)	patients are informed of e.g. their treatment – including procedures/technologies – used, as well as potential risks and possible alternative approaches.			health care providers and professionals have concerning the provision of information for patients at the individual level.
	The Personal Data Protection Act (<i>Wet Bescherming persoonsgegevens, Wbp</i>) *note: now replaced by the GDPR	Personal data rights. Ensures that personal patient information/medical information remains confidential and e.g. is not distributed to 3 rd parties without informed consent.	Yes, In 2013 was adopted so as to follow the European Directive on patient rights in cross-border care (when applicable) In 2016, it was replaced by the GDPR.		The Personal Data Protection Act is the main legislative tool for ensuring the confidentiality of medical information. The College for the Protection of Personal Data (<i>College Bescherming Persoonsgegevens, CBP</i>) is charged with overseeing fulfilment of the law.
	n/a	Fundamental health-rights of patients. Aims to reduce the risks of	Yes, over a 3-year transition period (ends in 2020), the		The aim of the new rules is to improve patient safety and ensure that innovative



		medical devices and their application for the patient.	Netherlands is adopting the new European Regulations for medical devices and IVDs (incl. active implantable medical devices (90/385/EEC) & medical devices (93/42/EEC)		medical devices remain available for the patient.
Insurance	The Dutch Insurance Law ((Zvw) 2006; part of the Civil Code).	Individual consumer rights. E.g. outlines how the insurance company is required by law to disclose all and any relevant information to the insured individual, including information about the insurance premium and other conditions. It grants a balanced set of	Yes, albeit a seeming breach, it follows the EU prohibition on government regulation by invoking the exception clause in Non-life Insurance Directives, which stipulates that the Non-life Insurance Directives do not apply		The main legal framework for the regulation of insurance in the Netherlands. It covers all areas of insurance (life, and non-life* insurance) as well as the general rules for insurance companies and their obligations towards the customer. *Note: Non-life insurance refers to property or vehicle insurance while life and



		right both to the insuring company and the insured individual.	to insurance schemes that fully or partly replace social insurance.		health insurance provide insurance policies for the individual.
	Financial Supervision Act (<i>Wet op het financieel toezicht</i> , FSA)	Under the FSA, insurance companies must meet certain requirements in order to offer life insurance, non-life insurance, prepaid funeral services insurance or reinsurance services in the Netherlands.			
Energy	2020 National Renewable Energy Action Plan* *note: not a piece of legislation; it's an action-plan	Outlines energy sectors where the Dutch government aims to e.g. reduce the emissions of greenhouse gasses, as well as targets for renewable energy per sector	Yes, outline national strategies to meet the Renewable Energy Directive targets for 2020 as set out by the EU per energy-sector		

	<p>The 2013 Agreement on Energy for Sustainable Growth (the 'Energy Agreement').*</p> <p>*Note: a policy, but not a binding piece of legislation</p>	<p>Signatories to the Agreement share responsibility and commitment to achieve four overarching objectives:</p> <ul style="list-style-type: none"> • An average energy efficiency saving of 1.5% per year (adding up to a reduction of 100 PJ by 2020). • 14% share of renewable energy in the Netherlands' total consumption of energy by 2020. • 16% by 2023 (4.5% in 2013). • Creating at least 15.000 additional jobs by 2020, of which a significant number to be created in the next years 			<p>In 2013, 47 (Dutch) organisations signed the Agreement on Energy for Sustainable Growth. The Social and Economic Council of the Netherlands (SER) facilitated this process.</p>
--	--	--	--	--	--



	<p>The Electricity Act</p>		<p>Yes, the Act was amended by the Act of 12 July 2012 to implement the Third Energy Package Directives and Regulations (2009)</p>		<p>It is the main source of energy regulation in the Netherlands. The Authority for Consumers and Markets (ACM) has been appointed as the national regulatory authority to supervise compliance with the Act.</p>
--	----------------------------	--	--	--	---

3 Future development

This country report has shown that AI is a hot topic in the Netherlands. AI is increasingly used by both public bodies and private companies, and many Dutch research institutes and universities are involved in AI-development and in research into the effects of AI on human beings and society as a whole. The various policy documents, norms and guidelines described in this report show that there is significant awareness of both the opportunities and risks of AI for fundamental rights and public values. Respect for fundamental rights is a core element of the government's newly presented Strategic Action Plan AI as well as of a variety of policy briefs and governmental or ministerial responses to requests by Members of Parliament and research reports.

Some general tendencies can be distilled from the various policy briefs and documents that are relevant to the future development of AI in the Netherlands:

- The government actively strives for and invests in development, innovation and use of human-centric, trustworthy and responsible AI and aims to contribute to creating a political, societal and digital environment in which such development, innovation and use can thrive: in the government's view, AI research and innovation in the Netherlands must be of high quality and must be leading in Europe.
- The government embraces and stimulates the establishment of public-private partnerships and collaborations between the government, private parties and academia in the field of developing human-centric, trustworthy and responsible AI. Experiments, living labs and similar plans in which the government is involved also will contribute to continued respect for fundamental rights and public values (such as transparency).
- The government stimulates the development of self-regulation and ethical codes in the private sector, although it also produces relevant guidelines and standards itself – but mostly these concern the use of AI by public bodies. It strongly encourages private parties and companies to comply with the standards set in ethical codes and take further steps to translate these rules and standards to everyday practice.
- The government aims to invest in education and awareness-raising where opportunities and risks of AI for fundamental rights and public values are concerned.
- The government has invested strongly (and will continue to do so in the future) in commissioning research projects to further study the impact of AI on society and individuals as well as on fundamental rights and public values, in particular in order to help it further develop its policies.
- The government's regulatory activities remain relatively limited; current legislation and fundamental rights treaties, as described in section II of this report, are generally regarded as sufficient to adequately protect fundamental rights. To the extent necessary (which will be investigated), research will be conducted into possibilities for certification of AI-

applications or certain AI-uses and into the possibilities for streamlining the activities of supervisory and monitoring bodies.

- The government actively promotes respect for fundamental rights and public values in its *European and international activities and policies*.
- The government will promote collaboration and coherence between the different policy activities and actors involved in order to *avoid fragmentation and overlap*; the Ministry of the Interior plays a key role in this regard.

In addition to this, it is evident that many private actors and research institutes are actively involved in developing and using AI. They, too, are willing to heed fundamental rights and other public values, as is apparent from the formation of various alliances, coalitions and platforms (such as the AI Coalition, NL Digital, the Platform for the Information Society and the Alliance for Artificial Intelligence, see [section I.1.7](#)) and public-private partnerships as well as the development of a variety of ethical codes and guidelines for the responsible use of AI.

4 References

Books and journal articles

F. Bex, 'Artificiële intelligentie in de praktijk' [Artificial intelligence in practice], *Rechtstreeks* 2019 (2) p. 26-35

R. van Est and J. Gerritsen, *Human rights in the robot age. Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality* (The Hague, Rathenau Institute 2017)

J.H. Gerards and J.W.A. Fleuren (eds), *Implementation of the European Convention on Human Rights and of the judgments of the ECtHR in national case law. A comparative analysis* (Antwerp, Intersentia 2014)

J.H. Gerards, 'The Irrelevance of the Netherlands Constitution, and the Impossibility of Changing It', *77 Revue Interdisciplinaire d'Études Juridiques* (2016)(2) pp. 207-233

J.H. Gerards, 'Grondrechten in de platformsamenleving' [Fundamental Rights in the Platform Society], Preadvies Vereniging voor Burgerlijk Recht (VBR) 2019 (Amsterdam, Paris Publishing 2019)

J.H. Gerards, F. van Ommeren and J. Wolswinkel, 'The Dutch Paradox. The Impact of the Pan-European General Principles of Good Administration in the Netherlands', in U. Stelkens et al (eds), *Pan-European Principles of Good Administration* (working title) (Oxford, Oxford University Press 2020 (forthcoming))

M. Vetz, J.H. Gerards and R. Nehmelman, *Algoritmes en grondrechten* [Algorithms and fundamental rights] (The Hague, Boomjuridisch 2018), via https://www.uu.nl/sites/default/files/rebo-montaigne-algoritmes_en_grondrechten.pdf

Other sources

Autoriteit Persoonsgegevens. 'AP doet onderzoek naar verwerking nationaliteit bij Belastingdienst', 20 May 2019. <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-doet-onderzoek-naar-verwerking-nationaliteit-bij-belastingdienst>.

Benelux Association for Artificial Intelligence. 'About BNVKI'. <http://ii.tudelft.nl/bnvki/> (blog). Accessed 20 March 2020. <https://ii.tudelft.nl/bnvki/>.

bnr.nl. 'Algoritme-Meldplicht En Grapheneos', 2 October 2019. <https://www.bnr.nl/podcast/digitaal/10391288/algoritme-meldplicht-en-grapheneos>.

Borst, Thomas. 'Fotograaf Thijs Heslenfeld doet aangifte tegen Facebook, nadat zijn foto's werden verwijderd: "Dit raakt aan onze vrijheid"'. de Volkskrant, 8 August 2019. <https://www.volkskrant.nl/gs-bf496ad2>.

Bouma, Rudy. "'Politici plaatsen steeds vaker desinformatie op sociale media'", 3 October 2019. <https://nos.nl/l/2304514>.

Bright. 'Algoritmes Facebook zorgen voor discriminatie bij reclame', 5 April 2019. <https://www.bright.nl/nieuws/artikel/4667426/algoritmes-facebook-zorgen-voor-discriminatie-bij-reclame>.

Damen, Franca. 'Blogserie uitspraken PAS (deel 3): toetsingskader en wijze van instemming'. Franca Damen, 30 May 2017. <https://www.fracadamen.com/natuurbescherming/blogserie-uitspraken-pas-deel-3-toetsingskader-en-wijze-van-instemming/>.

Digital Government. 'Digital Government Agenda: NL DIGIbeter'. Accessed 20 March 2020. <https://www.nldigitalgovernment.nl/digital-government-agenda/>.

Digitale Overheid. 'Beschermen van grondrechten en publieke waarden'. Webpagina. Accessed 21 March 2020. <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nldigibeter/beschermen-van-grondrechten-en-publieke-waarden/>.

———. 'Kamerbrief met reactie op UU-rapport Algoritmes en grondrechten'. Webpagina, 28 March 2019. <https://www.digitaleoverheid.nl/gebeurtenis/kamerbrief-met-reactie-op-uu-rapport-algoritmes-en-grondrechten/>.

———. 'Planning Agenda Digitale Overheid'. Webpagina, 2019. <https://www.digitaleoverheid.nl/nl-digibeter2019/planning-agenda-digitale-overheid/>.

Driessen, Camil. "'Willen we dat de overheid zo met burgers omgaat?'" NRC, 28 October 2019. <https://www.nrc.nl/nieuws/2019/10/28/willen-we-dat-de-overheid-zo-met-burgers-omgaat-a3978217>.

ECP. 'Artificial Intelligence: Whitepaper: Gespreksstof En Handvatten Voor Een Evenwichtige Inbedding in the Samenleving', 2018.

European Association for Artificial Intelligence. 'BNVKI/AIABN'. Accessed 20 March 2020. <https://www.eurai.org/node/4>.

FD.nl. 'Algoritmes Kunnen Discriminatie Juist Beperken, Maar Alleen Met Goede Data'. Accessed 21 March 2020. <https://fd.nl/opinie/1277940/algoritmes-kunnen-discriminatie-juist-beperken-maar-alleen-met-goede-data>.

———. 'Discriminatie Door Algoritmes Wordt Subtieler, Waarschuwt Raad van Europa'. Accessed 21 March 2020. <https://fd.nl/ondernemen/1289056/raad-van-europa-algoritmes-discrimineren-nieuwe-klassen-van-mensen>.

———. 'Mag de Staat Gluren in de Watermeter?' Accessed 21 March 2020. <https://fd.nl/economie-politiek/1322434/mag-de-staat-gluren-in-de-watermeter>.

Frins, Ralph. 'PAS Een Jaar Later. Waar Staan We Nu? - VMR', 17 May 2018. <https://www.milieurecht.nl/nieuws/pas-een-jaar-later-waar-staan-we-nu>.

Huisman, Charlotte. 'Rechter buigt zich over omstreden snuffelprogramma dat fraude via computers moet ontdekken'. de Volkskrant, 29 October 2019. <https://www.volkskrant.nl/gs-ba4fb626>.

———. 'Rotterdam stopt omstreden fraudeonderzoek met SyRI'. de Volkskrant, 3 July 2019. <https://www.volkskrant.nl/gs-becb336a>.

———. 'SyRI, het fraudesysteem van de overheid, faalt: nog niet één fraudegeval opgespoord'. de Volkskrant, 27 June 2019. <https://www.volkskrant.nl/gs-b789bc3a>.

IVIR. 'Prof. Dr. Natali Helberger Elected Member of a Council of Europe Expert Committee on Human Rights Dimensions of Automated Data Processing and Artificial Intelligence', 2019 2018. <https://www.ivir.nl/helberger-elected-to-council-of-europe-expert-committee/>.

'Kickstart AI: Five Dutch Companies to Further Boost Artificial Intelligence in the Netherlands', 2019.

Klaassen, Niels. 'De computer oordeelt: u krijgt zes jaar gevangenisstraf'. AD.nl, 6 September 2019. <https://www.ad.nl/tech/de-computer-oordeelt-u-krijgt-zes-jaar-gevangenisstraf~a9dad560/>.

Middendorp, Jan. 'Op naar een nieuwe balans tussen overheid, markt en algoritmen'. de Volkskrant, 26 May 2019. <https://www.volkskrant.nl/gs-b378b396>.

Ministerie van Buitenlandse Zaken. 'Mensenrechtenrapportage 2018 - Inzet en resultaten buitenlands mensenrechtenbeleid'. Rapport, 29 May 2019. <https://www.rijksoverheid.nl/documenten/rapporten/2019/05/29/bijlage-kamerbrief-mensenrechtenrapportage-2018>.

———. 'Vrijheid van meningsuiting, internetvrijheid en onafhankelijke journalistiek - Mensenrechten - Rijksoverheid.nl'. Onderwerp, 23 October 2012. <https://www.rijksoverheid.nl/onderwerpen/mensenrechten/mensenrechten-wereldwijd/vrijheid-van-meningsuiting-en-internetvrijheid>.

Ministerie van Justitie en Veiligheid. 'Kamerbrief over motie transparantie van algoritmes in gebruik bij de overheid - Kamerstuk - Rijksoverheid.nl'. Kamerstuk,

9 October 2018.
<https://www.rijksoverheid.nl/documenten/kamerstukken/2018/10/09/tk-transparantie-van-algoritmes-in-gebruik-bij-de-overheid>.

Moll, Maarten. 'Nederlandse fotograaf doet aangifte tegen Facebook na verwijderen "blootkiekjes" Namibische vrouwen'. AD.nl, 8 August 2019. <https://www.ad.nl/binnenland/nederlandse-fotograaf-doet-aangifte-tegen-facebook-na-verwijderen-blootkiekjes-namibische-vrouwen~ac8543a8/>.

Naafs, Saskia. "'Living Laboratories": The Dutch Cities Amassing Data on Oblivious Residents'. The Guardian, 1 March 2018, sec. Cities. <https://www.theguardian.com/cities/2018/mar/01/smart-cities-data-privacy-eindhoven-utrecht>.

NLdigital. 'Nieuwe ethische gedragscode AI voor ICT-sector', 21 March 2019. <https://www.nldigital.nl/news/nieuwe-ethische-gedragscode-ai-voor-ict-sector/>.

NOS. 'Algoritmes moeten discriminatie in vacatureteksten opsporen', 10 August 2019. <https://nos.nl/l/2296998>.

———. 'D66 en CDA willen richtlijn en toezichthouder voor overheidsalgoritmes', 18 June 2019. <https://nos.nl/l/2289495>.

———. 'Overheid gebruikt op grote schaal algoritmes, "risico op discriminatie"'. NPO Radio 1, 29 May 2019. <https://www.nporadio1.nl/binnenland/16765-overheid-gebruikt-op-grote-schaal-algoritmes-risico-op-discriminatie>.

———. 'VN-rapporteur zeer bezorgd over Nederlands opsporingssysteem voor uitkeringsfraude', 21 October 2019. <https://nos.nl/l/2307132>.

NRC. 'Nederlandse fotograaf doet aangifte tegen Facebook voor verwijderen naaktfoto's'. Accessed 21 March 2020. <https://www.nrc.nl/nieuws/2019/08/08/nederlandse-fotograaf-doet-aangifte-tegen-facebook-voor-verwijderen-naaktfotos-a3969507>.

———. 'Solliciteren bij een algoritme'. Accessed 21 March 2020. <https://www.nrc.nl/nieuws/2018/05/11/solliciteren-bij-een-algoritme-a1602656>.

NU.nl. 'Tweede Kamer wil een algoritmemeldplicht voor de overheid', 24 September 2019. <https://www.nu.nl/politiek/5997764/tweede-kamer-wil-een-algoritmemeldplicht-voor-de-overheid.html>.

NWO. 'Responsible Use of Artificial Intelligence: Call for Proposals', 2020. <https://www.nwo.nl/en/documents/enw/responsible-use-of-artificial-intelligence--call-for-proposals>.

Parlementaire Monitor. 'Wet van 21 Februari 2018, Houdende Verklaring Dat Er Grond Bestaat Een Voorstel in Overweging Te Nemen Tot Verandering van de Grondwet, Strekkende Tot Het Opnemen van Een Bepaling over Het Recht Op Een

Eerlijk Proces - Parlementaire Monitor', 21 February 2018. <https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vkn2c4mspxy6>.

Rathenau Instituut. 'Overview of ethics codes and principles for AI', 19 March 2019. <https://www.rathenau.nl/en/digital-society/overview-ethics-codes-and-principles-ai>.

RTL Nieuws. "Algoritmes politie kunnen leiden tot discriminatie", 6 February 2019. <https://www.rtlnieuws.nl/tech/artikel/4599766/algoritmes-politie-kunnen-leiden-tot-discriminatie>.

———. "Facebook gaat satire en opinie niet factchecken", 1 October 2019. <https://www.rtlnieuws.nl/tech/artikel/4867766/facebook-gaat-satire-en-opinie-niet-factchecken>.

———. 'Staat gedagvaard om "ondoorzichtige" risicoanalyses burgers', 27 March 2018. <https://www.rtlnieuws.nl/tech/artikel/4128921/staat-gedagvaard-om-ondoorzichtige-risicoanalyses-burgers>.

Schellevis, Joost. 'Rechtszaak over fraudebestrijding overheid: "Burgers bij voorbaat verdacht"', 29 October 2019. <https://nos.nl/l/2308110>.

Staalduine, Jochem van. "Algoritmes bedreigen solidariteitsbeginsel verzekeringen". Trouw, 25 July 2019. <https://www.trouw.nl/gs-b65f2053>.

———. 'De Rotterdamse huishoudens die verdacht worden van fraude zijn diep beledigd: "Het lijkt wel '40-'45'''''''''. Trouw, 20 June 2019. <https://www.trouw.nl/gs-be0bd77f>.

Stibbeblog. 'Afdeling Bestuursrechtspraak Verfijnt Toetsingskader Voor Geautomatiseerde Besluitvormingsprocessen (AERIUS)'. Accessed 21 March 2020. <http://www.stibbeblog.nl/all-blog-posts/environment-and-planning/afdeling-bestuursrechtspraak-verfijnt-toetsingskader-voor-geautomatiseerde-besluitvormingsprocessen-aerius/>.

Teeffelen, Kristel van. 'Frauderisicosysteem SyRI schendt privacy niet, zegt de staat'. Trouw, 29 October 2019. <https://www.trouw.nl/gs-be3f90e3>.

Timmer, Ellen. 'Geautomatiseerde besluitvorming in het bestuursrecht | uitspraak ABRvS in zaak over AERIUS'. Ellen Timmer - juridische artikelen en berichten (blog), 25 December 2017. <https://ellentimmer.com/2017/12/25/geautomatiseerde-besluitvorming-in-het-bestuursrecht-uitspraak-abrvs-in-zaak-over-aerius/>.

Trouw. 'Tommy Wieringa wil niet dat de overheid zijn risico meet', 12 January 2018. <https://www.trouw.nl/gs-b58f21b5>.

Twede Kamer der Staten-Generaal. 'AI, publieke waarden en mensenrechten'.
Text, 8 October 2019.
https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail/2019Z19125/2019D39850.

Vegelian, Stephan. 'Voorspellende algoritmes duiken overal op, ook bij de boer in z'n stal', 28 June 2019. <https://nos.nl/l/2291044>.

Verhagen, Christian. 'Angst voor algoritmes is onterecht: "discriminerend" algoritme geeft slechts weer wat mensen denken'. Trouw, 1 July 2019. <https://www.trouw.nl/gs-b3179e7b>.

Vetzo, M.J., J.H. Gerards, and R. Nehmelman. 'Algoritmes En Grondrechten'. Montaigne Centrum voor Rechtstaat en Rechtspleging, 2018.

VNO-NCW. 'Algoritmen Die Werken Voor Iedereen Samen Bouwen Aan Onze (Digitale) Toekomst Met Artificiële Intelligentie: Position Paper - Taskforce A', 18 July 2019.