Rathenau Instituut

Directed digitalisation

Working towards a digital transition focused on people and values - The Dutch approach.

Report

Authors
Linda Kool, Elma Dujso and Rinie van Est

Editor Arnold Vonk

Cover photograph
A visitor to the Rijksmuseum viewing The Milk Maid by Johannes Vermeer.
Photograph Rob Voss - Hollandse Hoogte

Preferred citation:
Kool, L., E. Dujso, and R. van Est (2018). *Directed digitalisation – Working towards a digital transition focused on people and values – The Dutch approach.* The Hague: Rathenau Instituut

Foreword

Not so very long ago, algorithms were sums for mathematicians, *A.I.* was a subject for science fiction movies and *augmented reality* was above all a way of boosting enjoyment for gamers. Even the digital society was something new, and viewed by many with optimism. Today, the realisation has grown that digitalisation is a huge force that is rapidly changing society. Facial recognition technology has turned our public life upside down and the construction of 5G networks has delivered a huge boost to the *Internet of Things*.

In February 2017 we published our report *Urgent Upgrade – Protect public values in our digitized society* [*Opwaarderen – Borgen van publieke waarden in de digitale samenleving*], in response to a request from the Dutch Senate, asking the Cabinet to investigate whether society was paying sufficient attention to the ethical aspects of digitalisation. The senators suspected that this was not the case. Our investigation confirmed that such public values as privacy, security, equal treatment and autonomy were being compromised.

Now, eighteen months later, this situation continues. This report is a summary of all the efforts undertaken in this area, between January 2017 and June 2018. We carried out a literature study and identified the developments we are facing in a number of key domains. Although society's governance system has been strengthened, never before was there so urgent a necessity to view digitalisation as a transition, in which values occupy a pivotal position and in which society ensures that no one is excluded. With that in mind, government, businesses and individual citizens must continue over the coming years to take responsibility and work together at local, regional and international level.

The Cabinet took the first step in June 2018, with its National Digitalisation strategy. The strategy lays down plans for reinforcing the governance system in these areas. One major advance is that the Cabinet has recognised that digitalisation is a transition process.

We have identified growing awareness, and numerous isolated actions. What is still missing is a link between social issues and innovation. To bring about a digital transition that is truly focused on people and values, government and business will have to digitalise more decisively. It is important that the stakeholders in the Digital Summit that will be organised by the Cabinet in 2019, go further than simply presenting their progress. In this report, we therefore issue five recommendations.

Dr. Ir. Melanie Peters
Director Rathenau Instituut

Summary

Over the past eighteen months, the Netherlands has started to realise the massive scale of the impact of digitalisation on society. Digitalisation is not longer essentially a reference to a collection of gadgets but has gradually been recognised as a transition process, with opportunities and risks. A key question for the future is therefore how the Netherlands should structure that transition.

The most important message from the Rathenau Instituut is that government, the private sector and civil society organisations need to shape and direct the digital society in such a way that greater focus is placed on people and values. Only then can a digital society be created, in which no one is excluded. With that in mind, in this report we propose five actions.

A follow-up to the report *Urgent Upgrade*

This report is a follow-up to our report *Urgent Upgrade* published in February 2017, written in response to the Gerkens motion that was adopted by the Dutch Senate. That report mapped out a broad spectrum of societal and ethical aspects of digitalisation.

In *Urgent Upgrade*, we concluded that digitalisation was compromising certain public values such as privacy, digital security, equal treatment and freedom of expression. Furthermore, the governance system – the collection of actors and institutions responsible for defining social and ethical issues and placing them on the agenda – was insufficiently prepared to protect these public values. We therefore called for an underpinning or upgrading of the governance system, and called upon all parties to take the necessary action.

The Rathenau Instituut considers it important that the *Urgent Upgrade* report itself be rapidly updated, in view of the social relevance and urgency of the protection of public values in a digital age.

Ethical issues are more prominent on the agenda

This report will show that government and many other parties have started to act on the message from *Urgent Upgrade*. A whole raft of social and ethical questions, for example about our understanding of algorithms and a fair data economy, are far more clearly present on the agenda than two years ago. Policy makers, regulators and civil society organisations are already developing knowledge about the new themes. In respect of privacy and security, the step has been taken from agenda shaping and policy making to actual policy implementation. Over the past eighteen months, therefore, the governance system has changed for the better.

In other areas, themes have been placed on the agenda, but not yet translated into actual policy measures. Examples are the protection of democracy, understanding of algorithms and a fair, competitive data economy.

A number of technologies and their related societal issues have also not yet been placed on the agenda. Examples are facial recognition, virtual and augmented reality and the possible health effects of digital technology.

Working towards a digital transition focused on people and values

Various parties such as policy makers, politicians, civil society organisations, regional and local governments, professional associations and regulators recognise the importance of protecting public values. They are clearly considering the issue of what digitalisation means for their organisation, sector or practice. The key question however is how we can best manage this digital transition. Many have recognised that protecting public values and fundamental rights must be the starting point for digitalisation.

This means a turnaround in the debate on the deployment and influence of digital technologies: from a focus on technology and the assumption that it will automatically lead to social progress, to a focus on the interaction between digitalisation and values. On the one hand, digitalisation is a tool for tackling social challenges while on the other hand it is a development that could compromise public values. By viewing digitalisation as a transition, the focus is placed prominently on the question ‘what type of digital society do we want to live in?’. To answer that question, an integrated approach to innovation is needed, that gives shape and direction to the digital transition and as a result to our society, from the viewpoint of public values.

Five actions to reinforce the governance system

The Rathenau Instituut has proposed five actions that will help policy makers, businesses and civil society organisations to reinforce the governance system:

Invest in a value-driven approach to innovation

Ethical and societal issues cannot be considered in isolation from innovation or digitalisation processes. To fulfil the ambitions of the Netherlands, for example in healthcare, in the energy transition or with regard to mobility, it is essential to link innovation to societal issues: the Netherlands must no longer view public values as the final step in an innovation process, but as a starting point. This ties in with thinking on innovation policy in terms of mission-based innovation policy or targeted innovation systems.

Arrive at a proactive, overarching agenda and action plan for the societal and ethical aspects of digitalisation
Societal and ethical issues in digitalisation have been placed on the policy agenda, but there is still no integrated vision. A number of questions have not yet been translated into specific policy measures. A proactive agenda also calls for attention for topics that as yet barely feature on the agenda such as facial recognition, virtual and augmented reality and the possible health effects of technology. Any truly overarching agenda will also contain a vision on how to involve society (see point 5).

Invest in a strong position for supervisory bodies
Supervisory bodies represent a vital link when it comes to reinforcing the governance system with regard to digitalisation issues. These watchdogs have indeed become more focused on those issues. It is their role to invest in establishing knowledge and collaborating with other supervisory bodies. A number of these watchdogs have been granted new authorities or increased budgets. It is essential that we continue to monitor whether and to what extent these new powers and increased funding are sufficient. These actions of strengthening the watchdogs can be regarded as first steps. We are only just beginning to understand the true potential of digitisation. From a strategic viewpoint it is therefore vital that we continue to invest in the capabilities and capacities of the supervisory bodies.

The private sector: engage in socially responsible digitalisation
Politicians and society as a whole are becoming increasingly aware of the societal and ethical aspects of digitalisation. This has resulted in growing pressure on the private sector to tackle these issues seriously. Corporate social responsibility in the field of digitalisation calls for a proactive attitude from the private sector in recognising and indeed anticipating the societal and ethical implications of the technology they are developing. In a whole number of ways, businesses are obliged to make the effort to protect human rights. It is now up to them to shape their duty of care, in practice.

Encourage technological citizenship
In order to help set the course for innovation, individual citizens must be closely involved. They must be informed of the possibilities and risks of technology and must be able to participate in the democratic debate and political decision-making processes. It is important that we continue to encourage these three elements in any strong governance system. There must also be clear attention for the limits of the self-reliance of citizens, and their willingness to participate. Values-driven innovation means shaping innovation on the basis of shared, public values. This can only be achieved in consultation with society and that in turn calls for a vision from government.

Contents

Foreword 3

Summary 4

1 Introduction 9
1.1 Background 9
1.2 Purpose of this report 11
1.3 Digitalisation and public values 12
1.4 Governance system 15
1.5 Research questions and approach 19
1.6 Readers' guide 21

2 Fundamental rights and human rights 22
2.1 The Netherlands 22
2.2 Council of Europe 24
2.3 International 28
2.4 Conclusion 31

3 Social actors and the public debate 33
3.1 Key issues from the debate in the media 34
3.1.1 The Netherlands 34
3.1.2 International 36
3.2 Civil society organisations 37
3.3 Umbrella organisations for businesses and employees 44
3.4 International developments 47
3.5 Conclusion 49

4 Politics and administration: agenda setting 51
4.1 The Netherlands 51
4.2 International developments 67
4.3 Conclusion 72

5 Politics and administration: policy development and political decision making 74
5.1 Cabinet and Ministries 75
5.1.1 Ministry of the Interior and Kingdom Relations (BZK) 75
5.1.2 Ministry of Economic Affairs and Climate Policy 79
5.1.3 Ministry of Justice and Security (JenV) 84

5.1.4 Ministry of Education, Culture and Science (OCW) 88
5.1.5 Ministry of Foreign Affairs (BuZa)... 90
5.2 Dutch Senate and House of Representatives............................ 91
5.3 European Commission 94
5.4 European Parliament.. 99
5.5 Conclusion... 103

6 Politics and administration: Supervisory bodies 103
6.1 Netherlands 103
6.2 International... 114
6.3 Conclusion... 118

7 Shaping the digital transition based on public values 119
7.1 Digital transition 119
7.2 The upgrading has begun.. 120
7.2.1 State of affairs mid 2018 121
7.2.2 Broadening the debate.. 123
7.3 Blind spots partially covered.. 124
7.4 Recommendations 131
7.5 Finally... 136

Bibliography 137

Appendix 1 Parliamentary questions and motions.. 151

Appendix 2 The significance of public governance 15160

1 Introduction

1.1 Background

In the motion tabled by Gerkens c.s. on 23 September 2014, the Dutch Senate called upon the government to 'ask the Rathenau Instituut to explore the desirability of appointing a committee that could advise on the ethical aspects of the digitalisation of society' (Dutch Senate 2014-2015, CVIII, E). The Ministry of the Interior and Kingdom Relations responded by asking for an investigation to be carried out, at the end of 2015.

On 9 February 2017, we published the report *Urgent Upgrade. Safeguarding public values in the digital society* (Kool et al. 2017).[1] In this report, we mapped out the nature of the 'governance system' with regard to the ethical and societal aspects of digitalisation: the combination of actors and institutions responsible for shaping and placing societal and ethical issues on the agenda.

In brief, governance relates to the collective administration of the issues facing our society. It deals with such questions as:

- Which public problems have been identified and placed on the political agenda?
- Which interests and values are fully or less fully elaborated?
- How do the various actors in society discuss these problems?
- Who is or is not involved, and to what extent?

We examined eight key trends in digitalisation technology (see also table 1):

1. robotics;
2. the Internet of Things (IoT);
3. biometrics;
4. persuasive technology;
5. digital platforms (including blockchain);
6. virtual and augmented reality and social media;
7. big data and algorithms; and
8. artificial intelligence (AI).

We revealed that these trends bring with them a range of societal and ethical questions. In addition to the already well recognised IT-related societal themes of privacy and security, other key issues emerging within the IT domain include autonomy, equity and equality, human dignity, control over technology and balances

[1] See also: https://www.rathenau.nl/en/digital-society/urgent-upgrade

of power. The broadening of the societal and ethical questions in respect of digitalisation goes hand in hand with the ‘cybernetic feedback loop’: the fact that data are collected on a huge scale and are in fact already being analysed and used on that scale (see figure 1). In other words, digitalisation is increasingly becoming ‘cybernetisation’.

In the *Urgent Upgrade* study, we revealed the limited capacity of the Dutch governance system to deal with the (emerging) societal and ethical themes relating to digitalisation, at the start of 2017. We identified five blind spots that needed to be addressed urgently. There was a need for action with regard to:

1. translating emerging societal and ethical issues into policy; we found a lack of interdepartmental consultation and coordination on digitalisation and political debate on these emerging issues;
2. safeguarding fundamental rights and human rights in the digital society;
3. strengthening supervisory bodies and seeing to it that they consult one another;
4. new responsibilities for companies that develop digital products and services; and
5. facilitating opposing voices by strengthening civil society, augmenting the public’s knowledge and skills, and promoting public debate on digitalisation.

The report *Urgent Upgrade* clearly revealed that public values were insufficiently safeguarded in our digital society. We concluded that the governance system needed to be strengthened. The key message was that ‘the government, industry and civil society must now take action to strengthen the governance landscape, thus ensuring that public values in the digital society will continue to be properly safeguarded’ (Kool et al. 2017, 12). We put forward a five-part proposal for the identified parties:

1. Appoint an interdepartmental working group charged with shaping a government vision on how to deal with the societal and ethical significance of digitalisation and with ensuring coordination in the political-governance domain.
2. Strengthen the role and position of supervisory bodies.
3. Draw up a ‘Digitalisation agreement’ laying out the commitment and responsibilities of businesses, government and civil society actors with regard to safeguarding public values in the digital society.
4. Hold a national debate on the significance of digitalisation in terms of safeguarding public values.
5. Schedule regular political debates in the Senate and House of Representatives in the Netherlands on the governance of societal and ethical digitalisation issues.

1.2 Purpose of this report

The report *Urgent Upgrade* was itself a wake-up call, addressed to government, business and civil society. It demanded greater attention and action with regard to safeguarding public values in respect of digitalisation. This report is at it were an update to the report *Urgent Upgrade.*

Why then did we decide to publish this update so soon after the initial report? Firstly, it relates to the urgency perceived by the Rathenau Instituut in safeguarding public values in our digital society. Two working conferences organised by the Rathenau Instituut in collaboration with the Social Economic Council (SER) demonstrated that this perceived relevance and urgency were equally shared by numerous societal stakeholders.[2] Within the Dutch House of Representatives and Senate, too, this sense of urgency is shared by many parties.

Secondly, in the past two years, a variety of activities have been undertaken in the governance of societal and ethical digitalisation issues. It would appear that the desired process of upgrading the governance system has been initiated.

The aim of this study is to identify the initiatives taken in a variety of fields. We have attempted to sketch a comprehensive overview of the way in which steps have been taken over the past two years in upgrading and updating the Dutch governance system in respect of the ethical and societal aspects of digitalisation. The aim of this study, via this update, is to contribute to the further strengthening and modernisation of the governance system, and as a result the proper safeguarding of public values in our digital society.

This goal is far from being reached. A broad overview of the current state of affairs with regard to the governance system may grant an insight into how the modernisation of that system can be successfully and effectively further shaped.

[2] See Rathenau Instituut & SER (2018). Acties voor een verantwoorde digitale samenleving (Actions for a responsible digital society). The aim of this study was to investigate which aspects of digitalisation the social actors view as urgent, and what possibilities those social actors see for possible solutions and actions in this respect. Participants included companies, knowledge organisations, interest groups representing consumers and citizens, the national government, implementing bodies, supervisory bodies and local government. See also: https://www.rathenau.nl/nl/digitale-samenleving/acties-voor-een-verantwoorde-digitale-samenleving

1.3 Digitalisation and public values

Digitalisation offers society a broad range of economic and social opportunities. For example, more efficient business practice, the early identification of diseases or more rapid knowledge sharing. Whenever we use the term ‘digitalisation’ in this report, we are referring to a cluster of digital technologies that now and over the coming years will acquire a place in our society. This cluster consists of eight areas of technology, as shown in table 1 (see also Kool et al. 2017).

Table 1 Overview of areas of technology

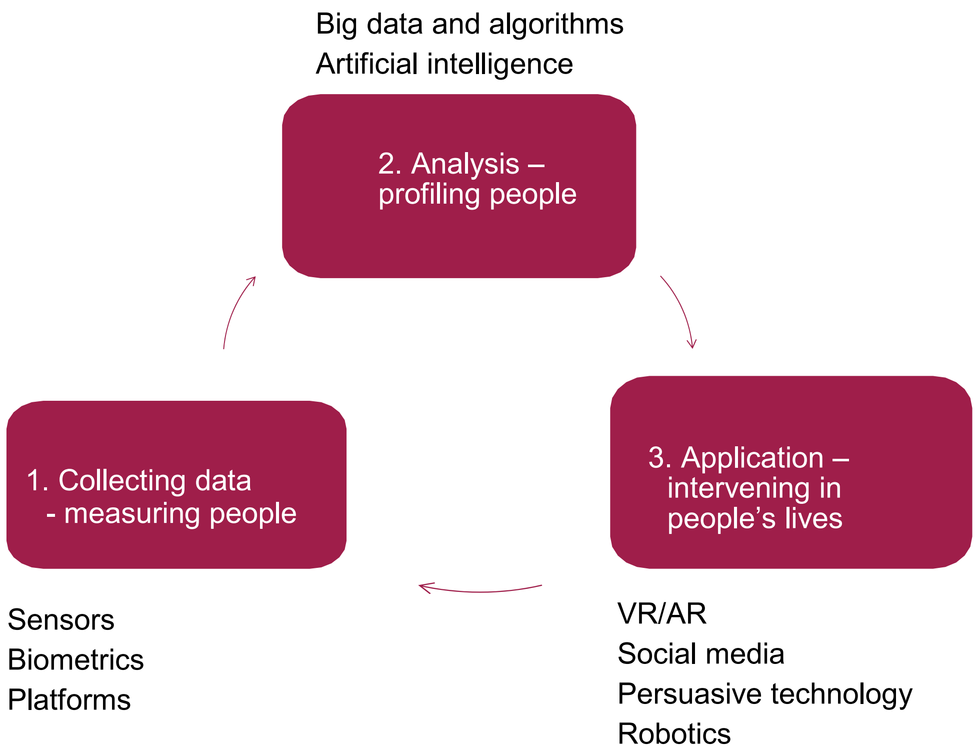
Overview of areas of technology
Robotics
Internet of Things (IoT)
Biometrics
Persuasive technology
Digital platforms (including blockchain)
Virtual and augmented reality
Big data and algorithms
Artificial intelligence (AI)

Source: Rathenau Instituut

As a result of these technologies, more and more aspects of the physical world are becoming intertwined with the digital world. A cybernetic feedback loop has been created, in which data are collected, analysed and immediately re-employed. In other words, a feedback loop in which people are measured and profiled, followed by intervention in the lives of people, their behaviour or their environment (see figure 1).

The areas of technology referred to above play an important role in various aspects of this feedback loop (see figure 1). People, for example, are profiled using big data and algorithms, as well as artificial intelligence (AI).
On the other hand, these technologies often incorporate multiple elements of the loop. A social network, such as Facebook, not only collects data but also analyses that data to adapt the platform.

Figure 1 Cybernetic feedback loop



Source: Rathenau Instituut

In the report *Urgent Upgrade*, we argued that although the process of digitalisation has been underway for decades, this feedback loop has sounded in the advent of a new phase in digital society. The feedback loop makes the real-time adjustment of the physical world possible.

This is demonstrated, for example, in smart learning platforms that monitor the performance of students and offer them adapted learning assignments on that basis. Or a smart thermostat, which on the basis of information about a house and an analysis of the behaviour of its residents automatically adjusts the temperature in the dwelling. Or a smart streetlamp that measures human behaviour using sensors, and attempts to influence that behaviour by the use of light.

The ability to 'complete' the feedback loop – in other words real-time fine tuning in the physical world – raises new ethical and societal questions. On the basis of scientific literature, in *Urgent Upgrade*, we identified seven ethical and societal topics, that will also play a key role in this report; see table 2. These topics can be viewed as essential public values, closely related to fundamental rights and human rights. Such issues as privacy and equality are for example reflected in the right to respect for personal privacy, the right to equal treatment and the right to a fair trial.

Human dignity and security are not elements of the Dutch Constitution but are referred to in international treaties such as the Charter of Fundamental Rights of the European Union and the Universal Declaration of Human Rights.
Values such as autonomy, equal balances of power and control over technology are not explicitly mentioned in these treaties or charters, but may be viewed as elements or natural consequences of these fundamental rights and human rights.

Table 2 Overview of societal and ethical topics[3]

Topic	Issue
Privacy	Data protection, digital inviolability of the home, mental privacy, surveillance, function creep
Autonomy	Freedom of choice, freedom of expression, manipulation, paternalism
Security / safety	Information security, identify fraud, physical safety
Control over technology	Control and transparency of algorithms, responsibility, accountability, unpredictability
Human dignity	Dehumanisation, instrumentalisation, de-skilling, de-socialisation, unemployment
Equity and equality	Discrimination, exclusion, equal treatment, stigmatisation
Balances of power	Unfair competition, exploitation, relation between consumers and businesses

Source: Rathenau Instituut

The processes within the data feedback loop raise a variety of societal and ethical questions as shown in figure 2. The process of data collection and processing (measurement) above all leads to discussions about privacy protection. The ever growing possibilities for collecting personal data are constantly threatening new dimensions of privacy.

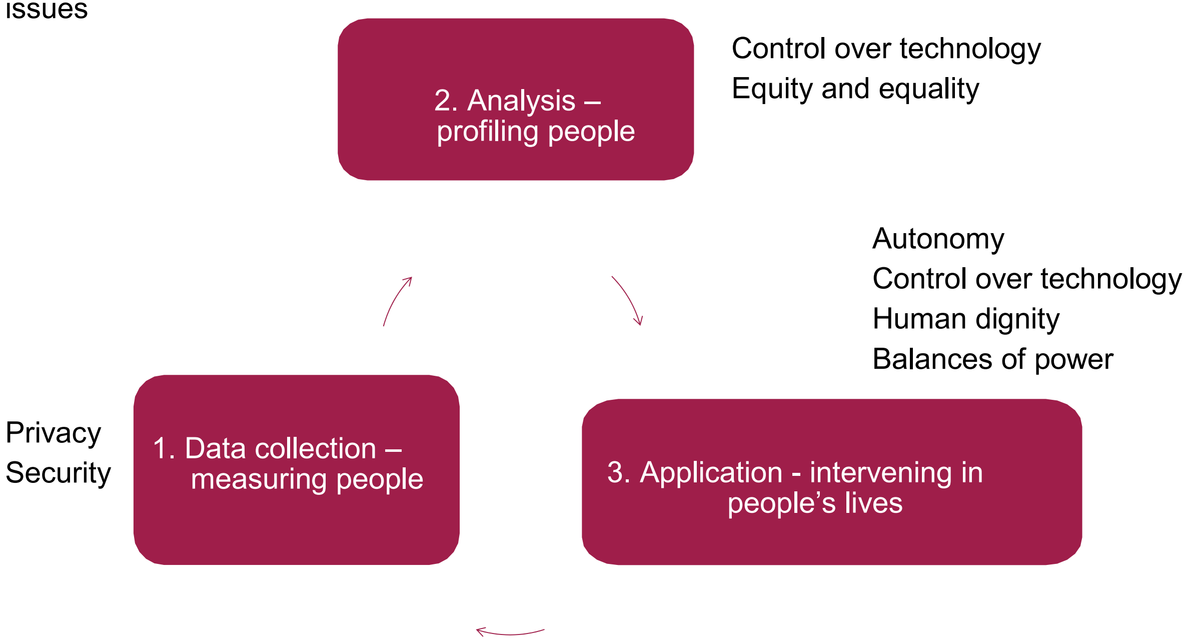
- Advances in such techniques as facial and emotional recognition have led to discussions about the freedom to think and feel what you want (mental privacy).
- The process of data analysis (profiling) and new techniques employed for that purpose (such as self-learning algorithms) lead to concerns about the right to equal treatment and human dignity (and the role of people in respect of computers and other machines).

[3] These themes were elaborated following an extensive literature study. For each area of technology, a search was undertaken in scientific literature for societal and ethical aspects in the period 2010-2016. The societal and ethical issues identified were clustered in these 7 themes (see also Royakkers et al. 2018).

- In the process of feedback to the physical world – intervention and (fine) tuning – discussions have emerged about how far technological influence can be allowed to go, how autonomy can be protected and who still has control over technology, and to what extent.

In this report, we use figure 2 to clarify how the discussion about the societal and ethical aspects of digitalisation has developed. Which areas of technology and which topics are on the agenda, and how?

Figure 2 Cybernetic feedback loop and the accompanying societal and ethical issues



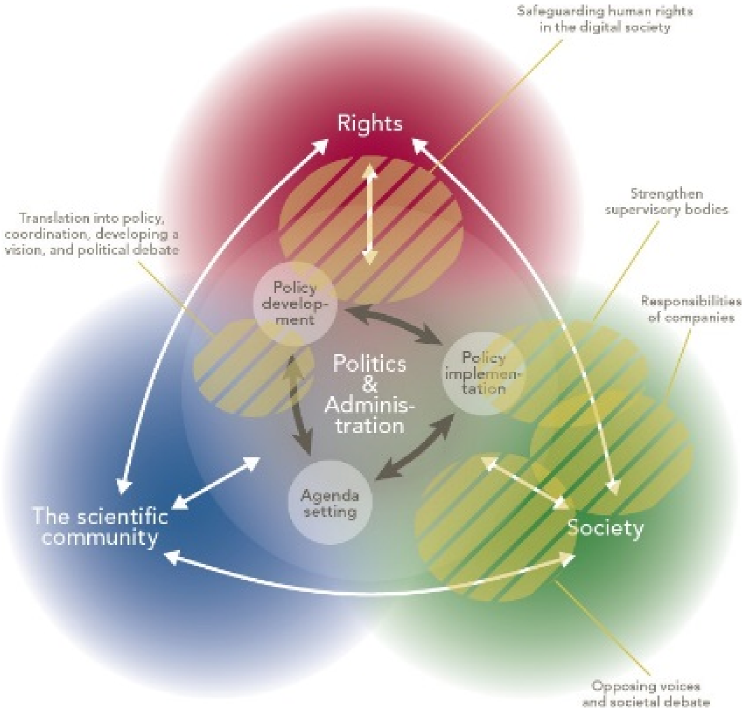
Source: Rathenau Instituut

1.4 Governance system

The central focus of this report is the governance of the ethical and societal challenges of digitalisation. In studying that question we use the conceptual framework from *Urgent Upgrade*. Essential to our approach is the distinction made between governance and meta-governance (see appendix 2).[4]

[4] This entire section 1.4 is based on section 4.8 ('Framework for the governance ecosystem') in Urgent Upgrade. Appendix 2 is almost identical to Appendix B from that report.

Figure 3 The governance system


Safeguarding human rights in the digital society
Rights
Strengthen supervisory bodies
Translation into policy, coordination, developing a vision, and political debate
Responsibilities of companies
Policy develop-ment
Policy implemen-tation
Politics & Adminis-tration
Agenda setting
The scientific community
Society
Opposing voices and societal debate

Source: Rathenau Instituut

Governance, as already stated, refers to the collective approach to the issues in our society.[5] It refers to such issues as:

- What public problems have been identified and placed on the political agenda?
- What interests or values have been successfully or less successfully elaborated?
- How do the various actors in society discuss these problems?
- Who is or is not involved, and to what extent?

Meta-governance suggests that the collective administration of societal problems takes place in a governance system, in other words in a collection of institutions, administrative and social processes and players. Meta-governance reflects the nature, structure and functioning of the governance ecosystem and refers to such questions as:

- Which institutions are available for discussing societal problems, and placing them on the political agenda?
- How is harmonisation achieved between public and private actors?
- How are public values safeguarded at an institutional level?
- Which institutions have been created over the years for that purpose?

[5] Governance is aimed at addressing public issues. These are societal problems, i.e. problems that can only be solved through collective action (cf. Hoppe 2010).

In this report, we above all consider the **governance system** for the societal and ethical aspects of digitalisation. In *Urgent Upgrade* we developed a framework to study such a governance system[6] In this framework, we distinguish between four domains; see figure 3: fundamental rights and human rights, society, the scientific community, and politics and administration.

Within the field of politics and administration, we distinguish between: a) agenda setting, b) policy development and political decision making, and c) policy implementation.

Fundamental rights and human rights

Ethical and societal discussions with regard to new technology often deal with the question of which values are at stake. Fundamental rights and human rights are often referred to. Human rights are the rights accruing to every individual. They are aimed at protecting people against the power of the state and their role is to ensure that everyone can live in human dignity.[7] They are for example laid down in:

- the Universal Declaration of Human Rights of the United Nations (1948);
- the European Convention on Human Rights (ECHR) of the Council of Europe (1950);
- and the Charter of Fundamental Rights of the European Union (2000).

Human rights are also laid down in national constitutions, such as the Dutch Constitution. In such documents, they are often referred to as ‘fundamental rights’.

These treaties record values that are important to the Netherlands, such as human dignity, freedom, security, equality and justice. Technological developments can strengthen human rights, but also place them under pressure. They can also give rise to a reformulation of existing human rights and fundamental rights. In this report, we consider these questions in the domain of activities of the bodies charged with examining the significance of new technologies for human rights and fundamental rights, such as Government Committees, the Council of Europe and the UN Human Rights Council.

Society

Actors in society such as businesses, non-governmental organisations (ngos) and individual citizens play an important role in the governance of societal and ethical aspects of digitalisation:

[6] We achieved this by providing a historical overview of dealing with societal and ethical issues in relation to four technologies: ICT, biotechnology, genome technology and animal experimentation

[7] See the website of the Dutch Human Rights Commission (College voor de Rechten van de Mens): http://www.mensenrechten.nl/wat-zijn-mensenrechten/wat-zijn-mensenrechten

- Businesses and technology developers shape digital technology and in that process make their own, sometimes moral choices. On the basis of self-regulation mechanisms – such as internal ethical committees, codes of conduct and covenants – businesses determine how they wish to behave.
- Civil society organisations feed the political-administrative and social discussion on ethical and societal aspects of digitalisation, and contribute to awareness among individuals.
- Every individual, by making their choices and through their own actions, of course also help to shape the place occupied by digital technology in society.

The scientific community

Scientific knowledge can be useful in

- identifying and articulating societal and ethical aspects,
- formulating a policy position and determining a perspective for action (policy shaping); and
- reflecting on policy implementation.

The scientific community makes a direct contribution to the political-administrative process by supplying scientific knowledge, on request, to assist politicians and policy makers. This for example takes the form of studies or when individual scientists are consulted as experts during a hearing or round table discussion in the Dutch House of Representatives or Senate. National advisory boards and public research institutes also provide knowledge used in policy making.

In *Urgent Upgrade*, we mapped out the societal and ethical issues identified by scientists with regard to digitalisation. We summarised these findings in seven public values, and in this report we make use of this scientific analysis to identify which issues have or have not been discussed.

Politics and administration: agenda setting

With regard to agenda setting, in this study, we examine the professional advisory bodies whose aim is to identify new social and ethical issues, to place them on the agenda and to advise policy makers and politicians accordingly. In addition, civil society organisations, public perceptions, citizens and the media all play their part in setting the policy agenda. This phase is also called ‘ethical deliberation’ (Ladikas et al. 2015).

Politics and administration: policy development and political decision making

Deliberation on ethical and social issues can lead to policy development and political decision making, a phase in which (political) decisions are prepared and made on the identified social and ethical issues. In a democratic society, there are always differences in insights, opinions and beliefs on how to deal with social and ethical issues. In that sense, political decision making by parliament occupies a special role.

The phase of policy development and political decision making can lead to the establishment or amendment of regulatory frameworks and to decisions on other policy instruments such as making a trend analysis, forming a temporary committee, holding a societal dialogue or providing research funding.

Politics and administration: policy implementation
A third phase consists of policy implementation, when the above decisions are put into practice. Here, too, all kinds of intermediary bodies are involved in steering or actually implementing the adopted policies. These include supervisory bodies who enforce the regulatory framework, the judiciary and ethical review committees, who time and again assess whether parties have adhered to these frameworks, on the basis of regulatory frameworks and protocols.

1.5 Research questions and approach

In summary, this report provides an update on the governance system for the ethical and societal aspects of digitalisation. In doing so, it answers the following questions: What actions have the various actors taken since 2017 to consider the ethical and societal aspects of digitalisation or to put them into policy? What has changed since *Urgent Upgrade*?

In this study, we above all aim to provide an overview of which issues and values have been placed on the political agenda by the various parties, and which have not, and to identify which parties and institutions are available for bringing these issues into the political arena. We provide no substantive assessment of the actions or initiatives by these various actors.

To identify which issues and digital technologies have been placed on the agenda, we use the eight areas of technology selected in *Urgent Upgrade* (table 1) and the seven ethical and societal topics (table 2).

On the basis of desk research, we map out which parties have identified which issues, and how the identified problems have been tackled in politics and policy making. The descriptions of the advisory boards, supervisory bodies and interest groups were prepared on the basis of desk research and contacts with the organisations in question. In each chapter we discuss one of the four domains that make up the governance system (fundamental rights and human rights, society, agenda setting, policy development and political decision making and policy implementation; see figure 3).

For each domain we discuss the relevant actors. The focus is on developments in the Netherlands but we also consider various relevant developments in Europe. The period of study is 1 January 2017 to 30 June 2018. The only exception is the Government Digital Agenda which was published in July 2018, but which was included, given its relevance for this subject. We summarise the activities in tables.[8]

In chapter 3, social actors, we refer to important subjects in the media. We also map out the activities of various interest groups representing citizens, consumers, professionals and businesses (including employers' and employees' organisations). We also refer to a number of European and international civil society organisations and interest groups. Legal actions instituted by these organisations are also discussed under the heading social actors. We do not consider organisations from individual European countries, and have also not considered individual businesses.

In chapter 4, agenda setting, we consider the reports published by advisory councils during this period. No consideration was given to essays and round table discussions and other activities involving these advisory councils. According to the framework, Cabinet reactions to reports from advisory councils belong in policy development (chapter 5) but to improve readability, they are discussed under agenda setting, alongside the reports themselves. In the chapter on policy development, we do of course refer back to these government reactions. The Rathenau Instituut is part of the governance system for the societal and ethical aspects of technology and digitalisation. The expressly stated task of the Rathenau Instituut is to encourage public and political opinion on science and technology. We therefore also refer to the activities of the Rathenau Instituut itself in chapter 4.

In chapter 5, policy development and political decision making, we deal with the policy activities of the Ministries most involved in the ethical and societal aspects of the digital society. These are the Ministries of Interior and Kingdom Relations (BZK), Economic Affairs and Climate Policy (EZK), Justice and Security (JenV), Education, Culture and Science (OCW) and Foreign Affairs (BuZa).[99] We discuss the most relevant documents such as agendas, strategies and policy documents on the societal and ethical aspects of digitalisation. We also examine the activities of the Dutch Senate and House of Representatives.

[8] We are grateful to Tim Jacquemard for the data processing involved.

[9] Of course other Ministries also deal with ethical and societal aspects of digitalisation in parts of their remit

For the period between 1 January 2017 and 30 June 2018, we examine the written questions and motions submitted about the societal and ethical aspects of digitalisation, and expert meetings (Senate) and round table discussions (House of Representatives) (see Appendix 1). In this chapter, we also discuss a number of policy initiatives by the European Commission (with regard to the digital single market) and the European Parliament (resolutions relating to the societal and ethical aspects of digitalisation).

A number of actors (umbrella organisations, ngos, advisory councils, etc.) are not considered in the analysis if they have not outlined any reports/undertaken any activities relating to ethical and societal aspects of the digital society during the period investigated. Actors, reports and policy documents that do deal with digitalisation, but focus mainly on the financial and economic or technical aspects, are not considered.
Nonetheless, given the huge number of relevant initiatives undertaken during the period investigated, it is not possible for our overview to be complete.

This study follows the quality guidelines of the Rathenau Instituut. The report was also submitted for an internal review by a researcher not involved in the study.

1.6 Readers' guide

This report is structured as follows:

- Chapter 2, **Fundamental rights and human rights***,* provides an overview of the activities of the institutions involved with fundamental rights and human rights in relation to digitalisation and public values, such as national committees and in Europe the Council of Europe.
- Chapter 3, **Social actors***,* maps out the activities of various social actors and the media in respect of public values and digitalisation. We discuss a number of different interest groups for consumers, employers and employees.
- Chapter 4, **Agenda setting***,* lists the publications from a variety of advisory councils in the Netherlands and Europe with regard to digitalisation and public values.
- Chapter 5, **Policy development and political decision making***,* outlines the activities of various Ministries and of the Dutch parliament. We also discuss relevant policy initiatives from the European Commission and a number of relevant initiatives abroad.
- Chapter 6, **Policy implementation***,* offers an overview of the activities of regulators and other supervisory bodies in the field of public values and digitalisation.
- Chapter 7, **Conclusions***,* summarises the findings and presents our conclusions.

2 Fundamental rights and human rights

In this chapter, we describe the activities of institutions that dedicate themselves to the significance of digitalisation for fundamental rights and human rights. We consider the Netherlands (its national committees, for example), the Council of Europe and the United Nations (UN).

As compared with the report *Urgent Upgrade*, we do observe a rise in the degree of attention focused on various areas of technology such as big data, AI, persuasive technology, platforms and robotics, and their significance for fundamental and human rights. As a consequence, other issues alongside privacy have been placed on the policy agenda. Such institutions as the Council of Europe and the UN are now also calling for attention for rights and freedoms (such as the freedom of expression and the freedom of association), equality, and the right to a fair trial in relation to digitalisation.

Notably, there is yet little consideration for such areas of technology as biometrics (facial recognition) and virtual and augmented reality and their significance for fundamental rights and human rights.

2.1 The Netherlands

Privacy

For some time now, there has been discussion in the Netherlands as to whether and to what extent the Dutch Constitution needs to be adapted to the digital age. In 2009, a national committee (Staatscommissie Thomassen) was appointed to advise on a possible revision of Dutch fundamental rights, partly in view of digitalisation. In 2010, the committee recommended revising fundamental rights in line with the developments in information technology.

Specifically, the committee proposed a revision of article 13 of the Constitution. Article 13 concerns the right to confidentiality of postal mail, telephone and telegraph. The committee proposed extending the scope of article 13 to include all means of communication, in order to arrive at technology-independent protection ((Parliamentary Papers II 2010-2011, 31570, no 20).

On 11 July 2017, the Dutch Senate adopted the proposed amendment to the Constitution.[10][11] As a result, the first reading of the proposal was passed by both Houses. In 2018 and 2019, a second reading will follow in the Dutch House of Representatives and the Dutch Senate respectively (as is necessary for any amendment to the Constitution).

Algorithms and fundamental rights

A new item on the Dutch policy agenda is attention for the significance of algorithms for fundamental rights other than privacy. The Dutch Ministry of the Interior and Kingdom Relations (BZK) is examining the significance of algorithms, big data and AI for fundamental rights (see also chapter 5). Specifically, their considerations relate to (Vetzo et al. 2018):

- rights to privacy (including human dignity, personal autonomy and self-determination;
- rights to equality (right to non-discrimination);
- rights to freedom (including freedom of expression, freedom of religion, freedom of association and the right to vote); and
- procedural rights (right to a fair trial).

The Cabinet expects to be able to send its response to this study to the Dutch House of Representatives, in the autumn of 2018.

Digitalisation and protection of democracy

The significance of digitalisation for the democratic system – in particular with regard to big data, algorithms and micro targeting (personalising political messages as precisely as possible) – has also recently been placed on the policy agenda. At the start of 2017, the ‘National Parliamentary System Committee’ was established. The aim of this committee is to investigate whether the Dutch parliamentary system still functions properly, and whether it is futureproof.[12] This national committee is also investigating the influence of digitalisation on the (future) functioning of the parliamentary system.

According to the committee, the use of big data and micro targeting in election campaigns and the possibility that democratic institutions can be hacked with this in mind could threaten fundamental democratic values (National Parliamentary System Committee, 2017, p. 57).

[10] The official statement for amendment to article 13 of the Constitution – namely the statement that there are grounds to consider a proposal to amend the provision in the Constitution concerning the confidentiality of postal mail, telephone and telegraph was issued on 19 August 2017 (Parliamentary Paper 2017, 33989, no. 334).

[11] In addition, the Minister of BZK announced that if initiatives are issued by the Dutch House of Representatives concerning the horizonta effect of article 13, wherever possible he would support these (Parliamentary Papers 2016-2017, T02460, no. 33989). The horizontal effect of fundamental rights and human rights applies to fundamental rights concerning the relationship between citizens and concern private law relationships. The vertical effect is the application of fundamental rights to the relationship between citizens and government.

[12] See: https://www.staatscommissieparliamentairstelsel.nl/

At the end of 2018, the national committee is expected to issue its recommendation. In addition, the Ministry of the Interior and Kingdom Relations (BZK) also called upon the Council for Public Administration (ROB) to investigate the effects of digitalisation on democracy, and possible perspectives for action by government (Parliamentary Papers II 2017-2018, 34 775 VII, no 52).

Table 3 Overview of developments in Dutch fundamental rights, in outline

(1 January 2017 - 30 June 2018)

	Technology	Issue	Action
National Parliamentary System Committee	Social media, digitalisation	Protection of democracy	Digitalisation as one of the six topics of the problem assessment
Government	Digitalisation	Specifically: confidential communication	Constitutional revision article 13 in 2017
Ministry of the Interior and Kingdom Relations	Algorithms	Specifically: impact of algorithms on fundamental rights	Investigation into the impact of algorithms on the effectiveness of fundamental rights
Ministry of the Interior and Kingdom Relations	Big data, algorithms and platforms	Specifically: protection of democracy and related fundamental rights	Request for Advice from the Council for Public Administration on digitalisation and democracy

Source: Rathenau Instituut

2.2 Council of Europe

In Europe, the Council of Europe plays an active role as the guardian of human rights. In 1950, this Council drew up the European Convention on Human Rights, and at the end of the 1980s the Council played an important role in the fields of ethics and biotechnology. In the period under review in 2017-2018, the Council of Europe has been active in a large number of fields, for example with regard to AI, automated data processing, persuasive technology (via platforms and social media), developments in the biomedical industry, robots and automatic weapons. We discuss the relevant areas below, in more detail.

Technology convergence

The Parliamentary Assembly of the Council of Europe (PACE) investigated the significance of technology convergence (ever more advanced integration of humans and technology) for human rights.

In April 2017, PACE issued its recommendations to the Council of Ministers.[13] Among others, PACE recommended:

1. allowing the basic principles from the Convention on Human Rights and Biomedicine,[14] such as the protection of private life, respect for autonomy and the right to information to also be applied outside the biomedical world, because just like biotechnology, digitalisation intervenes in human beings;
2. to develop measures for the use of (health)care robots and supporting technology in the *Council of Europe Disability Strategy 2017-2023*.[15]
3. to recognise the necessity of ensuring that every machine, every robot and every artificially intelligent artefact remains under human control;to adopt new rights relating to the right to respect for private life and family life:
   a. the possibility of refusing to be profiled, tracked, manipulated and influenced; and
   b. in the event of care and supervision for the elderly and disabled persons, the right to opt for human contact rather than a robot;
4. to introduce measures for the use of AI in the courtroom; and
5. to introduce tighter regulations for drones and other artificially intelligent systems that are used in wartime: there may be no automated procedures for the selection of individuals for targeted killing based on mass surveillance techniques.

In its response, the Council of Ministers announced the launching of the new *Disability Strategy 2017-2023*, with specific attention for the use of healthcare robots and assisting technologies and for the prevention of discrimination (Committee of Ministers, 2017).[16] In addition, big data guidelines have been adopted aimed at automated data processing.[17] Other recommendations from PACE, for example with regard to profiling and respect for family life, have either been included by the Council in these guidelines or submitted to the Human Rights Committee for inclusion of these aspects in the elaboration of human rights for the elderly.[18]

[13] The recommendations were drawn up in response to the motion *Technological convergence, artificial intelligence and human rights* (PACE, 2015). At the request of PACE, the Rathenau Instituut and the rapporteur wrote the report *Human rights in the robot age* (Van Est & Gerritsen, 2017), in which the institute called among other things for two new human rights: the right to not be measured, analysed or influenced and the right to meaningful human contact (Rathenau Instituut, 2017); see also: https://www.rathenau.nl/nl/digitale-samenleveing/mensenrechten-het-robottijdperk

[14] This convention is also known as the ‘Oviedo Convention’ (ETS No. 164). See: https://rm.coe.int/168007cf98

[15] See also: https://rm.coe.int/16806c400c

[16] See: https://www.coe.int/en/web/disability/cyprus-conference-march-2017

[17] See: https://rm.coe.int/16806ebe7a

[18] CM(2014)2, See: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c68ce

The Council also approved the recommendations from PACE for the Bio-ethics Committee (DH-BIO).[19] An action plan will be developed to chart out the impact of the developments in the biomedical industry on human rights, and on that basis to lay down the objectives of the DH-BIO (DH-BIO 2017). The plan was to be based in part on the outcomes of the conference to celebrate the 20th anniversary of the Convention on Human Rights and Biomedicine, in October 2017. The conference above all dealt with the challenges to human rights as a result of developments in the field of genetics and genomics, and the use of big data in healthcare.[20]

Automated data processing and AI

In 2017, the Council of Europe established a group of experts which was tasked with considering human rights and automated data processing, in 2018-2019. This Committee of experts on Human Rights Dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT)[21] was the successor to the Committee of experts on Internet Intermediaries (MSI-NET), that focused on the responsibilities of Internet platforms and automated data processing. In its final report 'Algorithms and human rights', the conclusions of the MSI-NET included the observations that:

- Public supervision of automated data processing is desirable; this supervision should not be entrusted entirely to private parties (Council of Europe, 2018).
- public organisations must be held responsible for the decisions they take on the basis of algorithmic processes; and
- greater public debate is needed on this subject.

On the basis of this report, the Committee of Ministers of the Council called upon the Member States to clarify the responsibilities of Internet companies and social media platforms (CM/Rec(2018)2).[22]

Digitalisation and the media

Also in 2017, the Council of Europe established the Committee of Experts on Quality Journalism in the Digital Age (MSI-JOQ).[23] As well as preparing standards for quality journalism in the digital age, over the next two years, this committee will also be examining media literacy in a digital environment.

[19] See: https://rm.coe.int/inf-2017-5-e-info-doc-dh-bio/168077c578

[20] See also: https://rm.coe.int/oviedo-conference-rapporteur-report-e/168078295c

[21] See: https://www.coe.int/en/web/freedom-expression/msi-aut

[22] https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2018-2-of-the-committee-of-ministers-to-member-states-on-the-roles-and-responsibilities-of-internet-intermediaries?inheritRedirect=false

[23] See: https://www.coe.int/en/web/freedom-expression/msi-joq

MSI-JOQ was preceded in the period 2016-2017 by the activities of the Committee of experts on Media Pluralism and Transparency of Media Ownership (MSI-MED).[24] Among the subjects examined by MSI-MED were the transparency of media ownership and the use of the Internet in elections. In its response to the recommendations from the committee of experts, the Committee of the Ministers of the Council of Europe emphasized the importance of the existing standards for media pluralism and transparency; they also called upon the Member States to regularly assess this framework (CM/Rec(2018)1).[25]

Disinformation and digital security

In resolution 2217 (2018), PACE also warned of a new 'risk of hybrid warfare' making use of cyberattacks, mass disinformation, interference in elections and disruption of communication networks. According to PACE, this new threat must and can be tackled within the realms of national criminal law. There are also relevant international standards with regard to cybercrime and terrorism.[26]

Privacy

In 2018, the Council of Europe modernised the Personal Data Protection Convention 108[27] , which dates back to 1981 and forms the foundations for European privacy protection. It was and still is the first binding international instrument that protects the individual against abuse in the collection and processing of personal data. The process of modernisation has placed privacy challenges in the light of the latest information and communication technology, and has reinforced the possibilities open to the Council for monitoring compliance with the convention.[28]

[24] See: https://www.coe.int/en/web/freedom-expression/committee-of-experts-on-media-pluralism-and- transparency-of-media-ownership-msi-med-

[25] See: https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2018-2-of-the-committee-of-ministers-to-member-states-on-the-roles-and-responsibilities-of-internet-intermediaries?inheritRedirect=false

[26] See: http://assembly.coe.int/nw/xml/News/News-View-EN.asp?newsid=7059&lang=2&cat=8 and 'Legal challenges related to hybrid war and human rights obligations' http://assembly.coe.int/nw/xml/XRef/Xref- XML2HTML-en.asp?fileid=24762&lang=en

[27] See: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

[28] See: https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet

Table 4 Overview of developments in European fundamental rights in outline (1 January 2017 - 30 June 2018)

Who/what	Technology	Issue	Action
Parliamentary Assembly of the Council of Europe (PACE) motion	NBIC convergence and artificial intelligence; digitalisation	Broadly: impact of NBIC on human rights	Study into the possible need to broaden the scope from bioethics to NBIC ethics. Recommendations submitted by PACE
Parliamentary Assembly of the Council of Europe (PACE) motion	Hybrid warfare	Impact of disinformation and cybersecurity on society	This new threat is covered by existing laws and legal standards
Council of Europe	Response to recommendations from PACE	Broadly: impact of NBIC on human rights	Recommendations in the PACE resolution adopted
Council of Europe (Steering Committee on Media and Information Society)	Digitalisation, platforms, AI	Freedom of expression, democracy	Committee on Human Rights impact of algorithms and AI (MSI-AUT), Committee on quality of journalism in the digital age (MSI- JOQ)
Council of Europe	Digitalisation	Privacy	Modernisation of Data Protection Convention (Convention 108)

Source: Rathenau Instituut

2.3 International

The work of the Human Rights Council of the United Nations relates to compliance with the human rights conventions and examines the relationship between digitalisation and human rights. In 2014, the Human Rights Council appointed David Kaye as a Special Rapporteur in the field of the right to freedom of expression, and in 2015 Joe Cannataci as first Special Rapporteur in the field of the right to privacy.

Privacy

The UN Human Rights Council adopted three resolutions in the period 2012-2017, each with minor expansions.

1. The first resolution, L13 *The promotion, protection and enjoyment of human rights on the Internet*, was submitted on 6 July 2012.[29] This resolution reconfirmed the Universal Declaration of Human Rights for the digital age by emphasising that the rights people enjoy offline must also be protected online in the digital world.
2. A second resolution, L24, was adopted on 26 June 2014, emphasising the importance of combatting hate on the Internet.
3. In response to reports from the Special Rapporteurs[30] and the 2030 Agenda for Sustainable Development, on 5 July 2016, the UN Human Rights Council unanimously agreed to a third resolution, L20, regarding *The promotion, protection and enjoyment of human rights on the Internet*. The resolution calls for the protection of online freedom as a human right, and emphasises the importance of access to information on the Internet.[31]

Big data and health

The United Nations Educational, Scientific and Cultural Organisation (UNESCO) uses education, science, culture and communication as a means of achieving the objectives of the UN, namely: the development of universal values and the improvement of living conditions for all people in the world.[32] Under the auspices of UNESCO, the International Bioethics Committee (IBC) and the World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) published reports in 2017 on big data and health, and robotics.

In its report on big data and health, the IBC (2017) argued that governance systems for big data must be used to protect fundamental human rights, but that no such governance structure yet exists. The responsible use of data and the transparency of algorithms are crucial elements in this respect. The IBC advises international organisations:

- to create a worldwide legal framework for the use of big data in healthcare and health research;
- to develop guidelines, ethical codes and ethics committees in this field.

[29] See: http://geneva.usmission.gov/2012/07/05/internet-resolution

[30] With regard to the right to privacy (A/HRC/34/60, 2017; A/HRC/31/64, 2016) and with regard to the protection of the right to freedom of expression on the internet (A/HRC/29/32, 2015; A/HRC/32/38, 2016)

[31] Because access to information strengthens the right to education and addresses the need for digital literacy. See: http://www.osce.org/fom/250656

[32] See: https://www.unesco.nl/unesco/unesco-wereldwijd

Robotics and ethics

With its report on robotics and ethics, COMEST (2017) reported that the spread of cognitive robots[33] in society is leading to social and cultural changes, and that they could compromise security, privacy and human dignity. COMEST aims to create greater awareness and encourage a dialogue on the ethical aspects of the use of autonomous, cognitive robots in society.

Key questions are the autonomy of robots and responsibility for robots. COMEST recommends:

- the regulation of the use of robots;
- the development of ethical guidelines for both manufacturers and users of robotics;
- the integration of ethics in the design process of robotics systems; and
- greater understanding within government and organisations of the implications of robotics for the labour market.

IoT and ethics

COMEST is also preparing a report on the ethical aspects of the IoT. For this report, in collaboration with the University of Twente, a workshop entitled *Ethics of Internet of Things* was held on 14 March 2018, which examined the implications of the IoT for social interactions and the balances of power.[34]

Table 5 Summary of international developments in fundamental rights, in outline (1 January 2017 - 30 June 2018)

	Technology	Issue	Action
UN Human Rights Council	Human rights on the Internet	Specifically: human rights on the Internet	Internet resolution L20
UNESCO, IBC	Big data & health	Broadly: ethical issues	Report on big data & health
UNESCO, COMEST	Robotics	Broadly: ethics and robotisation	Report on robotics
COMEST	IoT	Broadly: ethics of IoT	Preparations for report

Source: Rathenau Instituut

[33] Cognitive robots are robotics systems with human skills such as perception, language, interaction, problem solving, creativity and learning. The most important characteristic of cognitive machines is that their actions are unpredictable. The question concerning responsibility for actions by cognitive robots is therefore of crucial importance.

[34] See: https://www.utwente.nl/en/events/!/2018/3/188486/workshop-ethics-of-internet-of-things

2.4 Conclusion

Since the publication of the report *Urgent Upgrade*, on both a national and international scale, attention for the digitalisation and public values has grown, with regard to fundamental rights and human rights. Whereas in the past discussions on digitalisation and fundamental rights focused above all on the emergence of the Internet and privacy and privacy rights, the scope of the discussions is now broader.

The same applies to the discussion of the term ‘digitalisation’. It no longer refers exclusively to the Internet and new possibilities for communication, but also to the use of digital technology such as big data and algorithms, AI, platforms and persuasive technology and robotics.

This broadening of the scope has led to a similar broadening of the societal and ethical issues under discussion. As a result, such issues as the freedom of expression, equal treatment, autonomy and the protection of democracy have been placed on the policy agenda.

The Netherlands
There has been widespread concern about digitalisation and privacy rights in the Netherlands, for a long time, focused mainly on the emergence of the Internet and new possibilities for communication. These aspects were also addressed in 2017 and 2018. A first reading of an amendment to the Constitution has been adopted, to extend the scope of article 13 to include all forms of communication.

The discussion has also broadened to include new digital technologies and as a consequence other public values. In 2017, the Ministry of the Interior and Kingdom Relations (BZK) commissioned an investigation into how big data, algorithms and AI not only affect the right to privacy but also the right to freedom, the right to equality and procedural rights. In the autumn of 2018, the Cabinet is expected to send its response to this study to the Dutch House of Representatives.

The National Parliamentary System Committee is also investigating the influence of big data and microtargeting in election campaigns on fundamental democratic values. The Ministry of the Interior and Kingdom Relations (BZK) has also called upon the Council for Public Administration (ROB) to investigate the effects of digitalisation on democracy.

International

Internationally, too, there has been ongoing attention for privacy with regard to digitalisation (in particular the Internet) in the period 2017-2018. This is for example reflected by the Internet resolutions of the UN and the modernisation of Convention 108 by the Council of Europe. Greater attention is also focused on other digital technologies such as robotics and big data. Human rights institutions are calling for attention for such issues as human dignity, autonomy (agency) and control over technology (transparency and responsibility). They are calling for greater awareness, and the development of a new legal framework and ethical guidelines.

A new item on the agenda in 2017-2018 is the focus on such technologies as AI and the effects of automated decision making. There is also attention for platforms and social media and the related societal and ethical discussions on freedom of expression, media ownership, the democratic system, the balances of power and digital security and disruptions.

Both nationally and internationally, there is still limited attention for digital technologies such as biometrics (facial recognition and emotion recognition) and virtual and augmented reality, and their impact on human rights.

3 Social actors and the public debate

With their statements in the social and political debate, citizens, civil society organisations, interest groups and the media help form the way digital technology is acquiring a position in society. They feed the political-administrative and societal discussion on digitalisation and as such can play a role in placing these questions on the policy agenda. They also ensure a broader public awareness of various issues and may even contribute to the (digital) empowerment of the individual. In this chapter, we first consider a number of key issues from the debate on digitalisation and public values in the media, since the publication of *Urgent Upgrade*. This is not a systematic news analysis; we merely refer to a number of eye-catching occurrences in this respect. We then describe the issues that have been placed on the public and political agenda by various civil society organisations.

In *Urgent Upgrade*, we saw civil society organisations paying considerable attention to privacy and digital security. This continued to be the case in 2017-2018. Civil rights organisations, for example, argued against the introduction of government policy and systems such as the new Intelligence and Security Services Act (Wiv), the Computer Crime III Act and the Risk Profiling System (SyRi), the aim of which is to identify social security fraud.

At the same time, the discussion has broadened. Civil society organisations called for more focus on big data, algorithms and AI, and the effects of profiling. They tabled such issues as control over technology and justice. The Brexit campaign, the alleged Russian involvement in the presidential elections in the United States, and the Cambridge Analytica scandal led to considerable media attention for the considerable power of tech companies. The role of platforms in the spreading of disinformation was brought forward, and question marks were placed with regard to the consequences of technology for human mental health. Nonetheless, the latter topic – disinformation and the possible addictive effects of technology – are not reflected in the issues placed by Dutch civil society organisations on the public and political agenda.

3.1 Key issues from the debate in the media

3.1.1 The Netherlands

Privacy

A hotly debated topic in the Netherlands was the bill for the modernisation of the Intelligence and Security Services Act (Wiv). On the initiative of a group of students, a petition was organised in 2017 to hold an advisory referendum on this Bill. These students, from the University of Amsterdam (UvA), succeeded in collecting sufficient signatures for this purpose at the end of 2017. Many interest groups underlined their opposition to (parts of) the bill on the grounds of privacy, and joined the opposition campaign.[35]

The start of 2018 also saw criticism of the student monitoring system Magister. According to critics, the system violates the privacy rights of pupils.[36] Following an investigation, the Dutch Data Protection Agency (AP) observed that the three large education organisations have adapted their methods of working with the student monitoring system in such a way that it now satisfies the requirements of the Personal Data Protection Act.[37]

The introduction of new EU privacy legislation, the General Data Protection Regulation (GDPR), drew much media attention. Following an introduction period of two years, from 25 May 2018 onwards, all companies were required to satisfy the provisions of the GDPR. The media focused much attention on the new rights of citizens and obligations of organisations and businesses.[38] Problems facing businesses and government bodies with regard to satisfying the requirements of the GDPR also hit the headlines. Many small sports clubs with limited numbers of volunteers and small and medium-sized enterprises were revealed as often not having their data management processes in order.[39] At the moment it actually came into effect, various Ministries also failed to satisfy the requirements.[40] The media also reported staff shortages within the Dutch Data Protection Authority itself.[41]

[35] See: https://sleepwet.nl/contact.html

[36] See for example https://www.trouw.nl/opinie/schoolsysteem-magister-is-bedreigend-opdringerig-en-ontneemt-leerlingen-hun-vrijheid~aa1a39ad/

[37] See: https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/onderwijsorganisaties-passen-werkwijze-met-leerlingvolgsysteem-aan-na-onderzoek-ap

[38] See: https://www.ad.nl/economie/dit-betekenen-de-nieuwe-privacyregels-voor-jou~ad49ee8b/

[39] See: https://www.ad.nl/binnenland/duizenden-sportclubs-niet-klaar-voor-nieuwe-privacywet~af07644d/

[40] See: https://www.rtlnieuws.nl/economie/Ministeries-schenden-massaal-de-nieuwe-privacywet-avg

[41] See: https://fd.nl/economie-politiek/1254871/onrust-bij-privacywaakhond-autoriteit-persoonsgegevens

Algorithms and AI

At the start of 2018, the robot judge hit the headlines. Disputes between clients and among others health care insurers are now heard in the e-Court for private legal matters. There was criticism of the lack of transparency: judgements were not published and the identity of the 'judges' was unknown.[42] In response to media reports, the e-Court announced that it would be speeding up the publication of the decisions and the names of the arbiters on its website. At present, the e-Court has been shut down and no further disputes can be heard.[43]

The media also reported on the possible negative consequences of algorithms and AI, such as discrimination and exclusion. *NRC Handelsblad* published a series about the role of algorithms based on its own investigations. The thesis by Marlies van Eck (2018) on 'automated chain decisions & legal protection' and the report by the Kafkabrigade foundation on escaping from 'The digital cage' (Widlak & Peeters, 2018) drew much attention.

Disinformation

Following on from the reports of alleged Russian influence on the American presidential elections, disinformation also attracted much attention in the Netherlands.[44] A series of initiatives was launched to guarantee the quality and reliability of reporting, and to improve transparency, such as the cooperation between Facebook, NU.nl and the University of Leiden.[45] Since February 2018, however, cooperation between Facebook and this university has been suspended.[46] The critical news collective DROG developed a fake news article, aimed at making citizens more resilient to disinformation.[47]

The media also investigated the use of disinformation by the media itself.[48] In July 2018, *NRC Handelsblad* reported that so-called fake accounts from Russia were actively spreading reports aimed at dividing public opinion in the Netherlands.[49]

[42] See: https://www.groene.nl/artikel/vonnis-te-koop

[43] See: https://www.trouw.nl/home/digitale-geschillendienst-e-court-zit-zonder-geschillen~a843976c/

[44] Disinformation is false, inaccurate or misleading information that is deliberately created and distributed in order to earn money or to harm a person, social group, organisation or nation.

[45] In this cooperation, Facebook granted access to NU.nl and the university to a special Facebook dashboard which grants access to articles identified by users as disinformation.

[46] See: https://www.leidschdagblad.nl/leiden-en-regio/universiteit-leiden-schort-samenwerking-met-facebook-op-over-nepnieuws

[47] See: https://www.slechtnieuws.nl/

[48] See: https://www.nrc.nl/nieuws/2017/12/08/media-nederland-citeerden-trollen-als-bron-a1584306

[49] https://www.nrc.nl/nieuws/2018/07/15/de-russische-trollen-zijn-anti-islam-en-voor-wilders-a1610155?_sp=7b4920fd-e289-4511-96a4-63a7868dae2b.1533730155032

Effects on physical and mental health
Finally, attention was focused on the effects of social media on mental health, in response to a study by Statistics Netherlands (CBS).[50] An ever growing percentage (29%) of young adults – aged between 18 and 25 – view themselves as addicted to social media. A proportion of these young people admitted to the CBS that they are less able to concentrate, sleep less well and underperform at school.[51]

The physical consequences of social media, smartphones and tablets all featured in the news. Ophthalmologists warned of the consequences of the use of monitor screens by children. According to them, the long-term and repeated use of tablets and smartphones causes near-sightedness among children.[52] Other news items referred to 'tablet neck'. The healthcare support service Zorgkompas reported that a large and growing number of young people are suffering neck and back problems. These problems are caused by poor posture from the use of smartphone and tablet, and the limited amount of outdoor play.[53]

3.1.2 International

In the international media, there was much criticism of the major tech companies from scientists, former employees and investors, as well as the media itself. The central focus of this criticism was the unequal balance of power and the responsibility of the major tech companies to do something about the negative consequences of digitalisation.
During the World Economic Forum 2017 in Davos, the need to tackle the technology monopolies was clearly emphasised. It was argued that just like the cigarette industry, these monopolies were responsible for manufacturing addictive and unhealthy products.[54] Investors in Apple called upon the company to develop software aimed at limiting the use of smartphones by children.[55] Former employees of major tech companies such as Facebook, Apple and Google launched the

[50] See: https://nos.nl/artikel/2211072-helft-12-16-jarigen-vindt-zichzelf-verslaafd-aan-sociale-media.html and https://www.nrc.nl/nieuws/2018/02/07/sociale-media-zijn-slecht-voor-gezondheid-kinderen-relaties-en-democratie-a1591341

[51] See: https://www.cbs.nl/nl-nl/nieuws/2015/47/een-op-de-zes-jongeren-zegt-verslaafd-te-zijn-aan-sociale-media

[52] See: https://www.nu.nl/gezondheid/5298404/meer-jongeren-mogelijk-bijziend-gebruik-smartphones-en-tablets.html

[53] See: https://www.ad.nl/home/dag-muisarm-hier-is-de-tabletnek~acb3aecb/

[54] See: http://www3.weforum.org/docs/FOP_Readiness_Report_2018.pdf and https://www.nesta.org.uk/blog/observations-davos-wef-2018 and https://www.nrc.nl/nieuws/2018/01/23/hoog- tijd-dat-overheden-techmonopolies-gaan-aanpakken-a1589467?utm_source=NRC&utm_medium=related&utm_campaign=related2

[55] See: https://thinkdifferentlyaboutkids.com/

Truth about Tech campaign, and founded a *Centre for humane technology* aimed at broadening awareness of the ‘dark’ side of technology, and its impact on mental health.[56] Mark Zuckerberg, CEO of Facebook, was also called to account before the American Congress and in the European Parliament, following the Cambridge Analytica data scandal[57] and the alleged influencing of the US elections.

In the spring of 2018, Apple and Google launched widely reported new functions for mapping out smartphone use, with the aim of tackling excessive use.[58] There was also attention for the emergence of facial recognition, and concerns were expressed about privacy and misuse by government. Microsoft, for example, called upon the US government to regulate the use of facial recognition (by government authorities).[59]

Finally, academics from 14 American institutes published the report *The Malicious Use of Artificial Intelligence* (Brundage et al. 2018), to warn against the malicious use of AI, and to prevent and limit such misuse. In the same vein, Tesla founder Elon Musk established OpenAI, a research institute created to ensure the safe development and application of AI.[60]

3.2 Civil society organisations

Below we provide an overview of various relevant social actors and their initiatives in 2017 and 2018. Privacy and digital security remained prominently on the agenda during this period. With regard to digital security, organisations regularly referred to the risks of interconnected devices (IoT). New subjects also emerged, such as the risks of profiling (including discrimination and exclusion) and attention for human dignity, linked to the use of algorithms, automated decision making and AI.

[56] See: http://humanetech.com and https://www.volkskrant.nl/tech/oud-werknemers-facebook-en-google-beginnen-lobby-tegen-ontwrichtend-effect-van-sociale-netwerken~a4566913/ and https://www.nrc.nl/nieuws/2018/02/07/sociale-media-zijn-slecht-voor-gezondheid-kinderen-relaties-en- democratie-a1591341 and https://www.nrc.nl/nieuws/2018/01/08/aandeelhouders-apple-bezorgd-over- smartphoneverslaving-a1587522?utm_source=NRC&utm_medium=related&utm_campaign=related2

[57] See: https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm?CMP=twt_gu

[58] Bright.NL (2018) Hebben de nieuwe opties tegen telefoonverslaving zin? 6 June 2018. See: https://www.bright.nl/trends/artikel/4224696/smartphone-verslaving-android-ios-12

[59] See: https://www.theguardian.com/technology/2018/jul/14/microsoft-facial-recognition-technology-rules- potential-for-abuse

[60] See: https://openai.com/about/

Dutch Consumers Association

The Consumers Association aims to promote the interests and rights of consumers by means of campaigns, programmes, research and information provision. Online privacy and digital security are key topics addressed by the association, which for example in May 2018 – unsuccessfully – demanded in a lawsuit that Samsung should update its telephones throughout their entire useful life.[61] The association also warned of data leaks from baby monitors[62], and had previously issued similar warnings about the doll My Friend Cayla.[63]

Following the introduction of the GDPR, the association published a report on the extent to which Dutch websites comply with the latest privacy rules. According to the association, 2 out of every 3 websites investigated were non-compliant.[64] Previously, the Consumers Association had undertaken a random sample of 20 health-related websites. Advertisements were displayed without obtaining permission from site visitors. Partly in response to the efforts of the association and the Netherlands Authority for Consumers and Markets (ACM), this situation has since changed.[65]

ECP Platform for the information society

The mission of the ECP foundation is to promote a reliable, successful digital society in the Netherlands. It is a platform with 130 members, including government authorities, telecom and ICT companies and civil society organisations such as the Consumers Association. The five priorities of ECP are aimed at 1) a reliable Internet and the use of technology in business and production processes, 2) digital security, confidence in ICT and privacy, 3) digital skills for all, 4) digitalisation in the healthcare sector,[66] and 5) awareness of the importance of digitalisation and its translation into social domains and issues.

At its 20th annual conference, the ECP presented twenty building blocks for a successful and reliable digital society.[67] New topics for the platform include AI and blockchain technology. In the course of 2018, the ECP organised a series of debates on these issues, and published a white paper (ECP, 2018). The organisation also held a series of meetings about blockchain, and was the initiator of the Dutch Blockchain Coalition', aimed at promoting the rollout of this technology in the Netherlands. [68]

[61] See: https://www.consumentenbond.nl/nieuws/2018/teleurstellende-uitspraak-in-rechtszaak-tegen-samsung

[62] See: https://www.consumentenbond.nl/nieuws/2018/tienduizenden-foscam-camera%E2%80%99s-lek-direct-updaten-nodig

[63] See: https://www.consumentenbond.nl/nieuws/2016/pratende-pop-cayla-slecht-beveiligd

[64] See: https://www.consumentenbond.nl/nieuws/2018/2-van-de-3-websites-overtreden-nieuwe-privacywet

[65] See: https://www.consumentenbond.nl/nieuws/2017/twee-op-de-drie-websites-overtreden-cookiewet

[66] ECP took the initiative to establish a coalition in the field of digital competences for healthcare workers. The coalition works according to the idea that digital skills must be of a good standard in all areas of the healthcare system in order to make serious use of eHealth. See: https://digivaardigindezorg.nl/

[67] See the 20 building blocks: https://ecp.nl/20bouwstenen/

[68] See See: https://www.dutchdigitaldelta.nl/blockchain

Cultural organisations

Within the cultural domain, during workshops, lectures and exhibitions, various organisations such as Medialab SETUP, the Waag Society and V2_ considered the various aspects of digitalisation. In that way, they contributed to the strengthening of digital skills among the general public.

Medialab SETUP focused much attention on algorithms, for example by setting up the Algorithmic Historical Museum during the Dutch Design Week 2017. At this event, algorithms were placed in a historical context to encourage visitors to adopt a critical view on modern algorithms. In 2018, SETUP switched its attention to automatic decision making by algorithms, in the programme 'Weapons of Math Retaliation'.[69] Within this programme, as well as considering the themes big data and AI, attention was focused on the use of facial recognition (for example during job interviews).

The aim of the Waag Society is to ensure open and fair technology that is all inclusive. In 2017 and 2018, big data, algorithms and the IoT became important areas for attention. Part of the research programme for 2018 is aimed at the inclusion of ethics in technology (accountability), the term digital identity and the input by individual citizens in smart cities.

At V2_, an institute for the arts and media technology, big data, algorithms and profiling also enjoyed considerable attention in 2017 and 2018. One of the initiatives in 2017 was 'The Black Box Concerns', about the lack of transparency in smart algorithms. V2_ will continue to focus on this topic in 2018 (V2 2018).

Civil rights organisations

The Netherlands has a number of civil rights organisations including Bits of Freedom, Privacy First and Vrijbit, whose aims include promoting online privacy and access to information. In the period 2017-2018, their campaigns were directed in particular against the introduction of the Intelligence and Security Services Act (Wiv) and the Cybercrime III Act. A number of organisations also joined forces in a lawsuit against the Dutch State on the so-called System Risk Indication System, SyRi. The purpose of this system is to trace social security fraud, by combining a series of database files from a number of different bodies (such as municipal authorities, the employee insurance agency UWV, the Social Insurance Bank SVB, the Inspectorate SZW and the Tax and Customs Administration). The system analyses the data and generates risk notices on suspicious individuals or companies. The various bodies then undertake further investigation into the system notice (Parliamentary Papers 2016-2017, 26643 and 32761, no. 426).

[69] See: https://www.setup.nl/magazine/2018/01/civil-weapons-math-retaliation

The issues tabled by these organisations not only related to the collection of personal data but above all the new techniques for analysing data and profiling groups of people. They demanded greater attention for such issues as retaining autonomy, control over technology, justice, human dignity and the balances of power.

The **Bits of Freedom** foundation is a digital civil rights movement that since 1999 has been concentrating on the protection of freedom (of communication) and privacy on the Internet. It relies on campaigns, lobbies, lawsuits and the development of tools. One of its best-known campaigns is the annual presentation of the Big Brother Awards. In 2017, the Cabinet received one such award, for its Intelligence and Security Services Act (Wiv). During 2017, the foundation organised an active campaign against this Act, and against the Cybercrime III Act.

Bits of Freedom was also active in promoting the use of encryption and net neutrality.[70] In May 2017, Bits of Freedom called upon the Authority for Consumers and Markets (ACM) to enforce compliance with net neutrality rules through targeted actions, with a view to protecting the freedom of Internet users. The foundation also regularly organised Privacy Cafes, during which people were informed about secure and free Internet use. *My Data Done Right*, developed by Bits of Freedom, is an open source tool that enables individual citizens to demand greater transparency from parties using their data.

The **Privacy First** foundation was established in 2008 as an independent foundation aimed at maintaining and promoting the right to privacy. Privacy First works to tackle privacy violations via political lobbying, publicity campaigns and legal actions and lawsuits. It also organises the annual ‘Privacy Awards’ for Dutch organisations that operate a positive privacy policy. Key subjects are privacy and the security services (campaign against the Wiv), big data and profiling, privacy, autonomy and mobility in the public domain. In 2017 and 2018, a new topic was added, namely children and privacy (aimed at the broader use of digital learning environments in education), and the financial sector in relation to privacy. In connection with this particular issue, Privacy First joined the Volksbank in 2018 in developing a label for the banking and fintech sector, in advance of the new European Directive for payment services (the *Payment Services (PSD2) Directive*).[71]

[70] Net neutrality is the principle according to which Internet providers treat all data equally, without discriminating on the basis of user, content, website, type of application, etc. See: https://www.bof.nl/dossiers/netneutraliteit/

[71] Interview with Privacy First, 7 May 2018.

One important tool used by the foundation is legal proceedings, initiated in 2017-2018 among others against SyRi, automatic number plate recognition (ANPR) and number plate parking. The ANPR Bill was adopted by the Dutch Senate on 21 November 2017. According to the Bill, the police are permitted to record and store number plate details (such as the number plate, location, time and photograph of the vehicle) for a period of four weeks.[72] In June 2017, Privacy First filed a lawsuit about number plate parking, arguing that there is no legal basis for such a system, which means that citizens are no longer able to park anonymously. In October 2017, the court rejected the case. Privacy First has appealed against this decision.[73]

Civil rights organisation **Vrijbit** is active in safeguarding the right to privacy, freedom of communication and access to information. Just like other civil rights organisations, in 2017 and 2018, Vrijbit opposed the Wiv Act. To demonstrate that this Act negatively influenced the right to protection of private life and the physical integrity of Dutch people, Vrijbit sent a letter among others to the High Commissioner for Human Rights at the UN.[74]

Vrijbit also organised a series of legal actions. They called for an amendment to the Passport Act with the aim to preventing the further use of biometric personal data for the issuing of passports and ID card documents. Following the partial upholding of their complaint by the Council of State, the organisation is currently continuing its campaign before the European Court of Human Rights.[75] Vrijbit also successfully filed several lawsuits against the Dutch Personal Data Protection Authority (AP). According to Vrijbit, the AP has been inadequate in tackling the unlawful use of medical personal data.[76]

[72] See: https://www.privacyfirst.nl/rechtszaken-1/item/1097-privacy-first-begint-rechtszaak-tegen-wetsvoorstel-anpr.html

[73] See: https://www.privacyfirst.nl/rechtszaken-1/kentekenparkeren/item/1077-nieuwe-rechtszaak-over-anoniem-parkeren-met-contant-geld.html

[74] See: https://www.vrijbit.nl/dossiers/dossier-wet-en-regelgeving/item/1065-vrijbit-brief-aan-de-hoge-commissaris-van-de-mensenrechten-van-de-vn.html

[75] See: https://www.vrijbit.nl/dossiers/dossier-paspoortwet/item/1085-vingerafdrukken-weg-uit-paspoort-wachten-op-uitspraak-ehrm-of-wil-de-nieuwe-paspoort-piet-in-de-tweede-kamer-opstaan.html

[76] See the lawsuit on the use of a code of conduct that was declared unlawful by the court, the lawsuit on the failure of the AP to respond to the use of the Diagnosis Information System (DIS) by the Dutch Healthcare Authority, and legal proceedings aimed at forcing the AP to act against actions by the manager of the EPD-LSP system: https://www.vrijbit.nl/dossiers/dossier-gezondheidszorg/item/1058-persbericht- vrijdagmiddag-10-maart-dienen-in-utrecht-2-rechtszaken-over-onrechtmatig-verzamelen-en-verwerken-van-ieders-medische-gegevens-door-de-zorgverzekeraars-en-nederlandse-zorg-autorit and https://www.privacybarometer.nl/nieuws/3909/Rechter_geeft_Autoriteit_Persoonsgegevens_er_van_langs

On 27 March 2018, a **group of civil society organisations**, including Privacy First, the Netherlands Commission of Jurists for Human Rights[77], the Platform for the Protection of Civil Rights[78] and the National Clients Council, filed a lawsuit against the Dutch State on the fraud investigation system SyRi.[79] According to this coalition, the risk profiling system represents a threat to the democratic rule of law. In the view of the coalition, it is unclear to citizens which data the system uses, which analyses are undertaken and what elements make the system a risk. A series of requests for information referring to the Government Information (Public Access) Act (WOB) provided the organisations with little information. According to the Ministry of Social Affairs and Employment, if the information and risk models used were to be released, calculating citizens would be able to work out what to look out for, in committing fraud (SZW, 2018). According to the plaintiff, this refusal is in contravention among others of the duty of information and the right to a fair trial.

Amnesty International Nederland fights for human rights. Since 2017, the organisation has also been investigating the use of algorithms and AI, for example by the police, and the risk to human rights that this use represents (see also section 3.4). Amnesty believes that further discussion is needed about how the government uses AI. Amnesty is for example concerned about the bias in algorithms, and the lack of transparency about what systems do.[80]

[77] The Netherlands Commission of Jurists for Human Rights (NJCM) works to protect human rights in the Netherlands and Dutch foreign policy. The Commission focused its attention on the Wiv Act, the Cybercrime III Act and the amendment to Article 13 of the Dutch Constitution.

[78] The Platform for the Protection of Civil Rights is a network of organisations, groups and individuals whose aim is to improve the safeguarding and strengthening of civil rights in the Netherlands. Themes include biometrics in passports, privacy in healthcare, and profiling.

[79] SyRI is a government system that combines personal data of citizens with the aim of investigating fraud, abuse and violations. It is an elaboration of the SUWI Act (Structure of organisations implementing the Act on Work and Income) that was adopted in 2013.

[80] See: https://www.rathenau.nl/nl/digitale-samenleving/amnesty-international-algorithmes-moeten-zich-aan-de-mensenrechten-houden

Table 6 Overview of developments at civil society organisations, in outline (1 January 2017 - 30 June 2018)

Who/what	Technology	Issue	Action
Consumers Association	Internet, apps, consumer electronics, IoT	Privacy, digital security	Campaign on privacy awareness. Lawsuit on security updates, medical data storage and privacy
ECP	Digitalisation Blockchain, AI	Digital security, privacy, inclusivity	E.g. programmes for digital skills and security, blockchain, working group on AI code of conduct
Cultural organisations			
SETUP	Algorithms, AI, facial recognition	Control of technology, justice	Algorithmic Historical Museum, Weapons of Math Retaliation
De Waag Society	Big data, IoT algorithms	Privacy, autonomy, control over technology, human dignity, balances of power	E.g. Digital Identity Lab, Waag Makerbox
V2_	AI, digital platforms, big data, algorithms and profiling	Human dignity, privacy, autonomy	E.g. The Black Box Concerns, Test_Lab, 3x3
Civil rights organisations			
Bits of Freedom	Internet, digital communication	Privacy, digital security, freedom of communication	Big Brother Awards, privacy coalition, Internet freedom toolbox, Wiv 2017, Cybercrime III, net neutrality, My Data Done Right
Privacy First	Digital communication, digital government	Privacy, *big data*, profiling	Legal actions on storage of telecom data, SyRI risk profiling, ANPR Label for financial services
Civil rights association Vrijbit	Internet, digital government	Privacy, free communication and access to information, human rights	Wiv 2017, Passport Act, unlawful collection of medical data
Amnesty International Nederland	Algorithms, AI	Control of technology, justice, human rights	Risks from the use of algorithms for human rights, e.g. by the police

Source: Rathenau Instituut

3.3 Umbrella organisations for businesses and employees

Below we discuss various professional umbrella organisations representing businesses, programmers and professionals. In 2017-2018, these organisations focused their attention on privacy and digital security, for example with regard to future and recently introduced European legislation, such as the General Data Protection Regulation (GDPR), the ePrivacy Regulation (this proposal contains specific privacy regulations for the electronic communication sector that for example should apply to new platforms such as Whatsapp, Facebook Messenger and Skype) and the Cyber Security Act (see also chapter 5). The umbrella organisations also considered AI and the future of employment. A cautious start was made on the discussion about ethics and fundamental rights, for example within Nederland ICT and within the professional association for information professionals KNVI.

The employers' organisation **VNO-NCW** promotes the interests of Dutch business. In the field of digitalisation, in 2017 and 2018, the organisation focused its attention on privacy and digital security.[81] Together with **MKB-Nederland**, VNO-NCW developed the Privacy Quick Scan.[82] During this period, both organisations were involved in providing information and preparing the private sector for the new privacy legislation (GDPR). Earlier, towards the end of 2016, a campaign was launched against cybercrime, including the project Secure Business Internet. This project enabled businesses to test the security of their digital environment.[83]

Nederland ICT is an interest group and representative of the Dutch ICT sector. Its activities are focused on privacy, security (trust) and digital skills, among others in preparing for the GDPR, with its GDPR Helpdesk and GDPR Toolkit. In the period 2017-2018, ethics was a new topic on the organisation's agenda.

One of the spearheads of the **Trade Union Federation for Professionals (VCP)** is AI, because of the huge influence of this technology on developments in the labour market. The VCP believes that professionals must be able to keep working on their development, and is trying to generate greater awareness of the consequences of AI for the distribution of work and income.[84]

The **FME**, the Dutch employers' organisation in the technology industry, commissioned the consultancy firm Berenschot and Tilburg University to investigate

[81] https://www.vno-ncw.nl/standpunten/privacy
[82] https://www.vno-ncw.nl/standpunten/privacy
[83] See: https://www.vno-ncw.nl/projects/veilig-zakelijk-internetten
[84] At the end of 2016, the VCP symposium focused on the theme AI.

the influence of technological developments on employment in the technological industry (including robotisation and IoT). More than 6,900 employees were involved in this study. The resultant report entitled *Onderzoek Smart Working* [Smart Working Survey] (Hos et al. 2018) discusses how jobs and tasks are changing in the industry.[85] The majority of the employees interviewed believe that digitalisation will not result in jobs disappearing, but will in fact create new, and different, jobs. The report suggests that new technology calls for other skills and knowledge, making lifelong learning even more important. The majority of interviewed employees felt responsible for keeping up to date, and expressed the wish to keep up with the developments.

The Dutch professional organisation for information and IT professionals **KNVI** is an independent platform for the development and exchange of professional knowledge and the broadening of the network of its members. Each year, the organisation addresses a specific topic. The topic for 2018 was *Smart Humanity*, with reference to the continuing central position of humans. The title refers to the people who work with new digital technology, but also expresses the aim of ensuring that society maintains an ethically responsible approach to technology.

The KNVI also plays a role in placing knowledge and training on the agenda, and makes a substantive contribution to its implementation.[86] The KNVI feels that IT professionals have a crucial role to play in making sure the process of digitalisation remains on the right track, and in identifying and pointing out emerging threats to fundamental rights .[87] With that in mind, this year, the association plans to initiate a dialogue on this issue with the private sector, the scientific community and politicians.

The **Wetenschappelijk Bureau voor de Vakbeweging – De Burcht (the Trade Union Research Association)** published a report in 2018 entitled *Samen werken met robots* [Cooperating with robots]. The study discusses the consequences of automation, digitalisation and robotics for jobs, employees and the changing role of trade unions (Freese & Dekker, 2018).

In a test court case against the company Uber in 2017, the **Dutch Trade Union Federation (FNV)** argued that Uber promotes unfair competition against other taxi drivers, and the judge ruled in that Uber drivers are not sole traders.[88] Taxi drivers in Spain had previously joined forces against the company.[89] This led to a lawsuit

[85] See: https://www.fme.nl/nl/nieuws/medewerkers-industrie-laat-robots-komen
[86] See: https://www.knvi.nl/persbericht-smart-humanity/
[87] See: https://www.rathenau.nl/nl/digitale-samenleving/knvi-geef-iters-de-ruimte-om-schending-grondrechten-te-benoemen
[88] See: https://www.parool.nl/amsterdam/fnv-wil-zaak-tegen-uber-starten-maar-chauffeurs-durven-niet~a4542336/
[89] See: https://www.politico.eu/article/tito-alvarez-uber-battle-ecj-decision/ and https://www.politico.eu/article/uber- ecj-ruling/

culminating in a ruling by the Court of Justice of the European Union on 20 December 2017 whereby the service offered by Uber via an app is deemed a transport service as intended in EU law, and not a (digital) service (Court of Justice of the European Union 2017).[90] As a result, EU Member States are authorised to determine nationally the conditions according to which the service may be provided.[91]

Table 7 Overview of developments at umbrella organisations for businesses and employees, in outline (1 January 2017 - 30 June 2018)

Who/what	Technology	Issue	Action
OECD guidelines on corporate social responsibility	Specific case by case	Specific case by case	Businesses have a duty of care to respect human rights
VNO-NCW / MKB-Nederland	Digitalisation	Privacy, digital security	Project Safe Business Internet
Nederland ICT	Digitalisation	Privacy, digital security, ethics	GDPR Helpdesk, GDPR Toolkit
VCP	AI	Labour market, human dignity	Influence of AI on the distribution of work and income
KNVI	Digitalisation	Digital skills, ethics and fundamental rights	Focus on Smart Humanity
De Burcht	Robotics	Labour market	Consequences of digitalisation, automation and robotics for jobs, employees and the role of trade unions
FME	Digitalisation	Labour market	Digitalisation leads to new and other jobs
FNV	Platform and sharing economy	Balances of power	Test case against Uber
Spanish taxi drivers	Platform and sharing economy, location and telecom data	Private life, democratic values	Judgement that Uber is a taxi company and not a tech company

Source: Rathenau Instituut

[90] See: Article 58 TFEU: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

[91] See: questions by MP Gijs van Dijk (PvdA) to the Ministers on the judgement by the European Court of Justice that Uber is a taxi company (submitted 8 January 2018): https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2018D04785&did=2018D04785

3.4 International developments

Civil society organisations are encouraging lively international debate on the ethics of digitalisation, in particular with regard to human rights and AI. **Privacy International**, a non-profit- and non-governmental organisation, joined civil rights organisation **Article 19** in publishing a report in April 2018 that underlines the risks of AI for the right to freedom of expression and the right to privacy (Privacy International & Article 19, 2018).

According to this report, government policy should serve to protect human rights; to guarantee responsibility and transparency with respect to AI, and to encourage government authorities to review the adequacy of legal and policy frameworks.

The **European Digital Rights Initiative (EDRi)**, an association of civil rights and human rights organisations whose goal is to protect rights and freedoms in the digital age, is active in the field of privacy, the use of biometrics in means of identification, disinformation, digital security and control of technology.

In 2017, **Amnesty International** launched an *Artificial Intelligence and Human Rights Initiative* aimed at formulating human rights principles for AI and promoting a discussion of the ethics of AI.[92] Amnesty also launched a campaign against the development of killer robots,[93] and has now started to consider how AI can be used to help solve global challenges in respect of human rights.

Key subjects of discussion by the Bureau of European Consumers Associations **BEUC** include digital consumer rights, for example in the domain of privacy and security online and the IoT, net neutrality and geoblocking.[94] A new topic for the BEUC is AI. In June 2018, the organisation published its position paper on automated data processing and AI (BEUC 2018a). Among others, it calls for an *AI Consumer Action Plan*, in which the European Commission will investigate whether and where existing legal frameworks need to be adjusted, in order to offer better consumer protection.[95]

The BEUC also generated input for the proposals from the European Commission for modernising consumer rights in Europe (BEUC 2018b). The BEUC believes that new consumer rights are needed with regard to IoT, AI and algorithms.

[92] See: https://www.amnesty.org/en/latest/news/2017/06/artificial-intelligence-for-good/

[93] See: https://www.stopkillerrobots.org

[94] When geoblocking is used, online customers are not granted access to the services or products via a website in another EU Member State.

[95] The organisation also believes that more possibilities must be created for granting consumers an insight into the automated decision making processes and voicing their objections, and that there must be greater clarity on the liability of companies that use automated decision making processes.

For example, there is a clear need for collective procedures for consumer compensation. The BEUC also proposed changes in the field of information provision (about how algorithms work) and how information and prices are ranked and presented to consumers) and in the field of liability (BEUC 2018a).

The BEUC also published its comments on the Cybersecurity Act. It called for greater attention for IoT and the security of associated products and services. According to the BEUC, consumers must compulsorily be offered security *by design* (BEUC 2018c). According to the BEUC, the minimum binding requirements should be: compulsory software updates, and compulsory use of strong authentication mechanisms and encryption.

Finally, together with the international organisation for consumer groups **Consumers International**, among others, the BEUC published principles aimed at making privacy, safety and security the most important characteristics of the IoT.[96]

Since 2017, the international organisation for technical professionals **IEEE** has been investigating the attitudes of parents to interaction between children and intelligent systems.[97] With its initiative *Ethics in Action*, the organisation aims to support developers of autonomous systems in making ethically responsible choices and developing the relevant ethical guidelines.[98] At the end of December 2017, a second version of these ethical guidelines for autonomous and intelligent systems was published. In 2018, feedback on these guidelines will be collected.

[96] See: https://www.consumersinternational.org/media/154809/iot-principles_v2.pdf

[97] See: https://www.ieee.org/about/news/2017/ieee-unveils-generation-ai.html

[98] See: https://ethicsinaction.ieee.org

Table 8 Overview of developments at international organisations, in outline (1 January 2017 - 30 June 2018)

Who/what	Technology	Issue	Action
EDRi (EU)	Internet, AI	Human rights online, freedom of expression	Privacy, biometrics in identification, disinformation, digital security
Privacy International	Internet, AI	Privacy, freedom of expression	Policy must protect human rights and ensure transparency and responsibility with regard to AI
Amnesty International	AI, robotisation	Human rights	- Formulating human rights principles for AI - Campaign against killer robots
BEUC and Consumers International	Digitalisation, IoT, AI	Privacy, cybersecurity, consumer rights, control over technology	- AI Consumer Action Plan - Privacy and security - Principles for the IoT
IEEE (int.)	AI, algorithms, robotics	Ethics of autonomous systems	- Initiative for assisting designers of autonomous systems to make ethical choices - Children and AI

Source: Rathenau Instituut

3.5 Conclusion

Much attention for privacy and digital security

In the period 2017-2018, Dutch civil society organisations focused considerable attention on privacy issues and digital security. Civil rights organisations focused on campaigns and lawsuits against Dutch government policy, such as the introduction of the new Intelligence and Security Services Act (Wiv), the Cybercrime III Act and digital government systems such as SyRi and ANPR (automated number plate registration). The organisations not only demanded attention for data collection but also for new techniques for analysing data and profiling people, and the possible associated risks.

In that respect, profiling affects such issues as autonomy, control over technology, justice and human dignity. The Consumer Association particularly placed online privacy on the agenda, together with the security of devices connected to the IoT.

AI and human rights as a new topic

With the emergence of big data, algorithms and AI, attention is also growing for the significance of these technologies for human rights. Various organisations have identified AI and human rights as new topics within their organisation, including Amnesty International, medialab SETUP and the European consumer organisation BEUC. In comparison with the report *Urgent Upgrade*, such topics as control of technology, human dignity and justice are far more clearly present on the agenda of civil society organisations. Also among umbrella organisations for the private sector, attention for this theme has grown cautiously.

Not on the agenda

Whereas the agenda focused considerable attention on the power of platforms, social media and disinformation and the protection of democratic systems, as well as such issues as persuasive technology in social media and apps and their effects on human mental health, these themes are not reflected on the agendas of the Dutch civil society organisations. We have also seen very little evidence of emerging discussion about virtual and augmented reality. With the exception of attention for biometric applications in passports, there is relatively little attention for biometric developments, while developments in particular in respect of the use of facial recognition are taking place extremely rapidly. Finally, on the national agenda, robotics occupies a far less prominent position.

4 Politics and administration: agenda setting

Within the politic-administrative domain, we discuss the publications of the various national advisory councils and institutes that have identified the societal and ethical aspects of digitalisation, and placed them on the policy agenda. Subsequently, we discuss a number of international advisory organisations entrusted with the task of mapping out the ethical and societal issues regarding digitalisation.

To improve readability, in this chapter we also discuss Cabinet responses to various recommendations. These are then revisited briefly in chapter 5.

Since *Urgent Upgrade,* more and more advisory boards have been calling for attention for the significance of digitalisation for society. These reports emphasise that a variety of public values are compromised by digitalisation. In 2017, a number of the recommendations related above all to the consequences of digitalisation as a whole. In 2018, these were joined by recommendations calling for attention for specific sectors such as power supply, mobility, healthcare and the media, and for specific fields of technology such as AI and digital security. On a European scale, the various advisory boards have above all called for attention for AI.

4.1 The Netherlands

The Netherlands Scientific Council for Government Policy (WRR)
The Netherlands Scientific Council for Government Policy is an independent advisory body for government policy. The task of the WRR is ‘to provide scientific-based information on developments that could influence society in the longer term’ (WRR,1976).

In June 2018, the Cabinet called upon the WRR to investigate the impact of AI on public values (Parliamentary Papers, 2017-2018, 26 643, no. 529). Also in 2018, the WRR launched a project on so-called digital disruption (large-scale disruption of the digital infrastructure).

Previously, in 2017, the WRR published the report *Weten is nog geen doen. Een realistisch perspectief op redzaamheid* [Knowing is not the same as acting. A realistic perspective on self-reliance]. In this report, as a counterpoint to ‘thinking capacity’, the Council introduced the term ‘acting capacity’ of citizens, described as the capacity to take action in a given situation. This includes digital literacy. The

WRR concluded that considerable demands are imposed on this acting capacity when people are called upon to take more personal responsibility in what has been described in the Netherlands as the ‘participation society’. According to the Council, there are major differences between what is expected of citizens, and what they are actually capable of. The WRR recommends that policy be based on a *realistic* perspective of the thinking and acting capacity of citizens. When preparing policy, this can be achieved by assessing whether account has been taken of differences in acting capacity, and in policy implementation by establishing personal contact with citizens at an early stage, to offer support (WRR, 2017, p. 14-15).

In the Cabinet response to *Weten is nog geen doen* in 2018, the Cabinet supported the recommendations from the WRR (Parliamentary Papers II 2017-2018, 34775, no. 88), arguing for example that government should offer information that ties in with different levels of cognitive capacity and acting capacity[99]. The Cabinet also undertook to introduce an acting capacity test for all new policy setting, by incorporating it in the already existing Implementation and Enforcement test. The Cabinet will also strengthen the behavioural knowledge of the various Ministries by consulting the Behavioural Insights Network Nederland (BIN NL) of the departments. The BIN NL is a joint venture between all Ministries aimed at applying behaviour-based insight in policy, implementation, supervision and communication. Finally, the Cabinet announced that in 2018, the Research and Documentation Centre (WODC) of the Ministry of Justice and Security would be launching a study into the Legal aspects of algorithms capable of autonomous decision making (*Juridische aspecten van algoritmen die zelfstandig besluiten nemen*). This study will investigate the opportunities offered by AI for the timely identification of people who due to circumstances beyond their control are not self-reliant, with a view to offering those people better assistance at an earlier stage (Parliamentary Papers II 2017-2018, 34775-VI, no. 88).

Council for Culture

The Council for Culture is a body established to advise the Dutch government and parliament on the arts, culture and media. In February 2018, the Council published the sector recommendation *Audio Visual* [*Zicht op veel meer*] (Council for Culture, 2018). This report contained recommendations for making the Dutch audio-visual sector futureproof. Due to changes in the media landscape and the influx of major international players, Dutch products are increasingly having to complete with super platforms such as Netflix and YouTube.

[99] On behalf of the Ministry of the Interior and Kingdom Relations, TNO carried out the study *Inclusief iedereen* [Including everyone] which examined the possibility of providing better services to groups who express a strong preference for telephone or personal contact due to a physical or cognitive disability or a lack of knowledge and experience, and who find it difficult to make use of information and communication technology.

These platforms are squeezing out Dutch programme providers and reducing their outreach. As a result, essential public values, such as the telling of stories that build the Netherlands and represent the Dutch identity are under threat. The Council emphasises the importance of cooperation with these super platforms in order to respond effectively to the technological developments in the media domain.

At the same time, public financing for public broadcasters and the film sector has slumped considerably. The Council therefore called for additional investments in the audio-visual sector. Its recommendations include introducing charges for all end users of paid and free offline and online visual services – major foreign distribution platforms such as cinema chains, cable companies and paid and super platforms, that make little or no contribution to the financing of Dutch products – and turning what is today the Film Fund (Filmfonds) into a broad-based audio-visual fund. According to the Council it is also important to avoid too much money disappearing from the sector into large commercial companies that do not take any responsibility for telling Dutch stories.

Finally, the Council recommended further encouraging media literacy and film education, and strengthening cultural audio-visual products by investing in talent development and encouraging high-quality content (Council for Culture, 2018).

Council for the Environment and Infrastructure
The Council for the Environment and Infrastructure (Rli) advises the government and parliament on policy issues relating to sustainable development of the physical environment and infrastructure.

With its publication *Technologie op waarde schatten – een handreiking* [Assessing the value of technology – a handout] (Rli, 2017), the Rli addressed the complex effects of technological developments on our society and living environment, and provided guidelines on how to deal with technological developments.[100]
In this report, the RLi identifies management priorities for all stakeholders, including the broadening of knowledge and understanding of technological innovation by encouraging various parties to work together and share knowledge and work towards shared objectives. The Council recommends that the government adopts a prominent role in protecting public values. According to the Council, the use of technology also calls for the (re)definition of relationships between government, businesses, civil society organisations and citizens, and the establishment of new relationships. According to the Council, these changing relationships engender three vulnerabilities, namely the availability of vital infrastructures, access to technology – i.e. the skills of users – and the controllability of technology (specific algorithms).

[100] The report follows up on a previous report *Survey of technological innovations in the living environment* (Rli, 2015)

Finally, the Council calls for broad-based social debate about the choices that governments, businesses and citizens are required to make in the light of these technological developments (Rli, 2017).

In its recommendation *Stroomvoorziening onder digitale planning* [Electricity supply in the face of ongoing digitalisation] (Rli 2018), the Rli analyses the vulnerability of the power system as a result of the ongoing process of digitalisation. This relates not only to the threat of cybercrime but also to the possible consequences of software design errors and unforeseen behaviour by autonomous systems that to an ever increasing extent will be responsible for regulating the power supply. According to the Rli, these vulnerabilities create new risks for the reliability of the electricity supply. The Rli advises the government to recognise and investigate the possible consequences for the reliability of the electricity supply, and to take 'no-regret' measures to limit this digital vulnerability.[101] According to the Rli, the government should also invest in an infrastructure for shared knowledge gathering and seek cooperation at European level in order to tackle the vulnerability inherent in the digitalised electricity supply (Rli, 2018).

Netherlands Institute for Social Research (SCP)

The Netherlands Institute for Social Research (SCP) is a government agency that conducts research into the social aspects of government policy. Formally it reports to the Ministry of Health, Welfare and Sport (VWS). The SCP for example monitors the life situation and quality of life in the Netherlands, evaluates government policy and assesses society with a view to future policy.

In 2017, the SCP published its biannual report on the social state of the Netherlands, which included an assessment of the digital self-reliance of Dutch citizens. This capacity is subject to ever greater demands, for example due to technological developments and the flexibilisation of the labour market. However, there are large groups of people – for example those with limited literacy skills or people with a (mild) mental impairment – for whom digital self-reliance is difficult or even impossible. The information society appears to be ignoring these people, and thereby creating a digital chasm. As a result, according to the SCP, it is essential that society makes every possible effort to ensure that as many citizens as possible participate fully. This can for example be achieved by assisting them in acquiring the necessary (digital) skills. The SCP refers among others to the WRR report (2017) on what is described as the acting capacity of individuals (SCP, 2017).

[101] For example by taking preventive measures and guaranteeing that current insights into the safe design and updating of digital systems are laid down in standards.

Netherlands Bureau for Economic Policy Analysis (CBP)

The Netherlands Bureau for Economic Policy Analysis (CPB) carries out economic policy analysis. It is part of the Ministry of Economic Affairs and Climate Policy.

In 2018, in its report *CPB Risk Report on the Financial Markets 2018*, the CPB called for ‘cyber stress tests’ at banks, to assess the digital security of the banking system. According to the CBP, active supervision of IT systems by De Nederlandsche Bank (DNB) and the Authority for Financial Markets (AFM) is crucial. Together with its partners, the DNB is already hard at work organising cybersecurity tests.

In 2017, the CBP published another report, *Scientia potentia est: the emergence of brokers for everything* (CPB, 2017). In this report, the CPB warned about the negative consequences of digital platforms (search engines, social platforms and online marketplaces such as Google, Facebook, and Amazon). In particular, the bureau referred to the risk of platform companies abusing their information position. The CPB also referred to the risk of insufficient stimuli for platform companies to deal with undesirable behaviour by their users, such as the spreading of disinformation. The CPB wrote that the government is in a position to take measures to restrict the risks of platforms by increasing the transparency and liability of these platforms. The government must however on the one hand take account of the freedom of expression and on the other space for innovation. The CPB called for a system of licences for platforms, so that regulators can maintain some control over the parties active on those platforms. Other proposals from the CBP included forcing platforms to mark or filter harmful information and to make it clear when information originates from political parties (CPB, 2017).

In its response to the report *Scientia potentia est*, the Cabinet supported the risk of Internet platforms as identified by the CPB (Parliamentary Papers II, 2017-2018, 33009, no. 48). The Cabinet expressed its recognition of the importance of the space for platforms referred to in the report, that enables those platforms to continue innovative development. The Cabinet argued that tools are already available for dealing with the risks, in existing legislation and regulations, and referred to the desire to maintain good quality news reporting in the Netherlands, with particular attention for disinformation and covert influencing (Parliamentary Papers II, 2017-2018, 26643, no. 508). In its response, the Cabinet further referred to the adoption of the Heerma/Mohandis motion, that calls upon the government to ‘initiate an investigation into the future of independent journalism in the Netherlands in relation to the spreading of disinformation’ (Parliamentary Papers II, 2016-2017, 34550 VIII, no. 82). Finally, the Cabinet response referred to a

National Digitalisation Strategy[102] that will focus attention on the risks, transparency and liability of platforms (Parliamentary Papers II, 2017-2018, 33009, no. 48).

Netherlands Environmental Assessment Agency (PBL)
The Netherlands Environmental Assessment Agency (PBL) is the national institute for strategic policy analysis in the fields of the environment, nature and spatial planning. Formally it reports to the Ministry of Infrastructure and the Environment (IenM), but carries out research on behalf of a variety of departments.

In the publication *Mobiliteit en elektriciteit in het digitale tijdperk. Publieke waarden onder spanning* (2017) [Mobility and electricity supply in the digital era – Public values under pressure], the PBL argues that public values are under pressure due to digitalisation of the infrastructure. Examples include equal access to public transport, transparency, guarantee of supply and delivery reliability of vital (power) services such as electricity; protection of privacy and self-determination; and democratic control (above all in respect of intelligent systems). According to the PBL, digitalisation can cause certain groups, such as the less educated and the elderly, to be excluded from services if they do not have the necessary skills or are unable to make use of the new infrastructure services.

Another risk identified by the PBL is the growth in vulnerability to disruptions and failures, above all when networks become more complex. The agency therefore argues that direction by government is important to prevent a chasm emerging between (groups of) citizens due to differences in digital literacy, or social disruption as a result of the poor manageability of vital (power) supplies. The agency also encourages government to enter into active discussion with society on core values in order to lay down clear frameworks and objectives for protecting public values. The agency refers to the necessity of proper supervision and democratic control with regard to smart city applications.

Finally, the PBL advises greater investment in digital expertise in government based on the need at government level for greater technical knowledge of the newly digitalised systems, and more knowledge of the ethical and societal impact of digitalisation on society (PBL, 2017).

In its response, the Cabinet supports the recommendations from the PBL that public values such as accessibility, delivery reliability, privacy and democratic control are threatened by the growing complexity of systems (Parliamentary Papers II 2017-2018, 29023, no. 228). However, the Cabinet does not believe

[102] Announced during the budget discussions for Economic Affairs and Climate Policy on 14 December 2017 and published since that time.

that the digital security of the vital infrastructure is at risk. On the other hand, the Cabinet recognises that digital security is of growing importance for delivery reliability. At this moment, delivery reliability is guaranteed by the 1998 Electricity Act, whereby responsibility lies with the network operator. The Cabinet has promised to examine what guarantees are needed in order to maintain the current delivery reliability of electricity, and what lessons we can learn from other countries with regard to ensuring the security of vital infrastructure in the framework of digitalisation. Furthermore, with the implementation of the Cybersecurity Act (see chapter 5), attempts are being made to improve European cooperation in the face of ICT incidents, and to strengthen the resilience of network and information systems for vital services (Parliamentary Papers II 2017-2018, 29023, no. 228).

Education Council

The Education Council of the Netherlands is an independent governmental advisory body which advises the government and the Dutch Senate and House of Representatives on the outlines of policy and legislation with regard to education. According to the Education Council, the rapid digitalisation of our society is calling for a system of education that offers space for digital educational goals, the use of digital educational resources and the use of digital applications for the organisation of education.

In its recommendation *Thoughtful digitalisation* [*Doordacht digitaal*] (2017), the Education Council advocates thoughtful educational choices to ensure that education can derive the maximum benefit from the opportunities offered by digitalisation. The Council advises government to provide further support to schools in establishing the necessary conditions for digitalisation, such as Internet security and privacy.

The Council also advocates closer involvement by the educational field in digital developments and in designing innovative applications. In the opinion of the Council, the digital expertise in the world of education must be structurally expanded. This can be achieved by allowing schools themselves to experiment with ICT. The Council also warns of the possible negative consequences of excessive use of digital applications for the memory and powers of concentration, and harmful physical and psychological consequences of excessive use of the Internet, such as 'tablet neck', cyber bullying and 'disconnection fear', the fear of missing something whenever you are offline. In conclusion, the Council emphasises that the broad deployment of ICT in education should not result in any form of threat to a secure teaching and learning environment in which students must be allowed to be vulnerable or rebellious, and able to grow without having this thrown back at them later.[103] (Education Council, 2017).

[103] For example when certain traces remain on the Internet or if digital data about individual students remain stored in the education system.

In the Cabinet response, the Ministry of Education, Culture and Science supports the recommendations in the report (Parliamentary Papers II 2016-2017, 32034, no. 22). The Ministry for example recognises the importance of a sound basic infrastructure. For that reason, together with sector organisations, the Ministry plans to maintain control of the further development of this basic infrastructure. The Ministry of Education, Culture and Science also agrees that is important to separate technology and content. With that in mind, the educational sector has agreed on certain standards for ICT facilities with the private sector and the Ministry. The Ministry of Education, Culture and Science also shares the opinion that guaranteeing privacy and security are becoming ever more important. In a previous Parliamentary Paper, the Secretary of State already explained that a series of tools have been created, such as the social media protocol, a privacy quick scan and handouts aimed at informing parents. In addition, a system of pseudonyms will be created for students using digital learning resources, the aim of which is to improve the protection of the privacy of students (Dutch House of Representatives, 2016-2017, Appendix to the Proceedings, 2075; Parliamentary Papers II 2016-2017, 32034, no. 22; Parliamentary Papers II 2016-2017, 34741, no. 2).

The Social and Economic Council of the Netherlands (SER)

The Social and Economic Council of the Netherlands advises the Dutch government and parliament on outlines of social and economic policy. In 2017, supported by the international think tank OECD, the SER and the Cabinet started developing a ‘national skills strategy.[104] In June 2017, the SER published the report *Learning and development during career* [*Leren en ontwikkelen tijdens de loopbaan*] . Together with the Rathenau Instituut, the SER also organised two working conferences on working towards a responsible digital society (Rathenau Instituut & SER, 2018).[105]

Rathenau Instituut

The Rathenau Instituut is charged with encouraging public and political debate and opinion shaping on science and technology. Over the past thirty years, the institute has mapped out the influence of automation and digitalisation on all domains of society. For example, we have shown the significance of robotisation and digitalisation for employment, digital security and healthcare, and have identified the influence of big data and of technologies such as augmented reality and the IoT on human rights, patient rights and consumer rights, and what is needed to protect these rights.

[104] See: https://www.ser.nl/nl/actueel/werkprogramma/skills-strategy.aspx and OECD (2017) OECD Skills Strategy Diagnostic Report. Netherlands. Paris: OECD.

[105] See: https://www.rathenau.nl/nl/digitale-samenleving/acties-voor-een-verantwoorde-digitale-samenleving. This in response to the report *Urgent Upgrade* by the Rathenau Instituut, and the SER survey *People and Technology working together [Mens en Technologie: samen aan het werk*] (SER 2016), which sketches out the consequences of digitalisation and robotisation for the labour market, the organisation of work and employment relationships.

In the period 2017-2018, the focus was on safeguarding public values in the digital society.[106] On 9 March 2018, the Cabinet published its response to the report *Urgent Upgrade* and the report *Human rights in the robot age* (Parliamentary Papers II, 2017-2018, 26643, no. 529). This Cabinet response is discussed in chapter 5.

In 2017, the Rathenau Instituut wrote the report *Human rights in the robot age* at the request of the Parliamentary Assembly of the Council of Europe Europe (PACE) (Van Est & Gerritsen, 2017).[107] In this report, we advocated two new human rights: the right to not be measured, analysed or influenced, and the right to meaningful human contact. The report examines the use of robots, AI and virtual and augmented reality, and its effects on human rights. The report served as a source of background information for the rapporteur Mr Le Déaut, appointed by PACE. On the basis of the study, on 28 April 2017, PACE adopted the resolution *Technological convergence, artificial intelligence and human rights* and called upon the Council to examine how intelligent objects challenge human rights. On 19 October 2017, the Committee of Ministers of the Council of Europe adopted the recommendations in the PACE resolution (see chapter on fundamental rights and human rights).

With its report *A fair share. Safeguarding public interests in the sharing and gig economy* [*Waarborgen van publieke belangen in de deeleconomie en de kluseconomie*] (2017)[108], the Rathenau Instituut recommended that the interests of society in the sharing economy need better protection. The emergence of online sharing platforms is threatening public values, such as consumer protection, public order and privacy. The report issues a number of specific recommendations. First, the government should clarify the legal status of sharing and gig platforms. The government should also be able to appoint a trusted third party to monitor a platform in a manner that guarantees the privacy of the participants. Finally, the government should take measures to ensure that reviews of platforms are reliable and can be acted upon. In response to the report, the Dutch House of Representatives held a so-called thirty members debate (Proceedings House of Representatives 2017-2018, 9), and in January 2018 published the Cabinet response (Parliamentary Papers II, 2017-2018, 33009, no. 47) in which the Cabinet undertook to try to prevent or mitigate the negative effects of the sharing economy, and to encourage its positive effects.

[106] See working programme for 2017-2018: https://www.rathenau.nl/nl/publicatie/werkprogramma-2017-2018

[107] See: https://www.rathenau.nl/nl/digitale-samenleving/mensenrechten-het-robottijdperk

[108] See: https://www.rathenau.nl/nl/digitale-samenleving/eerlijk-delen

In its report *A never ending race* [*Een nooit gelopen race*] (Munnichs et al. 2017)[109], the Rathenau Instituut argued that greater priority should be given to strengthening the digital security of the Netherlands. We undertook this study at the request of the National Coordinator for Security and Counterterrorism (NCTV) and the General Intelligence and Security Service AIVD. The report makes it clear that as one of the most ICT-intensive economies in the world, the Netherlands is an attractive target for cybercriminals, cyber spies and hackers, and the existing vulnerabilities are compounded by the development of the IoT. According to the report, cyber threats undermine the innovative and competitive capacity of Dutch businesses and confidence in the digital society. Against that background, the Rathenau Instituut called for annual hacking tests and an independent centre of expertise and advice for SME enterprises. It also recommended investigating whether the existing liability legislation is sufficient for ICT products and services.
Supervisory bodies such as the ACM and the Telecom Agency should act more decisively when faced with the marketing of unsafe digital products.

The European Parliament commissioned us to investigate digital public participation. We published the report *Online meebeslissen – Lessen uit onderzoek naar digitale burgerparticipatie voor het Europees Parlement* [Online decision making – Lessons from the study into digital public participation by the European Parliament] (Korthagen & Van Keulen, 2017).[110] The report showed that digital participation can strengthen democracy. On the basis of numerous European case studies, six conditions were laid down for the government for arriving at successful digital participation programmes. It is for example essential that the process is linked to a specific agenda or resolution, that communication about the process and its objectives is clear, that feedback is issued to the participants with regard to their contributions and that more effort is made than simply collecting signatures. An effective communication and mobility strategy consisting of a variety of tailor-made tools is crucial in reaching specific target groups. Furthermore, public digital participation is a learning process, and must therefore be repeated and constantly improved.

In May 2018, the report *Digitalisering van het nieuws* [Digitalisation of the news] (Van Keulen et al., 2018) was published.[111] In this report, the Rathenau Instituut argues that to date, the Netherlands has not experienced any major negative impact from the spreading of disinformation. There are very few Dutch citizens who exclusively obtain their news via social media or search engines.

[109] See: https://www.rathenau.nl/nl/digitale-samenleving/een-nooit-gelopen-race
[110] See: https://www.rathenau.nl/nl/kennis-voor-beleid/online-meebeslissen
[111] See: https://www.rathenau.nl/nl/digitale-samenleving/digitalisering-van-het-nieuws

The Dutch people also enjoy considerable diversity in news reporting. Nonetheless, the vital functions of news provision for the public and political debate in the Netherlands could still be threatened by technological developments in the field of manipulation of audio and video material, the making of automatic computer accounts more ‘lifelike’ (*social bots*) and thereby more difficult to detect, and further personalisation of news flows. For all these reasons, the Netherlands must prepare for the future, for example by investing in ‘technological citizenship’ and acquiring a greater insight into how technology works, so that we can consider it critically and understand its importance for the world around us and society.

May 2018 also saw the publication of the report *Robotisering en automatisering op de werkvloer* [Robotisation and automation on the shop floor] (Freese et al., 2018).[112] In this report, we identified the choices facing businesses in the introduction of new digital technology. It offers specific guidelines for businesses that wish to gain an understanding of the key considerations when introducing new technology on the shop floor. The heart of the matter is: sound preparation is essential for successful digital innovation on the shop floor. The recommendations for shaping those preparations are: recognising that new digital technology requires new work processes, anticipating new earning models, being aware of new vulnerabilities in the business process, and involving the workforce in the introduction, and specific guidelines for businesses.

Finally, at the request of the Association of Netherlands Municipalities (VNG) we published the report *Waardevol digitaliseren* [Valuable Digitalisation] (Van Est et al. 2018),[113] in which the opportunities and risks of digitalisation for local administration are discussed. A key message is that innovation and digitalisation are not all about technological and economic innovation but also social and legal entrenchment. The report provides ten approaches that can help shape the actions of local administrators in this field.

Cyber Security Council

The Cyber Security Council (CSR) is a national, independent advisory body of the Dutch Cabinet composed of representatives from public and private sector organisations and the scientific community. The CSR undertakes efforts at strategic level to bolster cybersecurity in the Netherlands.[114]

With its report *Every business has duties of care in the field of cybersecurity* [*Ieder bedrijf heeft digitale zorgplichten*] (CSR, 2017a), the CSR offers a cybersecurity guide with an overview of the most important legal duties of care in the field of cybersecurity and a series of useful suggestions. In this report, the Council discusses the responsibility of the various different parties with regard to privacy and security.

[112] See: https://www.rathenau.nl/nl/digitale-samenleving/robotisering-en-automatisering-op-de-werkvloer
[113] See: https://www.rathenau.nl/nl/digitale-samenleving/waardevol-digitaliseren
[114] See: https://www.cybersecurityraad.nl/

In its report *Towards a safe, connected digital society* [*Naar een veilig verbonden digitale samenleving*] (CSR, 2017c), the Council emphasised the poor current state of security for IoT applications, and stated that public values such as security and freedom are threatened. The Council recommended the introduction of a label system according to which stickers and certificates or labels on the packaging of IoT products offer information to consumers about the security of the product. The Council also called for an information campaign and the drawing up of a guide on the label system. The Council furthermore recommended imposing security requirements on suppliers, and introducing greater supervision of manufacturers. Finally, the Council called for an independent monitor that provides information about those manufacturers and suppliers that inadequately protect their products.

With its report *Towards a nation-wide system of Information exchanges. Advice on information sharing in the field of cybersecurity and cybercrime* [*Naar een landelijk dekkend stelsel van Informatieknooppunten. Advies inzake informatie-uitwisseling met betrekking tot cybersecurity en cybercrime*] (CSR, 2017b), the CSR emphasised the fact that the sharing and analysis of information makes it possible to increase the digital security of organisations, and to make organisations more resilient to cyber incidents and/or to mitigate the damage caused. The Council proposed improving the exchange of information in the Netherlands by introducing a nationwide system of information exchanges, introducing the necessary parameters for successful information exchange via the information hubs, and increasing the understanding of cyber threats by encouraging the reporting of cybercrime, and strengthening public-private cooperation in this field.

Finally, in its report *Towards and open, secure and prosperous digital Netherlands. Recommendations regarding the Dutch National Cybersecurity Agenda (NCSA)* [*Naar een open, veilig en welvarend digital Nederland. Advies inzake the Nederlandse Cybersecurity Agenda (NCSA)*] (CSR, 2018), the CSR underlined the importance of a sound vision on protecting core values in an environment in which we as a country are often dependent for our cybersecurity on powerful international companies. According to the CSR, the Netherlands is facing the question of how to secure the core values that are essential to an open, secure and prosperous digital society. The CSR recommended an integrated approach whereby the Cabinet, government, businesses and the entire public sector are involved. The CSR called for the NCSA to focus on the following three subjects: an overview of fundamental issues and related decision making, decisive and comprehensive NCSA implementation, and structural investments in cybersecurity.

Council for Health and Society (RVS)

The Council for Health and Society (RVS) is an independent body that advises government and the Dutch Senate and House of Representatives. The task of the RVS is to issue strategic advice on policy implementation, taking into consideration all aspects that influence the health and performance of citizens in society.[115] Within the topic 'The promise of science and technology', the RVS is currently preparing recommendations as follow-up to the conference 'Man and Machine: who makes who?'. These recommendations will investigate changes in healthcare through the use of medical expert systems, and how freedom of choice and control can be maintained. The publication is expected in the second half of 2018.

Council for Public Administration (ROB)

The Council for Public Administration (ROB) is an independent body that advises on the structure and functioning of public administration and the principles of democracy and the rule of law. At the request of the Minister of the Interior and Kingdom Relations, the Council is currently investigating the opportunities and risks of digitalisation for democracy (Parliamentary Papers II, 2017-2018, 34775, no. 52). The Council is examining the position and negative consequences of platforms and digitalisation for the democratic debate, and the possible roles of business and the government. The recommendations are expected at the start of 2019.

Table 9 Overview of activities of advisory councils in the Netherlands on digitalisation and public values, in outline (1 January 2017 - 30 June 2018)

Who/what	**Technology**	**Issue**	**Action**
Netherlands Scientific Council for Government Policy			
Request for recommendation AI	AI	Public values	Multidisciplinary study into the impact of AI on public values
Digital disruption	Digitalisation	Digital security	Current
Knowing is not doing. A realistic perspective on self-reliance	e.g. digitalisation	Autonomy	In policy setting, government must assume a realistic citizens perspective
Council for Culture			
Advice on the audio-visual sector	Digitalisation, platforms	Safeguarding public values including Dutch stories in the audio-visual sector	Recommendation for smaller platforms to work together with super platforms to prevent exclusion and to introduce charges for end users to promote financial circularity within the sector

[115] See: https://www.raadrvs.nl/raad/over-rvs

Council for the Environment and Infrastructure

Assessing the value of technology – a guide	Digitalisation, autonomous vehicles, sharing economy	Security, autonomy, control over technology	Recommendations on balance between agility and stability, determining new relationships between parties, identifying new vulnerabilities and an eye for public values
Power supply under digital pressure	Digitalisation, AI	Digital security	Government must limit digital vulnerabilities of the electricity supply

Netherlands Institute for Social Research

The social state of the Netherlands 2017	E.g. digitalisation	Autonomy (reliance, digital skills)	Government plays an important role in providing the necessary resources

Netherlands Bureau for Economic Policy Analysis

Scientia potentia est: the emergence of the broker for everything	Digitalisation, platforms	Privacy, security, autonomy, democracy	Government needs to take measures in order to mitigate the risks of the passing on of misleading information by platforms

Netherlands Environmental Assessment Agency

Mobility and electricity in the digital age. Public values under pressure	Digitalisation	Security, control over technology, balance of power	More government control needed in order to safeguard public core values

Education Council

Thoughtful Digitalisation	Digitalisation in education	Privacy, security, autonomy(skills)	Education must be more closely involved and contribute to digital developments

Social Economic Council

Learning and development	E.g. digitalisation	Inclusive labour market	

Rathenau Instituut

Human rights in the robot age: challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality	Robotics, AI, virtual and augmented reality	Privacy, security, autonomy, control over technology, human dignity, balances of power	Call for a new European treaty with two new human rights: the right to not be measured, analysed or influenced and the right to meaningful human contact
A fair share. Safeguarding public interests in the sharing and gig economy	Platforms	Privacy, security, autonomy, balances of power	Advice on the sharing economy in which social interests need to be better protected
Urgent Upgrade. Safeguarding public values in the digital society	Digitalisation	7 public values (see table 2)	The government, regulators, businesses and society are insufficiently prepared for new ethical and societal questions
Rules for the digital human park	Digitalisation	Privacy, autonomy, control over technology, justice, human dignity	In an age of technological convergence and big data, a deliberate policy of ‘growing’ (through germline modification) and ‘taming of people (through persuasive technology) is needed
A never ending race	Digitalisation, IoT	Security	Strengthening digital security must be given greater priority in the Netherlands
Digital democracy	Digitalisation	Transparency, inclusion, democracy	Digital participation can strengthen democracy
Digitalisation of the news	Digitalisation, social media, platforms, persuasive technology	Democratic values, disinformation	The vital functions of news provision for the Dutch public and political debate may be at risk
Valuable digitalisation	Digitalisation	Public values	Mapping out the opportunities and risks of digital innovations at local administration level

Cyber Security Council			
Every business has digital duties of care	Digitalisation, IoT	Digital security, responsibility	Responsibility in the field of digital security explained
Towards a safe, connected digital society	Digitalisation, IoT	Digital security	Advice on digital security of the IoT
Towards a nationwide system of information exchanges	Digitalisation, IoT	Digital security	Advice on information exchange with regard to digital security and cyber threats
Towards an open, secure and prosperous digital Netherlands. Advice NCSA	Digitalisation, IoT	Digital security	Advice on how to safeguard an open, secure and prosperous digital society in the face of increased dependence on foreign tech companies
Council for Health and Society			
Advice following the conference ‘Man and Machine: who makes who?’	Digitalisation	Freedom, control	Safeguarding freedom of choice and control in care
Council for Public Administration			
Recommendations on the influence of digital platforms on the democratic process	Digitalisation, platforms, persuasive technology	Democratic values	Advice describes the opportunities and risk of digitalisation for democracy

Source: Rathenau Instituut

4.2 International developments

Organisation for Economic Cooperation and Developments

The Organisation for Economic Cooperation and Development (OECD) is a collaborative venture between 35 countries, the aim of which is to promote policy to improve the economic and social welfare of people throughout the world. The OECD organises a wide range of activities in the field of digitalisation. For example, it maintains a Directorate For Science, Technology and Innovation, and operates an all-encompassing *Going Digital* project, the aim of which is to promote strong and inclusive growth for the digital revolution, while it also organises all kinds of fora and conferences in the field of digitalisation. Subjects of discussion include AI; the digital economy, security and privacy; and digital government, transparency and inclusion.[116]

[116] See: http://www.oecd.org/going-digital/project/

In March 2018, a report was published on the challenges of levying taxation caused by digitalisation. In this report, the OECD argued in favour of taxing technology companies more heavily by requiring businesses to also pay tax in a Member State where they maintain a ‘digital presence’ so as to guarantee an equal basis for profit tax throughout the EU (OECD, 2018).

European Economic and Social Committee

The European Economic and Social Committee (EESC) is an EU advisory body comprising representatives of employers’ and employees’ organisations and other interest groups. The EESC advises the European Commission, the Council of the EU and the European Parliament on EU affairs, and as such acts as a bridge between EU decision making bodies and the citizens of the EU.[117]

In 2017, the EESC produced an own-initiative opinion paper on the societal and ethical impact of AI. In its recommendations, the EESC identified eleven domains in which IA is creating challenges which require action, namely: ethics; safety; privacy; transparency and comprehensibility; employment; education and skills; (in) equality and inclusiveness; laws and regulations; governance and democracy; warfare; and superintelligence (Muller, 2017).

The EESC called for the establishment of supranational policy chambers concerning AI, because the impact of AI is not limited to the national or European level but transcends national boundaries. The EESC also recommended that the European Union adopts an international pioneering role in adopting worldwide frameworks for AI policy, in line with European values and fundamental rights. The EESC furthermore called for an ethical code for the development and use of AI aimed at safeguarding the values of human dignity, integrity, freedom, privacy, culture and gender diversity and fundamental human rights. Finally, the EESC argued for the development of accountable European AI systems featuring European AI certification and labels, thereby safeguarding ethical values such as security and transparency.

European Group on Ethics in Science and New Technologies

At a European level, the European Group on Ethics in Science and New Technologies (EGE) plays an important identifying role in discussions about the ethical aspects of science and new technologies. The EGE is an independent international committee of experts that reports to the President of the European Commission, and is a central player in the network of national ethical councils from various EU countries.[118]

[117] See: https://europa.eu/european-union/about-eu/institutions-bodies/european-economic-social-committee_nl

[118] See ec.europa.eu/research/ege/index.cfm

In March 2018, the EGE published its report *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems* in which it emphasised the urgency of an internationally approved ethical framework for the design, production, use and governance of AI, robots and autonomous systems. The EGE furthermore called for broad and systematic public involvement and consultation with regard to the ethics of AI, robotics and autonomous technology in relation to public values. The EGE proposed a series of basic principles and democratic values as the first step towards ethical guidelines: human dignity, autonomy, responsibility, justice, equality and solidarity, democracy, accountability, security and integrity, data protection and privacy and sustainability. The EGE then called for a process to be started aimed at establishing an internationally approved ethical and legal framework.

In response to the report, the European Commission has established a committee of experts to study AI ethics. This committee will lay down guidelines for the ethical use of AI, based on the EGE report and the values described in it.

European Union Agency for Fundamental Rights

The European Union Agency for Fundamental Rights (FRA) is an EU organisation that assists the European Commission and offers expertise in the field of fundamental rights. One of the subjects in its working programme is the information society, with particular focus on respect for private life and the protection of personal data.

In May 2018, a paper was published on big data and discrimination in data-supported decision making (FRA, 2018). The report describes how discrimination can occur when big data, algorithms and AI are used, and proposes a series of solutions aimed at mitigating the risk of discrimination. The FRA is also a member of the European High Level Expert Group on Artificial Intelligence (see chapter 5). In 2019, the FRA intends to carry out research into the implications of AI and big data for fundamental rights.

European Political Strategy Centre

The European Political Strategy Centre (EPSC), formerly the Bureau of European Policy Advisers (BEPA), is the internal think tank of the European Commission and was established in 2014 by Commission President Jean-Claude Juncker.

In March 2018, the EPSC published its paper *The Age of Artificial Intelligence. Towards a European Strategy for Human-Centric Machines.* One focus of study in the paper is the ethical challenges arising from AI (EPSC, 2018). In the report, the EPSC called for an AI strategy and regulatory standards and guidelines to safeguard the ethical development of AI, with a central focus on human beings, with particular attention for liability.[119]

Table 10 Activities within the political-administrative domain in the field of agenda setting, in outline (1 January 2017 - 30 June 2018)

Who/what	Technology	Issue	Action
European Group on Ethics in Science and New Technologies			
Ethics of Artificial Intelligence	AI	Privacy, security, democracy, autonomy, control over technology, human dignity	International ethical and legal framework for ethical use of AI
Organisation for Economic Cooperation and Development (OECD)			
Going Digital	Digitalisation, AI, platforms	Privacy, security, justice, inclusion, balances of power	Developing policy for inclusive growth, sustainability and welfare
Tax challenges from digitalisation	Digitalisation, platforms	Balances of power	Proposal for imposing equal income tax on technology companies in the EU
European Economic and Social Committee			
AI	AI	Privacy, security, control over technology, autonomy, human dignity, inclusion, democracy	Among others social debate on AI design, development of ethical code

[119] The Institute of Electrical and Electronic Engineers (IEEE) also established the Global Initiative on Ethics of Autonomous and Intelligent Systems in 2016, aimed at establishing policy guidelines to promote the ethical implementation of AI.

European Union Agency for Fundamental Rights			
Theme Information society	*Big data*	Protecting fundamental rights, privacy, data protection, discrimination	Identifying challenges and solutions with regard to the information society
Report *Big data*: Discrimination	*Big data and* algorithms, AI	Justice, control over technology	Identifying challenges and solutions regarding to *big data*
European Political Strategy Centre			
AI challenges	AI	Safeguarding the development of human-centric AI	AI strategy and regulatory standards and guidelines

Source: Rathenau Instituut

4.3 Conclusion

Focus on digitalisation and protecting of public values
As compared with *Urgent Upgrade*, we have seen more advisory councils active in considering digitalisation and the related ethical and societal issues. The reports emphasise that public values are at risk as a result of digitalisation. In 2017 there was greater attention in the Netherlands for digitalisation as a whole: a series of recommendations were not so much aimed at specific technological practices or sectors but considered the influence of digitalisation and technological developments on society as a whole.

Since 2018, we have seen a shift in attention within the advisory councils towards specific sectors such as energy, mobility, healthcare and the media, and specific fields of technology such as AI and digital security. At international level (Europe), advisory councils are above all focusing their attention on AI.

More control by government and more dialogue
In their reports, the advisory councils recommend government to impose more direction and control. Both with regard to digital security and within education and at the level of the individual citizen, we are seeing calls for a different role from government because education and citizens are not able to cope on their own. The government is called upon to intervene to a greater extent to mitigate the potential negative consequences of technological developments on society.

The advisory councils have also emphasised the importance of initiating discussion with society (businesses, civil society organisations and citizens) in order to lay down new frameworks.

Attention for the self-reliance of citizens

A new theme in the Netherlands is the limits on the self-reliance of the country's citizens. Various advisory councils have called for attention for the pressure imposed on citizens by the growth of digitalisation and the government. As a consequence, various groups of individuals – not only small vulnerable groups such as the elderly, people with limited literacy skills or people with a disability – may experience difficulties as a result. Advisory councils have urged government to adopt a new role, and are calling for government to take greater account of the acting capacity of individual citizens.

5 Politics and administration: policy development and political decision making

In the policy development and political decision making phase, reports and recommendations aimed at policy preparation are translated into visions, policy, regulations and their political approval. In this chapter, we look at the actors that are institutionally responsible for policy and political decision making: the Cabinet, the Ministries and Parliament. Here we discuss the most relevant policy documents with regard to ethical and societal digitalisation issues from the Ministries of the Interior and Kingdom Relations (BZK), Economic Affairs and Climate Policy (EZK)), Justice and Security (JenV), Education, Culture and Science (OCW) and Foreign Affairs (BZ).

With the inauguration of the new Cabinet, at the start of 2018 a series of national agendas were announced including the overarching national digitalisation agenda, in June 2018. The agenda refers to topic such as privacy, digital security, platforms, consumer rights, skills and fundamental rights and ethics. Privacy and digital security have been on the policy agenda in the Netherlands for some time already. In 2017-2018, specific policy measures were announced, for example the establishment of the Digital Trust Centre for the SME sector and the plans for introducing compulsory certification for certain IoT products.

Other societal and ethical issues, such as control over algorithms or the effects of automated decision making are new on the agenda. In these areas, the Cabinet is considering how best to translate these questions into specific policy measures.

For other subjects, the Cabinet is turning to Europe. The European Commission is currently modernising a series of regulatory frameworks or formulating new frameworks, among others with regard to data protection, ePrivacy, audio-visual and media services, copyright, consumer rights and cybersecurity.

The Dutch parliament has been considering privacy and digital security, and such new issues as transparency of algorithms, justice and discrimination through the use of algorithms, the spreading of disinformation and the position of sharing and gig platforms.

5.1 Cabinet and Ministries

National Digitalisation Agenda
Societal and ethical aspects of digitalisation are reflected in various ways in the ambitions of the Cabinet. In June 2018, the Ministry of Economic Affairs and Climate Policy published the 'Dutch Digitalisation Strategy' in collaboration with the Ministry of the Interior and Kingdom Relations and the Ministry of Justice and Security (EZK 2018a). This strategy contains an overarching vision aimed at bringing about the policy aims of the Cabinet.

In a series of separate agendas, various points are to be further elaborated such as the National Cyber Security Agenda and the Digital Government Agenda; these will be discussed below under the individual Ministry headings. The strategy refers to a 'digital transformation' facing the Cabinet and society. In the strategy, the Cabinet formulates three ambitions:

1. taking the lead and grasping opportunities;
2. everyone participates and cooperates; and
3. confidence in the digital future.

In its strategy, the Cabinet has focused on research and innovation, the future of work, new skills and digital literacy, a competitive, fair and transparent digital economy, consumer rights, digital security and privacy, and fundamental rights and ethics in a digital age (including attention for the effects of automated decision making). For a further discussion of the strategy of the Ministry of Economic Affairs and Climate Policy, see section 5.1.2.

5.1.1 Ministry of the Interior and Kingdom Relations (BZK)

The Ministry of the Interior and Kingdom Relations (BZK) is involved in a number of different ways in the ethical and societal aspects of digitalisation for the government itself, and in its contact with the public and businesses. Key topics in the period 2017-2018 include digital government, fundamental rights, digital skills, smart cities, disinformation, privacy and digital security.

Digital government
In July 2018, the Ministry published a *Digital Government Agenda* [*'NL DIGIbeter – Agenda Digitale Overheid' BZK 2018a*]. Although strictly speaking this publication fell outside our study period, we have included it here in view of the overarching function. The agenda is part of the Dutch Digitalisation Strategy.

The Digital Government Agenda is aimed at government and contacts with the general public and businesses. The central focus is ‘grasping opportunities and protecting rights’ (BZK 2018a). The agenda follows five policy lines:

1. investing in innovation;
2. protecting fundamental rights and public values;
3. accessible, understandable and intended for everyone;
4. making services more personal; and
5. ready for the future.

June 2018 also saw the publication of the Digital Government bill, aimed at improving digital services to citizens and businesses (BZK, 2018b). The aim of the new law is to ensure that Dutch citizens and businesses can log in with (semi-) government in a secure and reliable manner, with electronic identification tools that are more reliable than DigiD.[120] In anticipation of that situation, the Digi programme 2018 was published in January 2018 entitled ‘Digitalisation with confidence’, about the development of the Generic Digital Infrastructure (GDI) (BZK 2018b).[121]

Digitalisation and fundamental rights

In March 2018, the Cabinet published its response to the reports from the Rathenau Instituut *Urgent Upgrade* and *Human rights in the robot age* (Parliamentary Papers II, 2017-2018, 26643, no. 529). In its response, the Cabinet outlined the frameworks in place for safeguarding public values and human rights in the digital society, and the initiatives to be taken (Parliamentary Papers II, 2017-2018, 26643, no. 529):

1. The Cabinet recognises the impact of the new wave of digitalisation on public values and human rights. It also undertakes to employ specific policy instruments for safeguarding public values and human rights, and will continue and where necessary intensify this policy.
2. The Cabinet will discuss supervision of the safeguarding of public values and human rights, and will hold a series of dialogues on new ethical questions.
3. The Cabinet will establish an interdepartmental working group with the purpose of elaborating the vision on the impact of digitalisation on public values and human rights. The group will also work on research into and specific actions regarding the further reinforcement of the framework of public values and human rights.
4. The Ministry of the Interior and Kingdom Relations will focus on dialogue about public values and human rights and how to safeguard them in the information society. It will also facilitate living labs in which government bodies can experiment with the proper use of data in the public space.

[120] See: https://www.digitaleoverheid.nl/

[121] Key driver for the Digital Agenda and the Digi programme of BZK is the report *Make it happen!* [*Maak Waar*] from the Study Group in Information Society and Government (Studiegroep Informatiesamenleving en Overheid, SIO) established in 2016 (SIO, 2017).

The Ministry of the Interior and Kingdom Relations (BZK) will also be commissioning a number of studies into the safeguarding of public values and human rights.[122] The University of Utrecht, for example, investigated the relationship between algorithms and fundamental rights (Vetzo et al. 2018). The Ministry has also ordered a study into the way in which digitalisation can be integrated in the National Human Rights Action Plan.

Furthermore, BKZ is investigating the use of (self) learning algorithms within government (Parliamentary Papers II 2017-2018, 26643, no. 527). In the announced 'open source policy vision', BZK will be further investigating the possibilities for the public provision of source codes for automated decision making (Appendix to Proceedings II 2017-2018, 1612).[123] Elsewhere, BZK aims to investigate blockchain and the law, and biometrics.

In the field of digital democracy, BZK has requested the Council for Public Administration (ROB) to investigate the threats and opportunities of digitalisation for a properly functioning and modern democracy.

Digital skills

The promotion of knowledge in the field of ICT in government is one of the spearheads in the Digital Government Agenda (BZK 2018a). This will be facilitated for decision makers via the Senior Civil Service and via the programme of the National Academy for Digitalisation and Automation of Government. Broadening the digital skills of individual citizens is another spearhead in the Digital Government Agenda. The Cabinet aims to work alongside civil society organisations to increase the range of courses on offer, and help people get started. The Cabinet is also investigating the problems that citizens face in their digital contact with government, with a view to improving its own systems. The Dutch House of Representatives will take receipt of the approach for digital inclusion before the end of 2018.

Smart cities

In 2015, alongside civil society partners, cities and central government committed to the *City Agenda* programme, aimed at improving innovation and quality of life in the Dutch cities network.[124] In 2016 and 2017, a series of City Deals were signed, as part of this programme. These are also referred to in the Cabinet response to the reports from the Rathenau Instituut.

[122] Other (announced) studies include a request for recommendation for the Advisory Council on Government Policy (WRR) on the impact of AI on public values. The Research and Documentation Centre (WODC) has ordered a study into the legal aspects of algorithms that autonomously take decisions.

[123] Reply to questions from Middendorp and Koopmans about reporting on the thesis by Marlies van Eck at Tilburg University, by Secretary of State Knops.

[124] See: https://agendastad.nl/

Various departments have established experimental environments in order to acquire experience with the effects of technologies.[125] Assessment frameworks have also been prepared for a series of experiments aimed at safeguarding the right to privacy (Parliamentary Papers II, 2017-2018, 26 643, no. 529). During this Cabinet period, the Ministry of the Interior and Kingdom Relations will be publishing a Code of Good Digital Governance, with the aim of drawing up rules of play for the use of data, in collaboration with the 'smart cities' (BZK 2018a).

Disinformation

There is also attention within the Ministry of the Interior and Kingdom Relations for covert influencing and disinformation. Minister Ollongren, in a letter to the Dutch House of Representatives, for example wrote that political influencing by state actors in Dutch internal affairs or democratic processes, such as elections, through the covert use of (fake) arguments, selective information and disinformation is viewed as most undesirable (Parliamentary Papers II, 2017-2018, 26643, no. 496). In the letter, Ollongren said that she had held discussions with media and tech companies such as Facebook, Twitter, Microsoft and Google about possible measures to be taken. She also revealed that the Dutch intelligence and security services have been investigating the intentions and capacities of state actors. The multi-year programme agreed by the parties in the current Dutch coalition government has also earmarked additional funding for digital security. The Cabinet is currently analysing potential vulnerability in the voting process.[126]

Privacy and digital security

Finally, the Ministry contributed to the modernisation of the Intelligence and Security Services Act (Wiv 2017). The new Act introduces a broadening of the powers of interception by the Dutch intelligence and security services (AIVD and MIVD). New guarantees have also been laid down, including advisory assessment prior to deployment of these powers and an evaluation of the Wiv after two years. Following the advisory referendum on 21 March 2018, in which a small majority (49.44%) came out against the Act, the Cabinet made a number of changes (Parliamentary Papers 2017-2018, 34588, no. 70). These above all relate to the sharing of information with other countries, the retention period and the targeted deployment of extraordinary powers. The Wiv came into effect on 1 May 2018.[127]

[125] The Living Lab Big Data, for example was established in the field of justice and security, to gain an insight into migration routes, migration motives and the level of education of asylum seekers, and to improve data quality within the information systems. The City Deal programme 'Vision on undermining' was launched to gain a better understanding of patterns in undermining crime, using data analysis.

[126] See: https://www.tweedekamer.nl/Kamerstukken/detail?id=2018Z09600&did=2018D30291

[127] In the field of security, attention was also focused on the reliability and security of support software during elections, the use and implementation of fingerprints in passport, and information security in government.

Table 11 Overview of societal and ethical aspects of digitalisation, Ministry of the Interior and Kingdom Relations (BZK), in outline (1 January 2017 - 30 June 2018)

Who/what	Technology	Issue	Action
NL DIGIbeter (Digital Government Agenda)	Digitalisation of government	Fundamental rights, privacy, security, autonomy	Capturing opportunities and protecting rights for digital government
Digital government (digital government bill, 'Digitalisation with trust')	Digitalisation of government	Privacy, security, skills, autonomy	Increased reliability of contact with government
Cabinet response to 'Urgent Upgrade' and 'Human rights in the robot age'	Digitalisation	Public values, human rights (including privacy, security, autonomy, control of technology)	Frameworks and policy instruments for safeguarding public values
Cabinet response to Knowing is not yet doing	Digitalisation	Resilience, autonomy	Including 'acting capacity test'
Digital skills	Digitalisation	Resilience, autonomy	Management of data; Approach to digital inclusion
Letter on covert influencing by state actors	Digitalisation, platforms, social media	Security, freedom of expression	E.g. in discussion with technology companies; AIVD & MIVD investigation into vulnerability of the election process
Smart cities	Digitalisation	Public values	Code of good digital governance
Modernising Wiv	Digitalisation, communication	Digital security	New authorities for security services

Source: Rathenau Instituut

5.1.2 Ministry of Economic Affairs and Climate Policy

Privacy and digital security

In the policy of the Ministry of Economic Affairs and Climate Policy (EZK), privacy, digital security and digital trust have been subjects of study for quite some time. In the period 2017-2018 these subjects are still on the Ministry's policy agenda. Increasing the resilience of citizens and organisations is one of the spearheads of the national digitalisation agenda: attention has been paid to digital security problems with regard to the IoT, and the Digital Trust Centre was established for the SME sector (see also Parliamentary Papers II, 2017-2018, 26643, no. 488).

Moreover, campaigns for citizens and SME enterprises have been linked to (new) policy for privacy and security, and the Cabinet has been working hard to bring about the establishment and implementation of the European ePrivacy-regulation.

In the ‘Roadmap for secure digital hardware and software’, the Cabinet has announced measures for a safer IoT (EZK 2018b). The Cabinet is focusing on standards and the certification of devices. This is reflected for example in the following actions:

- In European negotiations, the Netherlands has urged the rapid adoption of the Cyber Security Act that aims to lay down a European certification framework for ICT products and services.
- The Cabinet aims to introduce compulsory certification for specific product categories in the near future, and to gradually expand certification in the longer term.
- There will be a monitor with information about the digital security of IoT devices and a pilot programme for testing hardware and software.
- The Cabinet is investigating the possibilities of improving liability with regard to unsafe hardware and software. The Netherlands also takes part in the European high-level expert group on liability and new technologies.
- In negotiations on the European Directive on digital content and services, the Netherlands has proposed compulsory software updates for manufacturers.
- The Cabinet is investigating which minimum security requirements should be imposed on devices via the European Radio Equipment Directive, and will organise a dialogue session for the supervisory bodies to examine the role they can play in promoting digital security.
- The Cabinet is investigating the additional measures that may be necessary in central government procurement policy.

Skills

The future of work and the changing requirements imposed by work on the working population is part of the ambition ‘Involving everyone’ from the national digitalisation agenda. As well as modernising education with more attention for digital skills (see section 5.1.4), the Cabinet aims to support civil society organisations and initiatives with the aim of offering additional training to people with limited digital skills. The Ministry for example supports *‘Samen Digiwijzer’* [‘More digital wisdom together’] to promote the introduction of digital skills in education.[128]

The government programme on lifelong learning will be further elaborated. The aim of the Human Capital ICT Agenda is to increase the number of ICT students and the ‘Technology Pact’ is an attempt to make up the shortage of ICT specialists. The programme ‘Strengthening HR ICT in Government Service’ is available for ICT professionals in government.

[128] *Samen Digiwijzer* is an initiative of CodePact, Mediawijzer.net and Kennisnet and is supported by various partners. See: https://samendigiwijzer.nl/

Platforms and consumer rights

Other topics on the national agenda include the opportunities and risks of platforms and consumer rights. The Cabinet is working at European level on maintaining the competitiveness of digital markets and clarity on the question of whether alterations are needed in the competition system structures. The Cabinet will itself be investigating a variety of tools, including the regulation of charges and access. The House of Representatives will be informed on these issues in the autumn of 2018 (EZK 2018a).

There is a proposal from the European Commission aimed at improving the fairness and transparency of business relations between businesses and large platforms. The Cabinet recognises the importance of fair and transparent relationships but wants to avoid too many detailed requirements being imposed on platforms. This could have a negative outcome for smaller platforms. Wherever possible, the Cabinet encourages self-regulation by platforms; if this proves insufficiently effective, the Cabinet will consider the need for additional regulation (as in the case of the letting of residential property to tourists).

There are also new legislative proposals from the European Commission in the field of consumer protection. In that connection, the Cabinet is in favour of more stringent information requirements and greater transparency on platforms about the identity of the provider.

Fundamental rights and ethics

A new topic for the Ministry of Economic Affairs and Climate Policy in the period 2017-2018 is attention for fundamental rights and ethics in the digital age, one of the policy spearheads in the National Digitalisation Agenda. The Secretary of State for digitalisation has submitted a request for advice to the WRR about AI and public values (Parliamentary Papers II, 2017-2018, 26 643, no. 529).

The Cabinet has also announced the development of a new national innovation programme for AI, which will include attention for transparency of algorithms.

Futureproof legislation

The futureproof regulation programme has been undertaken over the past few years. It was concluded on 26 June 2017. The programme examined whether, as a result of technological developments, legislation and regulations have become either obsolete or obstructive, or fall short of their mark, and how such issues can be dealt with (Parliamentary Papers II 2016-2017, 33009, no. 42). On the basis of this programme, a series of measures has been announced aimed at increasing the transparency of the legislative process, including Internet consultation and the digital legislation calendar (Parliamentary Papers II 2016-2017, 33009, no. 39).

Over the coming period, too, futureproof regulation will be a point of attention. The Cabinet has announced that there is already considerable scope for innovation in existing legislation and regulations. Amendments are sometimes necessary, but the process is time-consuming. As a consequence, in its national digitalisation agenda, the Cabinet announced that strategic surveys will be undertaken more regularly at an early stage, with a view to evaluating the legal, technological and ethical consequences of new developments.

Business policy

The discussion in the field of a *techproof* economy is focusing on a successful digital transformation and retaining a strong competitive position in a global playing field. With its 2017 business policy *Navigeren met wind in the zeilen* [Navigating with wind in our sails], the Cabinet has focused on sustainable economic growth (EZK 2017).

In response to the Ester motion (Parliamentary Papers 33 750 XIII, E, 2014), in which the government was called upon to create space on a structural basis for reflection on ethical questions in its technology and innovation policy, the monitor has identified a number of activities in this area (Parliamentary Papers 2015-2016, 33009, no. 16). The monitor refers to research programmes at European and national level, including Horizon2020 (the SATORI project, in which an ethical impact assessment has been developed) and the NWO programme Corporate Socially Responsible Innovation, aimed at research into the societal, social and ethical aspects of innovation research. The monitor also refers to the attention being paid to ethical aspects within a number of top sectors.

Table 12 Overview of societal and ethical aspects of digitalisation, Ministry of Economic Affairs and Climate Policy (EZK), in outline (1 January 2017 - 30 June 2018)

Who/what	Technology	Issue	Action
Cabinet response to the report 'Equal share' from the Rathenau Instituut	Gig platforms and sharing economy	Consumer protection, public order and privacy	Striving to avoid or mitigate the negative effects of the sharing economy and to promote its positive effects
Cabinet response to report from CPB 'Scientia potentia est'	Gig platforms	Transparency and liability	Attention will be focused on platform risks in the National Digitalisation Strategy
Cabinet response to report from PBL 'Mobility and electricity in the digital age'	Digitalisation	Security	With the implementation of the Cybersecurity Act, EZK aims to improve European cooperation in ICT incidents
National Digitalisation Strategy	Digitalisation	Security	Specific agenda for the digitalisation of public administration
Roadmap for secure digital hardware and software	Digitalisation, IoT	Security, liability	Agenda aimed at improving the security of connected devices
Digital Trust Centre	Digitalisation	Security, digital security	The aim is to make businesses more resilient to cyber threats
Platforms and consumer rights	Digitalisation, IoT, platforms	Security, liability	Problems facing consumers when making purchases, investigation into competition tools
Human Capital Agenda, Technology Pact	Digitalisation	Digital skills	Retaining and increasing human capital; linking education with the labour market in the technology sector
Futureproof regulation	Digitalisation	Statutory frameworks	Matching legislation to technological developments
Business Policy 2017	Technology	Innovation	Including ethical aspects in developing of innovations

Source: Rathenau Instituut

5.1.3 Ministry of Justice and Security (JenV)

Privacy and digital security are well-known themes within the Ministry of Justice and Security. New on the Ministry's agenda are the significance of algorithms, profiling and AI, for example with regard to the administration of justice.

Digital security

On 21 April 2018, the Ministry published the Dutch Cybersecurity Agenda (NCSA) (JenV 2018a). This is the Ministry's third cybersecurity strategy. The first was published in 2011, and the second in 2013. In the current coalition government programme, a structural investment of €95 million has been allocated to cybersecurity, and this has been elaborated in the NCSA. Key points for attention are standards for IoT devices, software liability, promoting cybersecurity research and improving information campaigns. Policy measures in the field of secure IoT devices appear in the Roadmap for Secure Digital Hardware and Software (see EZK 2018b).

As concerns the vital infrastructure, the Ministry of Justice and Security submitted a bill for the Cybersecurity Act to the House of Representatives (Parliamentary Papers 2017-2018, 34388, no. G). The bill is the result of the Network and Information Security Directive (NIS Directive) of the European Union.[129] Based on this proposal, the number of providers of vital infrastructure subject to a duty of care and reporting obligations will be expanded.[130] Subject to the Cybersecurity Act, providers of essential services such as drinking water companies, banks and gas and electricity supply operators will be required to satisfy specific security requirements during the course of 2018. They must take adequate measures to prevent external breaches of their network and information security.

With regard to the authorities of investigative services, the Computer Crime III Act also known as the 'hack back Act' was adopted by the Dutch Senate in June 2018 (Parliamentary Papers I 2016-2017, 34372). The Act allows the police and prosecution service to carry out covert, remote (online) investigations in computers, servers and mobile telephones. The Act will be re-evaluated two years after its introduction.

[129] This is the first cybersecurity legislation on a European level and encourages the Member States to increase their digital resilience, and to work together better.

[130] At present, pursuant to the Data Processing and Cybersecurity Notification Obligation Act (Wgmc) 2017 providers of certain services are only required to report incidents of this kind to the National Cyber Security Centrum (NCSC)

Privacy

In the period 2017-2018, considerable attention was focused on the introduction of the General Data Protection Regulation (GDPR). This required the drawing up of the General Data Protection Regulation Implementation Act. Both came into effect on 25 May 2018.[131] The Ministry also published a guide to the new Act (JenV, 2018b) and a big data toolbox, with information about the responsible use of big data.[132]

A new model was also introduced for Privacy Impact Assessments for new legislation by Central Government (Parliamentary Papers II 2017-2018, 26643, no. 490), and a bill was submitted on the implementation of the European PNR Directive (PNR stands for 'Passenger Name Records') (2016/681/EU). This Directive relates to the use of personal data of passengers in the prevention, investigation and prosecution of terrorist crimes and serious crime (Parliamentary Papers II 2017/2018, 34861, no. 2).[133]

The Cabinet has said that it will be sending its vision on strengthening horizontal privacy between individual citizens to the House of Representatives in the autumn of 2018.[134]

Finally, in the general discussions in the Dutch House of Representatives on big data and the protection of personal data on 30 May 2018, the Minister for Legal Protection announced that a response will be issued to the Verhoeven and Van Nispen motion. This motion called upon the government to inform the House before the end of 2018 on how the Dutch Data Protection Authority intends to carry out its additional tasks and authorities (Parliamentary Papers II 2017-2018, 34851, no. 23).

[131] The GDPR reinforces and expands privacy rights with the right to be forgotten and the right to data portability. People now have more possibilities for standing up for themselves in the processing of their data. People can for example demand that organisations delete personal data and pass on this deletion to all other organisations who have received those data. People are also entitled to receive their personal data from organisations in a standard format. In addition, organisations are now responsible for demonstrating in documented form that they have taken the proper organisational and technical measures to satisfy the GDPR. Furthermore, European privacy regulators have been given greater authorities, including the authority to impose penalties of up to 20 million euro or 4 percent of global turnover in the event of violation of the principles of the GDPR.

[132] See: https://www.rijksoverheid.nl/documenten/publicaties/2018/04/20/big-data-factsheet. The toolbox includes a factsheet *Big data*, 10 principles for experimenting with big data, a JenV model processing agreement, and an addition to the model GEB Rijksdienst (PIA) with privacy pointers for big data processing.

[133] Airlines are required to issue their passenger details to the Passenger Information Union Netherlands, whose task is to process and analyse this information, during the course of 2018

[134] This will also include the response from the Cabinet to the initiative memorandum from Member of Parliament Koopmans on horizontal privacy (Parliamentary Papers II 2017-2018, 34926, no. 1-2).

Control of technology

The Ministry of Justice and Security is focusing increased attention on algorithms. In response to the recommendations from the WRR report *Big data in een vrije en veilige samenleving* [Big data in a free and safe society] the Cabinet prepared ten action points (Parliamentary Papers II, 2016-2017, 26643;32761, no. 426). In May 2018, the Minister for Legal Protection outlined the situation with regard to the implementation of these action points (Parliamentary Papers II 2017-2018, 26643/32761, no. 537). The action points, among others, relate to:

- **a clear legal basis for the use of data analyses**
  The Cabinet will be examining whether the legal basis for the implementation and use of data analyses requires reinforcement. A working group has been established for this purpose, which is expected to have completed its work in the second half of 2018.

- **transparency of algorithms**
  The Cabinet is investigating how algorithms can be made sufficiently transparent for supervisory bodies and judicial assessment. A working group has drawn up a circular (notice for government bodies) entitled ‘Transparency of algorithms’, that will be included in the big data toolbox. The toolbox contains information and guidelines for professionals working with big data. The Cabinet has also investigated whether it is possible for ICT government tenders to demand the tendering parties to make their algorithms sufficiently transparent, at least for the regulator and the courts. The outcome was that the Interdepartmental Committee on Corporate Law Advice (*Interdepartementale Commissie Bedrijfsjuridisch Advies*) sees no grounds for adjusting the general terms and conditions for IT agreements (ARBIT) because ‘at present the demand is too limited to justify inclusion in the general terms and conditions’ (Parliamentary Papers II 2017-2018, 26643/32761, no. 537).
  The Cabinet has also called upon the Council for the Judiciary (Raad voor de Rechtspraak) to consider the knowledge that will be needed to deal with lawsuits in which big data analyses play a role.

The Minister for Legal Protection will be issuing a letter about the significance of algorithms and AI for the administration of justice in the autumn of 2018 (EZK 2018a).

Legal position of citizens

The Research and Documentation Centre (WODC) at the Ministry of Justice and Security commissioned a study into the possibility and desirability of extending the opportunities available to citizens and interest groups in seeking recourse before the courts for an assessment of big data applications. The study, undertaken by the University of Tilburg, is expected to be completed in the second half of 2018.

Table 13 Overview of activities relating to the societal and ethical aspects of digitalisation, Ministry of Justice and Security, in outline (1 January 2017 - 30 June 2018)

Who/what	**Technology**	**Issue**	**Action**
Computer Crime III Act	Digitalisation	Security	New authorities for security services
General Data Protection Regulation (GDPR), General Data Protection Regulation Implementation Act	Digitalisation	Privacy	Strengthened and extended privacy rights; Organisations given more responsibilities
Toolbox	Digitalisation, big data and algorithms	Privacy	Privacy
Bill PNR data	Digitalisation	Security	Registration of passenger data
Vision on horizontal privacy	Digitalisation, social media, platforms	Privacy	Autumn 2018
Dutch Cybersecurity Agenda (NSCA)	Digitalisation, IoT	Security	Cybersecurity, research, skills, vital infrastructure
Cybersecurity Act	Digitalisation	Security	Providers of essential services must satisfy security requirements and take adequate measures against external breaches of their network and information security
Cabinet response to report from ACVZ ‘Profiling and selection’	Algorithms	Control of technology, justice (profiling, discrimination)	Justice and Security will investigate whether the current legal framework requires strengthening
Working group on strengthening legal basis for use of data analyses	Big data and algorithms	Control of technology, justice (profiling, discrimination)	Second half 2018
Algorithms in administration of justice	Big data and algorithms, AI	Control of technology, justice (profiling, discrimination)	Second half 2018

WODC study into the legal aspects of (autonomous) algorithms	Digitalisation, algorithms	Control of technology, justice (profiling, discrimination)	2018
WODC study into the legal position of citizens		Autonomy	Possibilities for citizens and interest groups to turn to the courts for assessment of big data, second half 2018

Source: Rathenau Instituut

5.1.4 Ministry of Education, Culture and Science (OCW)

The Ministry of Education, Culture and Science is involved in the ethical-societal aspects of digitalisation in a number of different ways. Existing topics include: (digital) skills, media literacy, promoting independent journalism and media plurality. A new item on the agenda is tackling disinformation and the personalisation of news.

Digital skills

The goal of the Cabinet is to have a new educational curriculum for primary and secondary education put in place by 2021, whereby there will be greater attention for digital literacy (EZK 2018a). The Ministry of Education, Culture and Science has been working on this new curriculum for some time. At the start of 2015, for example, the Platform Education2032 was established. Following the final recommendations issued in 2016, nine development teams consisting of teachers and head teachers from primary and secondary education started work in 2018. At the start of 2019, the outcomes will be shared with the Dutch House of Representatives, for further decision making and to determine the follow-up processes.

The Ministry of Education, Culture and Science is also implementing policy aimed at increasing media literacy among young people. At the initiative of the Ministry, the network *Mediawijzer.net* was established, a network of organisations that together develop teaching programmes, issue publications and organise public campaigns. The aim is to help young people, teachers and educators to make more conscious and critical use of digital technology (BZK, 2018a).[135] In its National Digitalisation Strategy, the Cabinet has announced that the approach to media literacy will be evaluated in the summer of 2018, and the House of Representatives will be informed in the autumn (EZK 2018a).

[135] See: https://www.mediawijzer.net/over-mediawijzer-net-2/

Digitalisation in education

The aim of the Cabinet is to improve the quality of education through the use of digital educational technology (EZK 2018a). Over the past few years, work has been undertaken in the Breakthrough Project 'Education and ICT' on improving the parameters with regard to privacy, standards and Internet access. Also, the schools' procurement cooperative Sivon (Samen Inkopen Voor Onderwijs Nederland [Joint Procurement for Education in the Netherlands]) was established. A privacy covenant has also been drawn up, and a number of tools have been developed, including a privacy quick scan and the Social Media Protocol (OCW, 2018).

On 1 February 2018, the new Student Data Pseudonymisation Act came into effect (Netherlands Government Gazette 2018, no. 11). Students using digital resources are given a pseudonym, the aim of which is to better protect the privacy of students (Parliamentary Papers II 2016-2017, 34741, no. 2). Work will also be undertaken in 2018 on new security standards. Over the coming years, the Cabinet has announced in its National Digitalisation Strategy that the Ministry of Education, Culture and Science and the Ministry of Economic Affairs and Climate Policy will be joining the Primary Education Council, the Secondary Educational Council and professionals from education in examining the strategy for digitalisation in primary and secondary education (EZK 2018a).

Disinformation

A new item on the policy agenda for the Ministry of Education, Culture and Science is disinformation and the targeting of news. The Ministry organised round table discussions on these subjects, also focusing attention on independent journalism. The Ministry commissioned an investigation into disinformation and personalisation of news, and the future of independent journalism in the Netherlands.[136] In June 2018, the results of these investigations were shared with the Dutch House of Representatives (Parliamentary Papers 2017-2018 32827, no. 127). Also in June 2018, the Ministry sent a letter to the House of Representatives concerning the spending of resources allocated within the government programme for investigative journalism (Parliamentary Papers II 2017-2018, 32827, no. 126).

[136] In response to the Heerma/Mohandis motion (Parliamentary Papers II 2016-2017, 34550-VIII, no. 82)

Table 14 Overview of activities relating to the societal and ethical aspects of digitalisation, Ministry of Education, Culture and Science, in outline (1 January 2017 - 30 June 2018)

Who/what	Technology	Issue	Action
Curriculum adjustment primary and secondary education	Digitalisation	Digital skills	Digital literacy in the core curriculum of education
Media literacy	Digitalisation, social media, platforms	Digital skills, privacy, security, online interaction	Evaluation of approach to media literacy, autumn 2018
Student Data Pseudonymisation Act	Digitalisation of education	Privacy	Introduction of pseudonyms for students using digital learning resources
Privacy covenant, privacy quick scan, social media protocol	Digitalisation of education	Privacy, digital security	Agreements and standards on data processing and security
Disinformation and personalisation of news	Digitalisation, platforms, social media	Freedom of expression, protection of democracy	Round table discussions and investigations. Letter autumn 2018
Future of media policy	Digitalisation, platforms, social media	Independent news provision, protection of democracy	Additional resources for independent (research) journalism

Source: Rathenau Instituut

5.1.5 Ministry of Foreign Affairs (BuZa)

The Ministry of Foreign Affairs has above all focused attention on digital security. For example the Ministry published an International Cyber Strategy, *Building digital bridges* [*Digitaal bruggen slaan*] (2017).[137] In this International Cyber Strategy, it is stated that the Cabinet actively seeks to promote and strengthen digital security. The coming into force of the European network and Information Security Directive (NIS) is an important step, and one which the Netherlands, among others, actively campaigned for. The Netherlands has identified a number of key priorities:

[137] In this strategy, the Cabinet has met its obligations contained in the Cabinet response to the recommendation from the AIV , *The Internet, a global free space with limited state control* [Het Internet, een wereldwijde vrije ruimte met begrensde staatsmacht]; and the WRR, *The public Core of the Internet. An international agenda for internet governance* [. *De publieke kern van het internet: naar een buitenlands internetbeleid*].

- To promote international investigation in the cyber domain, the Netherlands is encouraging intensification of international cooperation and the strengthening of international legal frameworks.
- To support the international effectiveness of fundamental rights and freedoms, the Cabinet is actively seeking to bring about an international cyber policy for human rights. In international forums and multi-stakeholder platforms, the Netherlands is an active contributor to the further recognition and safeguarding of fundamental rights online, aimed at reversing negative trends that are increasingly restricting Internet freedom in a growing number of countries.
- To achieve protection and recognition of the right to protection of personal data and the right to privacy, the Cabinet is supporting initiatives in various multilateral forums, aimed at safeguarding and recognising the right to protection of personal data and 'respect for the individual's right to privacy' in the digital context.

In May 2018, the Ministry published the *Mensenrechtenrapportage. Actualisering buitenlands mensenrechtenbeleid en resultaten* [Human rights report. Update of foreign human rights policy and results] (BuZa, 2018). This report focuses attention on Internet freedom, freedom of expression, freedom of religion and accountability.

Table 15 Overview of activities relating to societal and ethical aspects Ministry of Foreign Affairs, in outline (1 January 2017 - 30 June 2018)

Who/what	**Technology**	**Issue**	**Action**
International Cyber Strategy	Digitalisation	Digital security	Focus on promoting and strengthening digital security
Human rights report	Digitalisation	Human rights online	Reconfirmation of Human rights letter 2013, Respect and justice for all human beings

Source: Rathenau Instituut

5.2 Dutch Senate and House of Representatives

As the people's representatives, the Senate and House of Representatives play an important role in generating attention for societal and ethical issues with respect to digitalisation. Based on their controlling task, they critically monitor government policy. Appendix 1 provides an overview of the parliamentary questions and motions issued in this field in the period 1 January 2017 - 30 June 2018.

Dutch Senate

The Dutch Senate organised a series of expert meetings about societal and ethical aspects of digitalisation. In 2018, the senators asked experts to explain the stratus of the rule of law, as it is changing due to the influence of digitalisation, and in 2017 called for an explanation of the recording and storage of number plate details by the police and the Computer Crime II Act. They also requested a discussion session with the Intelligence and Security Services Oversight Committee (CTIVD).

The motions submitted on societal and ethical digitalisation issues refer to the latter two bills. There were also calls for an overarching insight into the significance of digitalisation for the safeguarding of public values, see for example the (postponed) motion by senator Duthler on the question 'whether and how the process of digital transformation requires further standards' (Parliamentary Papers I 2017-2018, 34 775 VI, V).

House of Representatives

In the period 1 January 2017 - 30 June 2018, the Dutch the House of Representatives actively enhanced its knowledge of new societal and ethical topics via round table discussions,[138] for example with regard to the dominance of tech companies, the sharing and gig economy and AI in law. These are discussed below, point by point.

Round table discussions

The topics of the round table discussions organised by parliament relate above all to the sharing economy, privacy, and digital security. They are discussed point by point.

- There was a round table discussion on *FinTech* in June 2017, aimed at control of technology and how technology will influence the future of the financial sector. This was followed in January 2018 by a round table discussion on *Cryptocurrencies*.
- In July 2017, a round table discussion on *Data & Analytics,* focused on developments in the field of data analysis specific to the Tax and Customs Administration.
- In November 2017, round table discussions were held on *Work in the platform economy,* focusing on the risks and opportunities of online platforms. In January 2018, this was followed by a further round table discussion, in response to the report *A Fair Share* [*Eerlijk delen*] (2017) by the Rathenau Instituut, focused on safeguarding public interests that play a role in the sharing and gig economy.

[138] In round table discussions, members of the House of Representatives invite (experience-based and other) experts to share their views on a subject on the agenda, answer questions and provide additional comment. Discussions of this type are in principle public, and no record is produced.

- In the round table discussion *Horizontal privacy* in December 2017 – on how citizens interact with regard to the rights and obligations concerning privacy – a discussion took place on whether and how this form of privacy can be better safeguarded.
- In January 2018, a round table discussion took place on *Market dominance of Internet and tech companies*. Points for attention included market access, competition law and the societal impact of the market force of a number of large tech companies.
- The round table discussion on *Cybersecurity* in February 2018 focused on strengthening the resilience of Dutch society to cyber threats.
- In March 2018, a round table discussion was held on *Artificial intelligence in the law,* whereby it was deemed important to determine the boundaries for which decisions in law may be taken by AI, and subject to what conditions.
- Also in March 2018, a round table discussion was held on *Drones*. This focused on a legal and regulatory framework for the use of drones, for example in relation to security, enforcement and privacy.
- In May 2018, a round table discussion was held on Internet companies (including Google and Facebook) and privacy protection.

In the period 1 January 2017 - 30 June 2018, the societal effects of digitalisation were regularly the subject of Parliamentary questions and motions (see Appendix 1). Privacy and digital security are often subjects of discussion in the Dutch House of Representatives.

- In respect of privacy, important subjects are the (unlawful) sharing of
- information, use of data for advertising purposes, the role of social media and the organisation of supervision.
- In respect of digital security, a key topic is how resilient the Netherlands is to cyber attacks, for example with a view to the IoT.
- Relatively new topics are control of technology, justice and autonomy. The House of Representatives wishes to acquire greater insight into algorithms and their possible negative consequences (such as discrimination). As concerns autonomy, questions were asked about persuasive technology (for example in games but also on social media), political micro targeting, the spreading of disinformation and the skills and freedom of choice for consumers.

Furthermore, the House of Representatives demanded attention for the power of platforms, the position of employees and working conditions for employees, with reference to the topic of human dignity and balances of power. A new related topic is the possibility of taxing digital services and platforms. Robotics, biometrics (facial recognition) and augmented and virtual reality were less prominent on the agenda of the House of Representatives, in the period under review.

Also within the House of Representatives there is a clear need for an overarching insight into what digitalisation means for the safeguarding of public values, as reflected for example in the motion by the members Van Dam and Van der Molen in which the government was called upon to arrive at a 'values-driven approach to digitalisation', and to inform the House, and to 'establish an opportunity to be involved in this values development' (Parliamentary Papers 2017-2018, 32761, no. 120).

Table 16 Overview of activities in parliament relating to societal and ethical aspects of digitalisation, in outline (1 January 2017 - 30 June 2018)

Who/what	Technology	Issue	Action
Parliamentary questions and motions	Internet, algorithms, IoT, platforms, digitalisation in general	Attention for all 7 public values (see table 2, chapter 1)	Call for clarification or tightening of policy and legislation and regulations
Round table discussions	Digitalisation, big data and algorithms, platforms, AI	Privacy, digital security, control of technology, justice, balances of power	Knowledge building

Source: Rathenau Instituut

5.3 European Commission

On a European level, the *Digital Single Market agenda* has reflected the strategic ambitions of the European Commission since 2014.[139] On this basis, the Commission is preparing reforms regarding a range of legal frameworks, for example in respect of e-commerce and consumer protection, copyright, audio-visual and media services, telecom, privacy and cybersecurity. Below we discuss a number of the proposals.

[139] See: https://ec.europa.eu/commission/priorities/digital-single-market/#background

E-Commerce and consumer protection

In February 2018, the European Council adopted a regulation aimed at ending geoblocking. Geoblocking prevents online customers from gaining access to products and services from a website in another Member State.[140] In April, the European Commission issued a proposal for a 'new deal' for consumer protection.[141] A new directive will replace four existing directives. The operating principle of the Commission is that the existing regulation must be 'effective' and that better possibilities must be established for enforcement and compliance.

Other legal proposals relate to online purchasing and the provision of services, tax rates, etc.

Copyright and illegal content and online platforms

The European Commission has drafted new proposals for reforming European copyright law.[142] In addition, on 1 March 2018, the Commission adopted a proposal for tackling illegal content on the Internet.[143]

On 26 April, the Commission issued a proposal for a regulation for improving fairness and transparency in interactions between businesses and online platforms.[144] The regulation contains a framework with minimal requirements for transparency and rights of recourse for businesses.

An observatory will also be established for the online platform economy, and there will be a new directive featuring rules on contracts for offering digital content.[145]

Disinformation

In January 2018, the European Commission established the 'High Level Expert Group on Fake News and Online Disinformation' (HLEG). Its task is to advise on policy initiatives for tackling disinformation and online disinformation. The expert group published its final report in March, in which it discusses best practices for tackling disinformation (HLEG, 2018). The expert group calls for

- increasing the transparency of online news
- promoting media literacy;

[140] See: http://europa.eu/rapid/press-release_STATEMENT-18-667_en.htm

[141] See: http://europa.eu/rapid/press-release_IP-18-3041_en.htm, http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-modernisation-of-consumer-protection-rules

[142] See: https://ec.europa.eu/digital-single-market/en/modernisation-eu-copyright-rules

[143] See: https://ec.europa.eu/digital-single-market/en/illegal-content-online-platforms & https://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vki0gceun8zi

[144] See: https://ec.europa.eu/digital-single-market/en/news/regulation-promoting-fairness-and-transparency-business-users-online-intermediation-services

[145] See: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2018)614707

- developing tools to assist users and journalists in countering disinformation;
- monitoring the diversity of the media ecosystem; and
- monitoring the impact of disinformation and evaluating policy measures (EC, 2018a).

On 26 April, the European Commission issued a Communication for a European approach to tackling disinformation.[146] The Commission argued that online platforms must develop a code of practice, with attention for:
- transparency of sponsored content;
- the operation of algorithms; and
- measures for countering fake accounts and automatic bots.

The Commission also wants:
- a European independent network of fact checkers;
- greater media literacy;
- support for Member States in making elections resilient to cyber threats;
- encouragement for voluntary online identification systems.

Finally, the European Commission wants Member States to do more to guarantee the quality of journalism and the diversity of information.

Privacy and digital security
In May 2018, the General Data Protection Regulation (GDPR) came into effect. Over the past period, the European Commission has also been working on a revision of the ePrivacy regulation in respect of privacy.[147] The relevant proposal contains specific privacy regulations for the electronic communication sector, that should for example apply to platforms such as Whatsapp, Facebook Messenger and Skype. The proposal also aims to simplify cookie provisions.

In 2017, the European Commission also submit a bill for the ‘Cybersecurity Act’ (2017/0225/COD), according to which the European Cybersecurity Certification Framework for ICT products and services can be adopted. It also specifies the tasks and functions of the European Network and Information Security Agency (ENISA) with regard to cybersecurity certification.

[146] See: http://europa.eu/rapid/press-release_IP-18-3370_en.htm & https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach
[147] See: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

Audio-visual media services

On 26 April 2018, the European Parliament, the European Council and the European Commission reached initial agreement on the amendment of the Directive on audio-visual media services.[148] The new Directive for example expands the rules for the protection of young people; the Directive is also extended from media services to video services in respect of the spreading of hate. The Directive also aims to strengthen the independence of the relevant watchdogs.

Three priorities

In its mid-term review (May 2017) of the Digital Agenda, the Commission identified three priority areas requiring further action: online platforms, the data economy and cybersecurity.[149] In March 2018, the European Commission issued new proposals for taxing digital companies such as Facebook and Apple throughout the European Union. This proposal will be discussed this year with the European Commission and the Member States.[150] The European Commission is also investigating a number of new policy priorities, including digital skills and AI.[151]

In May 2018, the European Commission launched a communication about AI (EC, 2018c), arising from the statement issued shortly beforehand by 25 European Member States in which they undertook to work together in the field of AI.[152] The communication addresses three priorities:

1. increasing public private investments in the development of AI;
2. preparing for socio-economic changes (such as modernisation of education); and
3. ensuring a suitable ethical and legal framework.

Together with the Member States, the Commission will draw up a coordinated AI plan which is expected at the end of 2018.[153] The draft of the ethical guidelines will also be published at the end of 2018. The European strategy will be elaborated in collaboration with the High Level Expert Group on Artificial Intelligence.[154] The Commission has also launched a European AI Alliance, a forum for discussion in which stakeholders can deliver input for this High Level

[148] See: http://europa.eu/rapid/press-release_IP-18-3567_en.htm

[149] See: https://ec.europa.eu/digital-single-market/en/news/digital-single-market-mid-term-review & https://ec.europa.eu/commission/commissioners/2014-2019/ansip/announcements/statement-vice-president- ansip-press-conference-mid-term-review-digital-single-market-strategy_en

[150] See: http://europa.eu/rapid/press-release_IP-18-2041_en.htm

[151] Other areas are digital industry, ‘high performance computing’, the modernisation of public and egovernment services and healthcare. See: https://ec.europa.eu/digital-single-market/en/policies/shaping- digital-single-market

[152] See: https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence

[153] See: http://europa.eu/rapid/press-release_IP-18-3362_nl.htm

[154] See: https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

Expert Group.[155] In respect of AI strategy, the European Commission is examining legal frameworks for security, responsibility and liability. An expert group has also been appointed to discuss these subjects.[156] This group will assist the Commission in determining whether existing regulations in the European Union are suitable for new technologies such as AI, robotics and the IoT.

[155] See: https://ec.europa.eu/digital-single-market/en/european-ai-alliance

[156] See: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=615947

Table 17 Overview of activities of the European Commission concerning the societal and ethical aspects of digitalisation, in outline (1 January 2017 - 30 June 2018)

Who/what	Technology	Issue	Action
E-commerce and consumer protection	Digitalisation, social media, platforms	Privacy, autonomy, justice, balances of power	Including modernisation of consumer law and geoblocking
Copyright, illegal content and platforms	Digitalisation, social media, platforms	Privacy, autonomy, justice, balances of power	Proposals on copyright, illegal content, relationship between platforms and businesses, digital content
Disinformation	Digitalisation, social media, platforms, persuasive technology	Autonomy (manipulation, freedom of expression), protection of democracy	Expert group on fake news and disinformation; advice on policy initiatives; Communication on policy proposals to tackle disinformation
Privacy and digital security	Digitalisation, IoT social media, platforms	Privacy, security	GDPR 25 may 2018 in effect, ePrivacy – negotiations Cyber Security Act
Audio-visual media services	Digitalisation, social media, platforms	Security, autonomy, independent news provision, pluralism of media range	Revised Directive including expanded rules to video services, strengthening of independence of watchdogs

Source: Rathenau Instituut

5.4 European Parliament

Within the European Parliament, too, there were numerous developments on these themes in the period 2017-2018. Here we refer to a number of notable developments, in particular adopted resolutions.

The European Parliament (EP) adopted the resolution Civil Law Rules on Robotics (2015/2103/INL), with recommendations to the European Commission about civil rights with regard to robots. The members considered it essential that a guarantee be provided that people always have control over intelligent machines, when working with robotics and IA. The parliament also emphasised that a clear, strict and efficient guiding ethical framework is needed for the development, design, production, use and adaptation of robots.

In its resolutions, the European Parliament focused much attention on the relationship between platforms, balances of power and human rights. According to the European Parliament, digital platforms and services offer new opportunities on the market, as well as challenges to society:

- In the resolution *Towards a digital trade strategy* (2017/2065(INI)), it does so in respect of digital trade and safeguarding consumer rights and human rights.
- The resolution *The digitalisation of European industry* (2016/2271(INI)) from June 2017 calls for a strategy that tackles 'the most urgent economic and societal challenges for Europe' arising from digitalisation.[157] Here the European Parliament focuses attention on the societal consequences of the sharing economy. In that respect, separate resolutions were adopted in June:
  a. the European agenda for the sharing economy (2017/2003(INI));
  b. and Online platforms and the digital single market (2016/2276(INI))

  These resolutions call for a fair competitive position for companies, consumers and other bodies with regard to the sharing economy.

Another important public value for the EP was justice, in particular the position of women. In two resolutions, the European Parliament referred to the position and opportunities for women online and of women in digital sectors, respectively (EP, 2017/2210(INI); 2017/3016(RSP)).

Finally, the European Parliament adopted resolutions on privacy and data protection:

- *The fight against cybercrime* (2017/2068(INI)), October 2017;
- *The consequences of big data for fundamental rights* (2016/2225(INI)), March 2017;
- *A European strategy for cooperative smart transport systems* (2017/2067(INI)), March 2017;
- *Resolution of the European Parliament on the suitability of the protection offered by the EU-US privacy shield* (2018/2645(RSP)), June 2018.

[157] See: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0183+0+DOC+XML+V0//NL

Examples from abroad
Much is also happening abroad in the field of societal and ethical digitalisation. Here we mention a number of notable examples.

- **Japan** introduced a statutory five-yearly science and technology strategy (5th Science and Technology Basic Plan, 2016-2020). In this strategy, under the heading ‘Society 5.0’, it introduced a vision for a sustainable, affluent and inclusive future thanks to technology. With its strategy, Japan hopes to be able to offer solutions for societal problems, such as low birth rates and the ageing population. To make this possible, breakthroughs will have to be achieved in five areas, including the way in which government works, in respect of legal affairs, in the field of technology, as regards the availability of human capital and in the field of social acceptance of technology.

- In the **United Kingdom**, a British parliamentary committee published an AI Code for developers and users of intelligent systems in its report. The code is aimed at the ethical implications of AI (Authority of the House of Lords, 2018). To ensure the safe and ethical use of AI in the United Kingdom, and to maintain a solid worldwide position in this field, the Committee proposed five principles: 1) AI must be used for the benefit of society, 2) AI must be based on fairness and explainability, 3) AI must not be used to reduce privacy or the data rights of individuals, families or communities, 4) all citizens are entitled to education so that they can thrive mentally and emotionally, and 5) the autonomous power of hurting, eliminating or misleading people may never be granted to AI. The country has now also announced an AI Sector Deal to promote investments in AI.[158]

- On 29 March 2018, **France** introduced an AI strategy ‘AI for humanity’, with the aim of making France the European leader in the field of AI, and building an AI ecosystem in Europe (Villani, 2018). The strategy consists of six spearheads: building up a data-oriented economic policy, investing in French AI research, using AI for sustainability, the ethical aspects of AI, and inclusive AI. To secure the ethical aspects, the report recommends the establishment of an ethical committee. As part of the AI strategy, President Macron wishes to invest 1.5 billion euro in French AI research

- Since 1 January, the ‘Netzwerkdurchsetzungsgesetz’ (Network Enforcement Act) has been in force in **Germany**. This law requires social media to take measures to prevent unlawful spreading of hate on its platforms. The platforms are required to delete hate-spreading content on pain of a fine (Article 1 G. v. 01.09.2017 BGBl. I S. 3352, no. 61). In addition, the ethical committee for the

[158] See: https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal

German Ministry of Transport and Digital Infrastructure has formulated ethical guidelines for autonomous vehicles (BMVI 2017). These guidelines for example deal with situations in which damage is unavoidable, the availability and protection of data, the interaction between man and autonomous cars and the broader implications of autonomous cars. Security is an essential principle for these guidelines, alongside non-discrimination. According to the guidelines, the cars are not permitted to discriminate in the event of an unavoidable accident on the basis of personal characteristics (race, gender, or mental state).

Table 18 Examples from abroad of activities undertaken in relation to the societal and ethical aspects of digitalisation (1 January 2017 - 30 June 2018)

Who/what	**Technology**	**Issue**	**Action**
United Kingdom – AI code	AI	Privacy, security, control of technology, justice, human dignity, inclusion	5 principles for an AI code for shaping developments and mitigating the risks of AI
France – AI-strategy	AI	Control of technology, human dignity, balances of power, inclusion	AI-strategy: e.g. data based economic policy, effects on labour market and ethical aspects of AI (establishing ethics committee)
Germany – Network Enforcement Act	Social media	Security	Act obliges social media to take measures to counter criminal spreading of hate
Germany – Ministry for Transport and Digital Infrastructure	Autonomous cars	Safety, control of technology, justice	Ethical guidelines from the ethics committee for autonomous cars
Japan – Society 5.0	IoT, big data, AI, robotics, platforms	Quality of life, sustainability, ethical aspects	Five-yearly science and technology strategy, e.g. ethical aspects of technology

Source: Rathenau Instituut

5.5 Conclusion

Ethics and fundamental rights on the national policy agenda
In *Urgent Upgrade*, we above all saw such issues as privacy and digital security on the policy agendas of various Ministries. There was little attention for an overarching vision on the significance of digitalisation. In the period 1 January 2017 - 30 June 2018, this situation changed. A whole raft of societal and ethical questions is now clearly on the agenda.

With the arrival of a new Cabinet, a series of national agendas were announced during the first half of 2018, including the overarching National Digitalisation Agenda in June and the intention to release a series of policy documents in the second half of 2018 (including documents about open source, horizontal privacy, media literacy and AI in the administration of justice). In the published agendas, ethics and fundamental rights are an integral element of the policy spearheads. Societal and ethical questions are therefore clearly on the national agenda. In the agendas, the Cabinet emphasises that society is facing a period of transition, with positive and negative aspects, and that digitalisation is no longer just a question of implementation but for 'boardroom discussion' (BZK 2018b, 2).

Privacy and digital security
Since 2017, on a national level, there has also been considerable attention for privacy and digital security. As regards privacy, legislation has long been in place. On 25 May 2018, the European General Data Protection Regulation (GDPR) came into effect. A series of new policy measures have been announced in the field of digital security. In this field, the shift has been made from agenda shaping to political decision making. In the Netherlands, for example, the Cybersecurity Act has been adopted, and a Digital Trust Centre was established for the SME sector, to increase the volume of knowledge and information exchange (in the past, a similar centre was only available for 'vital' sectors) and a roadmap has been laid down for secure hardware and software, with specific measures to improve the security of IoT devices.

Investigation of new themes
New subjects have also been placed on the policy agenda, such as the spreading of disinformation, the influence of digitalisation on democracy, the influence of algorithms, fundamental rights, digital skills and balances of power. In these respects, policy development is still in the investigative phase. Across a broad range, the Cabinet has announced new investigations, or is in the process of investigating the situation. Examples are investigations into the use of algorithms within government, research into digitalisation of democracy and research into the significance of AI and the protection of public values.

Statutory frameworks

In a number of areas, the Cabinet is investigating the extent to which existing legal frameworks are adequate, and whether changes are needed. For example, the Cabinet has commissioned an investigation of the extent to which current competition regulations are still adequate. There is also a desire to examine the relationship between blockchain and the law, and to determine whether the legal framework for implementing and using data analysis requires further strengthening (Parliamentary Papers II 2016-2017, 266423/32761, no. 426).

Senate and House of Representatives

The Dutch parliament has often considered privacy and digital security. New topics have also been placed on the agenda of the Senate and House of Representatives, such as control of technology (transparency of algorithms), justice (discrimination by algorithms), autonomy (about disinformation, political microtargeting and freedom of choice) and human dignity and balances of power (position of sharing and gig platforms, employee conditions and the power of tech companies).

Via round table discussions and meetings of experts, the Senate and House of Representatives are actively acquiring knowledge of new societal and ethical digitalisation issues, for example in the field of digitalisation and the administration of justice, data analytics and the sharing and gig economy.

International level

Digitalisation and its societal and ethical aspects are clearly on the agenda at the European Commission. On the basis of the Digital Single Market Agenda, the Commission is preparing reforms of a whole range of legal frameworks, including those governing the relationships between businesses and platforms, consumer rights, geoblocking, copyright, audio-visual and media services, illegal content, privacy and digital security.

New topics for the Commission are the spreading of disinformation, liability issues with respect to new technologies and AI. The data economy and cybersecurity are other key priorities at the European Commission.

6 Politics and administration: Supervisory bodies

The key element of the policy implementation phase is that regulators and supervisory committees ensure that the rules, standards and laws are implemented and complied with. A regulator is an independent and impartial body appointed by government to ensure compliance with legislation and regulation, by various organisations. In this chapter we discuss the national regulators relevant to the societal and ethical aspects of digitalisation, and other organisations such as the National Ombudsman and the National Cyber Security Centre.

Among many of the regulators, we have observed a growing awareness of the societal and ethical aspects of digitalisation, for example with regard to media and advertising, the financial markets and the market power of platforms. A number of regulators have become focused on the significance of digitalisation for their domain or are currently acquiring new knowledge. In the period 2017-2018, the mandate of a number of regulators was extended or adjusted, in combination with a rise in budget or capacity.

6.1 Netherlands

Dutch Data Protection Authority

The Dutch Data Protection Authority (AP) is responsible for ensuring compliance with privacy legislation and advises on new laws and regulations. In 2017, a key topic for the AP was new EU privacy legislation in the form of the GDPR, which came into effect on 25 May 2018. The AP released a great deal of information about the imminent legislation[159] and carried out an internal reorganisation with a view to the expansion of tasks and authorities (AP 2018). Since 25 May 2018, the AP has for example been required to process any complaints received from individual citizens. At the end of June 2018, the AP reported that since the introduction of the new law, 600 people had submitted complaints regarding privacy.[160] The new regulation has also increased the authority of the organisation to impose fines, and the number of staff at the regulator has grown. In 2018, the

[159] See for example: https://autoriteitpersoonsgegevens.nl/nl/nieuws/start-campagne-privacy-gaat-iedereen-wat-aan
[160] See: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ruim-600-mensen-dienen-privacyklacht-bij-ap

Cabinet intends to increase the budget of the AP by 5 million euro, and in 2019 by a further 2 million euro (Parliamentary Papers II, 2017-2018, 26643, no. 529).[161] no. 529).[161]

In addition to the GDPR, other key topics for the AP in 2017 were transparency in profiling, the processing of special personal data, and the security of personal data (AP, 2017a). In respect of the latter point, the AP called upon Airbnb to halt the use of Citizen Service Numbers (BSN). Airbnb now automatically deletes the BSN from all digital copies of identification documents, and has removed all BSNs from previously collected identification documents.[162] During the course of 2017, the AP issued recommendations on proposed legislation such as the Basic Registration of Persons Act (BRP) (AP, 2017b), the Passenger Names Register Act (PNR) (AP, 2017c), the Payment Services (PSD2) Directive Implementation Act (PSD2) (AP, 2017d), and the Cybersecurity Act (AP, 2017e).

The use of personal data by social media also attracted the attention of the AP. In 2017, together with a number of other regulators across Europe, the AP investigated the processing of personal data by Facebook. The investigation revealed that Facebook had failed to provide users with full information about the use of their personal data. The AP also concluded that Facebook makes use of special details of a sensitive nature, without the explicit consent of the users. For example, the platform processed the data about sexual orientation with a view to supplying targeted advertisements, on that basis. Facebook has now put an end to this practice (AP, 2017). Following the reports about Cambridge Analytica, a working group of European regulators, including the AP, announced their intention of examining the way in which social media platforms obtain their data and how they prevent others from gaining unlawful access to that data, in 2018.[163]

Authority for Consumers and Markets

The Authority for Consumers and Markets (ACM) is responsible for monitoring competition, telecommunication and consumer rights. In 2016-2017, one of the spearheads of the ACM was 'Digitalisation – the online consumer'. The focus of this spearhead was preventing problems with regard to competition and consumers on the Internet and monitoring businesses that use personal data to strengthen their power position on the Internet. In 2018-2019, the digital economy remains a key agenda item.[164] In particular, the ACM plans to focus on a sound and open

[161] In 2017, the consultancy firm Andersson Elffers Felix investigated the capacity and resources required by the AP in the future. It developed three scenarios for the expected additional budget (on top of the current budget of 7.7 million): low 12 million, medium 16 million, high 22 million (Parliamentary Papers 2016-2017, 32761, no. 112).

[162] See: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-airbnb-be%C3%ABindigt-verwerking-bsn

[163] See: https://autoriteitpersoonsgegevens.nl/nl/nieuws/europese-privacytoezichthouders-trekken-samen-op- aanpak-social-media

[164] See: https://denkmee.acm.nl/thema/digitale-economie?status=inactief

infrastructure for a rapid and affordable Internet, the power of business based on the use of data and algorithms, and clear information and freedom of choice for online consumers (see also *Het Signaal 2018* published by ACM).

Within its strategy, ACM focuses on three spearheads, namely:

4. investing in knowledge about the functioning of digital markets;
5. actively following developments; and
6. aiming for international and national cooperation (ACM, 2018).

ACM also intends to establish a special digital competition team (Government Programme 2017-2021; EZK 2018a). Together with other European regulators, the ACM took a close look at the general terms and conditions of social media platforms, for example relating to the right to withdraw from a purchase and the recourse to local courts rather than the American courts. A number of platforms have adapted their general terms and conditions to the satisfaction of the regulators, while others have promised to make the necessary changes.[165] Together with the Dutch Media Authority (CvdM), the ACM also investigated the digitalisation of the news, during the course of 2018 (see below).

Human Rights Commission

The aim of the Human Rights Commission (CRvdM) is to protect human rights in the Netherlands (including the right to equal treatment), to broaden awareness of our rights, and to promote compliance with those rights.[166] In its strategic plan 2016-2019, the Commission made no reference to the way in which technological developments affect human rights. As a result there is no separate report about digitalisation and human rights.

Wherever relevant, however, the Commission does consider the consequences of digitalisation for human rights, for example with regard to access to information. As a regulator charged with supervising compliance with the UN Charter on the rights of the disabled, the Commission focuses on disabled people who are not able to participate fully in society. One of the tasks of the Commission is to increase awareness of this situation. In this respect, the Commission considers the right to access to information, for example with regard to the digital accessibility of websites for disabled people on the basis of the Equal Treatment Act and the UN charter, and for the elderly.[167] In its report on access to elections for disabled people (CRvdM, 2017a), the Commission argued that digital voting in polling stations could be seen as a solution. In its recommendation (CRvdM, 2017b), in response to the

[165] See: https://www.acm.nl/nl/publicaties/social-mediaplatforms-google-facebook-en-twitter-passen-algemene-voorwaarden-aan-onder-druk-europese-toezichthouders

[166] Human Rights Commission Act (Netherlands Government Gazette 2011, 573)

[167] There is for example a report about municipal websites: https://mensenrechten.nl/publicaties/detail/35682

‘Generic digital infrastructure’ bill, the Commission argued that access to digital information is of significant importance to disabled people, and that accessibility (which also applies to digital accessibility) is one of the basic principles embodied in the UN charter.

There is also constant reflection between the Commission and other regulators such as the AP and the National Ombudsman, who are also members of the Commission’s own Advisory Council. Finally, the Commission’s budget was not enlarged in the period 2016-2018 specifically with regard to digitalisation but instead new tasks relating to the UN charter were added.

Review Committee on the Intelligence and Security Services

The Review Committee on the Intelligence and Security Services (CTIVD) reviews the activities of the General Intelligence and Security Service (AIVD) and the Defence Intelligence and Security Service (MIVD). It investigates the legality of operations and data collection by the security services, and is called in as an independent advisory committee whenever complaints are submitted about the actions of the security services (CTIVD, 2017). The key subjects of investigation by the CTIVD include the balance between national security and protection of civil rights, transparency, and social debate. In its independent role, the CTIVD plans its oversight activities on the basis of these subjects. As a consequence, such subjects as ‘bulk cable interception’,[168] automated data analysis and data reduction will be of key importance.[169]

As a consequence of the introduction of the Intelligence and Security Services Act 2017 (Wiv, 2017), the mandate of the CTIVD has changed. When the Wiv 2017 came into effect, the CTIVD was divided into a monitoring department and a complaints handling department, with binding rights of complaint. Its oversight task remains unchanged, and comprises non-binding post-event review. The budget of the CTIVD was enlarged in 2016 and further enlarged in 2018, in view of the introduction of the Wiv 2017. This increased budget accommodates expanding the staff of the CTIVD, with new staff taken on to man the complaints handling department, and for the formation of an ICT unit.

Following the introduction of the Wiv 2017, the CTIVD will be responsible for the intensive oversight of the activities of the AIVD and MIVD, in particular with regard to the (targeted nature of) new authorities, such as bulk cable interception, the process of responsible data limitation during the processing of data, and the use of new technologies.

[168] This relates to the collection and filtering of data collected via the Internet (the cable); in the past, the services were only able to intercept Internet traffic via the ether.

[169] Interview with Frank Brasz of the CTIVD on 4 April 2018.

An important extension of responsibilities within the Wiv 2017 is the statutory duty of care of the services for the quality of data processing (article 24 of the Wiv 2017). This duty of care also applies to the algorithms and models used by the services. The newly established ICT unit will play an important role in this supervisory task. Within this unit, knowledge has been assembled of the work processes of both intelligence services, of the technical resources used by them, and more generally of data analysis processes and cyber and Internet technology.[170]

Authority for the Financial Markets

The Dutch Authority for the Financial Markets (AFM) is an independent body that supervises the conduct of the financial markets with a view to ensuring honesty and transparency within the financial markets so that the public, businesses and government have trust in those markets.[171] Technological developments are also bringing about changes in the financial markets and financial businesses, for example through internationalisation and digitalisation. An agenda spearhead for 2018 at the AFM is a sharper focus on supervising technology and data, and the inherent risks of technology within the financial sector (AFM, 2018a).

Since the start of 2016, the AFM has been operating the so-called Innovation & Fintech programme, aimed at the provision of support for technological innovation in the financial sector, in as far as it contributes to the sustainable financial prosperity of the Netherlands (AFM, 2017a). During the course of 2017, the AFM issued repeated warnings about the hype concerning Initial Coin Offerings (ICOs) and crypto currencies, because to a large extent these products are beyond the scope of supervision, their exchange rates fluctuate wildly and the market is susceptible to fraud, money laundering and price manipulation (AFM, 2017b). At the start of 2018, the AFM warned about the gamification of financial products, a trend according to which often very high-risk financial products are offered using aggressive persuasion techniques commonly used in the online gaming and gambling industry. The providers concentrate on young people, for example by offering free demos or the use of celebrities to promote a product (De Waard & Haegens, 2018). In 2018, the AFM has focused more specifically on data-driven supervision so as to offer consumers and investors better protection against high-risk financial products, abusive practices and market abuse (AFM, 2018b).

Radio Communications Agency

The Radio Communications Agency Netherlands (AT), part of the Ministry of Economic Affairs and Climate Policy, is responsible both for implementing and supervising legislation and regulations in the field of telecommunication, and guarantees the availability and reliability of the IT and communication networks in the Netherlands, by undertaking investigations and monitoring developments.[172]

[170] Idem.
[171] See: https://www.afm.nl/nl-nl/over-afm
[172] See: https://www.agentschaptelecom.nl/over-agentschap-telecom/organisatie

For example, the AT is regulator for the system of agreements on electronic access services (ETD system) and from May 2018 onwards will also act as watchdog for the Cybersecurity Act on behalf of the Ministry of Economic Affairs and Climate Policy in respect of the power supply and telecommunication.[173]

Given the technological developments, the AT is responsible for the security and use of the digital infrastructure. A new challenge identified by the AT is safeguarding trust in the digital environment. Another new task of the AT since 2016 is supervision of the security and reliability of electronic trust services such as electronic signatures, electronic stamps, digital delivery services and website authentication. These electronic trust services make an important contribution to a reliable digital society (Radio Communications Agency, 2017).

The AT is also in discussion with the Ministry of Interior and Kingdom Relations on structuring the system of supervision according to the Digital Government Act, that is due to be introduced in January 2019, with regards to the functioning, security and reliability of the system of electronic identities, including eHerkenning [eRecognition] – login model for businesses in interacting with government) and DigiD (the login tool for citizens). Finally, the AT is calling for broader authority pursuant to the Radio Equipment Directive with regard to the reliability of security software for IoT devices. In the Roadmap for Secure Digital Hardware and Software (EZK 2018b), the Cabinet has undertaken to investigate how this can be achieved.

The AT is also collaborating with the National Cyber Security Centre and the Digital Trust Centre, and for years has actively collaborated with the ACM; the result is a growing number of interfaces in the field of digitalisation and cyber activity (in particular through the digitalisation of telecommunication). The capacity of the AT has also been extended for electrical services and the Cybersecurity Act.[174]

Dutch Media Authority

The Dutch Media Authority (CvdM) is responsible, among others, for supervising compliance with the Media Act 2008, according to which the Authority protects the independence, plurality and accessibility of the audio-visual media in the Netherlands.[175] The Authority has identified two strategic topics in its supervision statement for 2018:

[173] The ETD system is a system of agreements in which a variety of providers of authentication tools and services, such as eHerkenning [eRecognition], all participate. It ensures that public and private organisations are able to guarantee secure and user-friendly access to digital services.

[174] In total, staffing for eIDAS and ETD amounts to approx. 13 FTE. As soon as supervision takes on more structure pursuant to the Cybersecurity Act, this can be extended to between 25 and 30 FTE.

[175] See: http://wetten.overheid.nl/BWBR0025028/2017-02-01

1. **the online domain;**
   Supervision of the online domain was a focus of attention in 2017, and in 2018 will increasingly become an integrated element of regular supervision activities.
   The Agency aims to protect the plurality and independence of online media services. Together with the ACM, for example, the Agency examined the digitalisation of news (CvdM & ACM, 2018). The report by the regulators noted that to date, the Netherlands has experienced few problems with the spreading of disinformation, but that the impact of this problem must be taken seriously. With that in mind, CvdM and ACM are already investigating possible measures such as investing in the diversity and sufficient numbers of quality news providers.
   Another key topic in the online domain is greater transparency with regard to commercial influencing. In 2017, the focus was on self-regulation (see e.g. CvdM 2017a).[176] At the end of 2017, in collaboration with a group of YouTubers, the Agency established a code containing agreements that should result in greater transparency about advertising in videos (CvdM, 2017b). In 2018, the CvdM will continue to monitor the operation of this code.

2. **independence of the media**
   The Agency monitors the independence of the media. Because of the relentless growth of online media, just like in respect of traditional media, there must be clarity on the presence of commercial or political influencing. According to the Agency, as far as possible, media institutions must take their own responsibility for the governance and internal management of their organisations (CvdM, 2017a). Policy rules in this area came into effect on 1 January 2018, and monitoring those rules is an important point of focus for the supervision by the Agency in 2018.
   Finally, together with a number of other supervisory bodies – the ACM, the AP, the AT and the Advertising Code Authority – the Agency is working to encourage effective supervision (CvdM, 2017c; CvdM, 2017d).

[176] Video services are currently often beyond the frameworks of the Media Act. This is expected to change when the new European Directive on Audio-Visual Media Services comes into effect. At that point, the Agency will also have more possibilities for calling online video services to account for the mixing of editorial and commercial activities (Supervision Statement 2017 CvdM).

Table 19 Overview of developments at regulators, in outline (1 January 2017 - 30 June 2018)

Who/what	Technology	Issue	Action
AP	Digitalisation	Privacy, data protection	Supervision of data processing by government and businesses: extended mandate and capacity, supervision of GDPR
ACM	Digitalisation, platforms	Privacy, autonomy, balances of power	Power of Internet providers, digital economy, network neutrality legislation; establishment of digital competition team
CRvdM	Digitalisation	Human rights (special focus discrimination), inclusion	Recommendation on Generic digital infrastructure
CTIVD	Digitalisation	Privacy, security	Supervision of security services; changing mandate following introduction of Wiv and increased budget
Authority for the Financial Markets (AFM)	Fintech, big data and algorithms, persuasive technology	Autonomy, control of technology	Contributing to sustainable financial welfare, warnings about crypto currencies and gamification of investment
Radio Communications Agency	Digitalisation, IoT	Digital trust, cybersecurity	Safeguarding digital trust, reliable telecommunication; extended mandate and extended capacity
Dutch Media Authority	Digitalisation	Independence, plurality and accessibility of media, freedom of information	Transparency regarding advertising: media institutions must take responsibility through self-governance

Source: Rathenau Instituut

Other regulators and supervisory committees
The **National Cyber Security Centre**[177] (NCSC) responds to cyber threats and incidents and works to strengthen a secure and resilient digital society. A key point of focus is the protection of the information society against cybercrime. In the *Cybersecurity Assessment Netherlands 2017: Digital resilience of the Netherlands lagging behind the increasing threat* [*Cybersecuritybeeld Nederland 2017: Digitale weerbaarheid Nederland blijft achter op groeiende dreiging*] (2017a), the NCSC argues that cyberattacks are attractive, and the development of the IoT is also a source of potential risks. According to the NCSC, over the coming years, further investment will be needed to increase the digital resilience of the Netherlands.

The NCSC also aims to boost awareness and capacities in the field of information security and privacy among citizens, businesses and government. The Cybersecurity Act, for example, offers a framework for the way in which the NCSC should handle confidential information, and forms the legal basis for the tasks and authorities of the NCSC (NCSC, 2017b).

In 2017, the NCSC published its ICT security guidelines for mobile apps, as a guideline for the more secure development, management and provision of apps for mobile devices (NCSC, 2017c). The Cyber Security Council (already discussed in ‘Agenda shaping’) is responsible for supervising the NCSC Strategy. Finally, over the past few years, the capacity of the NCSC has been significantly expanded (a process that is set to continue over the coming years), while the NCSC budget has been rising for a number of years. This will continue during the current Cabinet period. A proportion of the 95 million euro reserved by the Cabinet for cybersecurity in the government programme has been earmarked for the NCSC.

The **National Ombudsman** helps citizens in dealing with problems with government, and informs government authorities on how they can improve their services. One of the themes on the research agenda for 2018 is ‘digitalisation’. The Ombudsman has noted that given the high pace of digitalisation within government, the relationship between individual citizens and the government and the way in which citizens and government communicate with one another have been clearly influenced (the National Ombudsman, 2018). According to the Ombudsman, the government must make citizens the central point of focus in the digitalisation process, for example emphasising that government must take responsibility for ensuring that accessibility is safeguarded, so that citizens can continue to participate in society, and no one is excluded. The Ombudsman has also argued that government must be solution-based and user-friendly, and must take responsibility for the structure and implementation of the process of service provision.

[177] In formal terms, the NCSC is not a regulator.

Within the topic of digitalisation, in 2015-2017, the National Ombudsman investigated digital government, the blue envelope (Tax and Customs Administration) and MijnOverheid (digital government portal) and the digitalisation of the Employee Insurance Board (UWV), the Social Security Bank (SVB) and the Education Implementation Service (DUO). One clear observation was that digitalisation should not result in reduced access to government (the National Ombudsman, 2017). Recently, the Ombudsman has focused on investigating 'data links/big data', focusing on the way in which the use of big data is guaranteed, from the perspective of the citizen. For example, the organisation investigated the use of digital forms and the possibility of cancelling the digital identity of individuals following death.

An investigation is also planned into what citizens can expect from government when it comes to respecting privacy in applying for services (the National Ombudsman 2018).

The budget available to the Ombudsman was cut severely during the Cabinets Rutte I and Rutte II. This effect will be reversed this year, and the budget will be increased. There is no additional mandate for activities with regard to the theme digitalisation.

The **Dutch Advertising Code Authority** (SRC) is the body dealing with the self-regulation of advertising. It is an initiative by companies that use advertising. To ensure (socially) responsible advertising, the Authority is active in the field of proactive service provision (encouraging advertisers to develop campaigns that satisfy the rules) on the one hand, and regulations and the complaints procedure on the other.

The Dutch Advertising Code contains rules that all advertisements must satisfy, including advertisements that are distributed digitally. According to the Code, advertisements must always be recognisable and may not be misleading or be in violation of the law or untrue or at odds with good taste and decency. The Dutch Advertising Code also includes specific rules for example for advertisements via social media and email. The Advertising Code Authority, an independent body for handling complaints, tests the responsibility of advertisements, according to the Dutch Advertising Code. If a party disagrees with the judgement, appeals can be submitted to the Board of Appeal. In December 2017, in response to a complaint, the Board of Appeal censured one of the large tech companies. In a newspaper advertisement, Google had claimed that consumers were able to deactivate the setting 'remember my Internet searches' in the privacy portal, so that Internet searches would no longer be remembered. Google undertook to keep this promise.

The Board of Appeal, however, judged that this was not the case, and that consumers had been poorly informed. In reality, it is not possible to select to have no record made of a search. Google still keeps certain data from all searches, even if the user has opted to switch off this function. According to Google, the data in question are those required by the company to investigate statistical trends, to prevent typing errors and to optimise its services.[178]

Geonovum is a government-financed foundation that grants access to geo-information from the public sector[179], develops relevant standards and assists the government in making better use of geo-information. Geonovum acts as the link between policy and implementation in establishing the national geo-information infrastructure. [180]

The multiyear strategy of Geonovum for the period 2017-2020 reflects a focus on continuing digitalisation and the related role of location data. More data are available than ever, the geo-information landscape is becoming increasingly rich and complex, and location data are ever more commonly used for profiling. The location data services sector is one of the fastest-growing sectors worldwide, and with its knowledge and capital is the driving force for the development of geo-information technology.

In 2017, Geonovum published the *Verkenning locatiegegevens en sociale platforms* (2017a) [Review of location data and social platforms]. The organisation aims to focus more on sharing geo-information on the web, by working on improved findability of public geo data on the web. Location information is also essential for smart city applications. Real time data are used to improve mobility. According to Geonovum, the smart use of an information system is one of the ways to make government more efficient in improving quality of life, mobility and security in urban areas. With that in mind, the foundation has drawn up a set of practical tools and rules of play.[181]

In 2018, Geonovum will be adapting its governance structure for geo standards, and publishing a multiyear plan for geo standards in the form of a roadmap. This will be an extension of the white paper on geo standards published in 2017 (Geonovum, 2017b).

[178] The full judgement can be read here: https://www.reclamecode.nl/webuitspraak.asp?ID=189633&acCode

[179] This relates to information with a location component, for example a building or a canal, or sensor measurements carried out at a particular location.

[180] See: https://www.geonovum.nl/over-geonovum/waar-wij-voor-staan

[181] See: https://meteninhetopenbaar.locatielab.nl/

Table 20 Activities in policy implementation, other organisations, in outline (1 January 2017 - 30 June 2018)

Who/what	Technology	Issue	Action
NCSC	Digitalisation	Security, privacy, information security	Encouraging a secure and resilient digital society; expanded budget
National Ombudsman	Digital government services	Autonomy, human dignity, digital accessibility, responsibility	Complaints concerning errors by digital government systems, big data, digital identity; reduced budget Rutte I and Rutte II reversed
Advertising Code Authority	Digitalisation	Responsibility	Supervising the responsible making of advertisements
Geonovum	Geo-information; sensor data regulation	Accessibility, standardisation	Granting access to geo-information for public sector/government

Source: Rathenau Instituut

6.2 International

The **European Data Protection Supervisor** (EDPS) advises the European Commission and the European Parliament on legislation and policy in the field of privacy and data protection, and works alongside national regulators and supervisors to arrive at uniform data protection. The EDPS strategy 2015-2019 *Leading by example* consists of three main spearheads:

1. '*data protection goes digital*': promoting technologies that strengthen privacy, promoting cross-disciplinary policy solutions and increasing transparency, user control and accountability;
2. establishing worldwide partnerships in which
   a. data protection also acquires an ethical dimension;
   b. data protection becomes mainstream in international politics; and
   c. more uniformity is achieved in the EU;
3. a new chapter in European data protection among others by implementing up-to-date regulation and increasing the accountability of EU organisations (EDPS, 2015).

In the light of this strategy, the EDPS established an ethical advisory committee in 2015, to investigate the relationship between human rights, digital technology and business models in the 21st century.[182] In 2018, the advisory committee's final report was published (EDPS 2018a). This publication discusses the debate concerning digital ethics and how technology can contribute to human dignity. The report identifies the following principles:

1. human dignity must remain inviolable in the digital age;
2. personality and personal data are indivisible;
3. digital technologies engender the risk of weakening the foundations of democracy;
4. digital data processing encourages new forms of discrimination such as profiling; and
5. the 'commodification' of data (data becoming a commodity) is shifting the value from persons to personal data.

The EDPS also advised on the new proposed legislation from the European Commission, including the GDPR, the ePrivacy regulation (EDPS, 2017a; 2017b), the Schengen Information System (EDPS, 2017c) and systems for police cooperation (EDPS, 2017d).

The European supervisor also published an opinion on online manipulation and personal data (ETGB, 2018b), in which it explained that the existing complex ecosystem of digital information makes it possible to manipulate people and political processes. According to the ETGB, any effective approach requires cooperation between various policy domains and regulators, including data protection regulations, competition legislation, consumer law and regulations in the field of elections.

Finally, in 2017, the European regulator started the '*Big data & Digital Clearinghouse*', the aim of which is to bring together the regulators from the domains referred to above. The Clearinghouse is for example responsible for examining fake news and voter manipulation, the emergence of 'attention markets' and the opacity of algorithms.

[182] See: https://edps.europa.eu/sites/edp/files/publication/15-12-03_ethical_dimensions_nl.pdf

Table 21 Overview of developments at regulators, international, in outline (1 January 2017 - 30 June 2018)

Who/what	Technology	Issue	Action
EDPS	Digitalisation (services processing personal data), big data	Broadening from privacy to autonomy, human dignity, discrimination, data protection	Advisory group on digital ethics, investigating the impact of digitalisation on human rights, supervision of GDPR

Source: Rathenau Instituut

6.3 Conclusion

Greater attention for ethical aspects of digitalisation among more regulators
The awareness of societal and ethical aspects of digitalisation has grown among practically all regulators, for example in respect of media and advertising, the financial markets, the market power of platforms and large tech companies, and digital security. Many regulators are now investigating the significance of digitalisation for (new) aspects of their field of expertise and their own role in that process, and in building up new knowledge and expertise. At some regulators, this is resulting in new spearheads for supervision, for example at the Authority for the Financial Markets, that will be focusing more specifically on the use of data in the financial sector.

In the period 1 January 2017 - 30 June 2018 we also observed a broader or adapted mandate among the various regulators, in response to adapted and new legislation, resulting in increased budgets or capacity.

New collaborative ventures
Because digitalisation is a field that affects a variety of different regulators, it is also important that those regulators work together. As compared to the period of *Urgent Upgrade*, we have seen the emergence of a number of new collaborative ventures between regulators, for example between the Radio Communications Agency and the Dutch Media Authority and between the Radio Communications Agency and the National Cyber Security Centre and the new Digital Trust Centre.

7 Shaping the digital transition based on public values

The essential question is: what sort of society do we want to live in?[183]

7.1 Digital transition

In February 2017, in response to the Gerkens motion, the Rathenau Instituut published its report Urgent Upgrade – Protect public values in our digitized society [Opwaarderen – Borgen van publieke waarden in de digitale samenleving] (Kool et al. 2017).[184] This report mapped out a wide range of societal and ethical issues relating to digitalisation. One key conclusion was that the current wave of digitalisation is compromising many public values such as privacy, digital security, equal treatment and freedom of expression. Another conclusion was that the governance system – the system of actors and institutions responsible for shaping and placing the relevant societal and ethical issues on the agenda – was insufficiently prepared to adequately protect public values in the digital society. With that in mind, the Rathenau Instituut suggested that an update or upgrade of the governance system was urgently needed in order to adequately safeguard public values in the digital society. This urgency relates directly to the realisation that establishing an adequate governance system itself is often a process that takes decades.

Now (autumn 2018) we are eighteen months further on. This report is an update of Urgent Upgrade. It lays out an integrated view of the steps taken by a variety of parties in the period 1 January 2017 - 30 June 2018 with the aim of strengthening the governance system with regard to the ethical and societal aspects of digitalisation. Given the extreme relevance and urgency of this strengthening process from a societal perspective, a rapid update is needed. The adequate safeguarding of essential public values in a digital society is clearly at stake. The key question therefore, as expressed at the top of this page is: What sort of society do we want to live in? In that sense, digitalisation has penetrated to the very heart of the democratic debate.

[183] Quote from : Ministry of Home Affairs (2018, 25-26) in NL DIGIbeter: Agenda Digital Government
[184] The motion, submitted on 23 September 2014, called on the government to ask the Rathenau Instituut to investigate the desirability of instituting an advisory committee on the ethical aspects of digitalisation in society

The fact that this question now occupies a prominent position at governance level is evidence that digitalisation has long passed the stage of referring merely to a collection of technological gadgets. It goes beyond the automation of government services or the directionless promotion of innovation. The realisation has hit home that digitalisation is leading to a new world, a new economy, a new democracy; in short, a new society that is constantly being changed in surprising ways, by new digital resources (Van Est et al. 2018). In that light, digitalisation is increasingly viewed as a process of transition, and the shaping of that transition as a challenge. The Dutch Digitalisation Strategy *Nederland Digitaal* regularly uses the term ‘digital transition’ (EZK 2018a). In this chapter, we will discuss how public values relate to this challenge.

Section 7.2 is a summary of what the governance system with regard to the societal and ethical issues of digitalisation currently looks like (mid 2018). At the start of 2017, the study *Urgent Upgrade* identified five blind spots in the governance system (see figure 4). Section 7.3 is a reflection on the question as to what extent those five blind spots have been dealt with, over the past two years. Finally, in section 7.4, we discuss how the governance of the societal and ethical aspects of digitalisation can be further strengthened over the next few years. The key challenge is to shape the digital transition from the point of view of shared public values in order to establish an inclusive digital society, in which no one is excluded.

7.2 The upgrading has begun

In the previous chapters, we discussed what the governance system with regard to societal and ethical issues looks like, in mid 2018. This system consists of four domains: fundamental rights and human rights, society, the scientific community, and politics and administration (agenda setting, policy development and political decision making, and policy implementation). In this section, for each domain we summarise our findings from the previous chapters.

It is clear that a whole raft of parties in society are actively discussing the ethical and societal aspects of digitalisation: the upgrading of the governance system in this field has begun.

7.2.1 State of affairs mid 2018

Fundamental rights
In the domain of fundamental rights and human rights, our analysis reveals that attention for the significance of digitalisation has grown at both national and international level. From a technological perspective, the discussion has broadened from a focus on the Internet to interest in a broad range of areas of technology including big data and Artificial Intelligence (AI), persuasive technology, robotics and Internet platforms. This has in turn broadened the discussion of the significance of digitalisation for a number of fundamental rights and human rights
In this connection, in addition to privacy, a number of other issues relating to digitalisation have been placed on the agenda, including freedom of expression, equal treatment, autonomy and the protection of democracy.

In the Netherlands, particular attention has been focused on fundamental rights and algorithms, digitalisation (including persuasive technology and platforms) and the protection of democracy. In Europe, or more specifically at the Council of Europe, an even broader range of technology is now on the agenda. The Council is for example investigating the significance of converging technologies, AI, automated data processing, platforms, the biomedical industry, genomics, big data in healthcare, robots, autonomous weapons and hybrid warfare, all with regard to human rights.

Neither nationally nor internationally is there yet much focus on biometrics (facial and emotional recognition), the Internet of Things (IoT), or virtual and augmented reality and human rights, despite the rapid pace of development of these technologies.

Civil society organisations and debate
At the start of 2017, the public debate was above all focused on privacy and digital security. These have continued to be important topics over the past eighteen months. The referendum on the Intelligence and Security Services Act (Wiv) in March 2018, for example, attracted much attention from the media and civil rights organisations. Civil rights organisations also criticised other Dutch government policy, such as the introduction of the Computer Crime III Act (that grants powers to the police to hack into other systems) and the profiling system SyRI (used by the government for tracing fraud).

Our analysis shows that social debate has also broadened in scope over the past eighteen months. New areas of technology such as big data, algorithms and AI have been placed on the agenda, together with new societal and ethical questions.

Civil society organisations are now demanding attention for the potentially negative effects of profiling. They have focused on such issues as the transparency and testing of algorithms (control of technology), and their potentially discriminatory or excluding effects. A number of organisations have made human rights and digitalisation a new spearhead within their organisation, including Amnesty International. In umbrella organisations for business, attention for ethics and digitalisation is cautiously gaining ground.

During the period of investigation 1 January 2017 - 30 June 2018, the media played an important role in placing these issues on the political agenda. Due to to the alleged Russian involvement in the American presidential elections in November 2016 and the Cambridge Analytica scandal, the media focused huge attention on the power of tech companies and the role of their platforms in spreading disinformation. Within the academic community, the deliberate influencing of behaviour via information technology, so-called persuasive technology (cf. Van 't Hof et al. 2012) has been a subject of discussion for some time. For the first time, this subject attracted the attention of the general public, as a result of the Cambridge-Analytica scandal.

There was also attention for the impact of digital technology on human health, and the addictive character of social media. These two issues have not yet been championed by Dutch civil society organisations and there is equally limited discussion of virtual and augmented reality and biometrics (with the exception of attention for biometric applications in passports), despite the fact that applications in the field of facial recognition are developing at a rapid pace, and are already broadly employed in society.

Politics and administration: agenda setting

Since early 2017, growing numbers of advisory councils have been demanding attention for the significance of digitalisation for society. A number of these councils have become focused on digitalisation in its entirety, emphasising that as a result of digitalisation, public values are at risk. Our analysis reveals that 2018 has seen recommendations issued about digitalisation with regard to specific sectors such as power supply, mobility, healthcare, democracy and the media, with specific attention on such areas of technology as AI and digital security. The various councils have emphasised the urgency of protecting public values, and are calling for greater governance and control by government with a view to placing digitalisation on the right track.

They have also recognised that digitalisation is changing the relationships between government, business, civil society organisations and individual citizens.

In response, a number of these advisory councils have emphasised the importance of initiating discussion with social actors in adopting new frameworks, within the digital society. They have also called for attention for the boundaries of self-reliance of individual citizens. On a European level, advisory councils have above all been focusing their calls for attention on AI.

Politics and administration: policy development and political decision making

At the start of 2017, attention within the various Ministries was mainly focused on privacy and digital security. In the period 1 January 2017 - 30 June 2018 we have seen a strengthening and broadening of attention for digitalisation from both a technological and ethical and societal perspective. Various societal and ethical issues have now been placed on the policy agenda. Since the start of the Rutte III Cabinet in October 2017, a series of agendas have been laid down, and June 2018 saw the publication of the overarching National Digitalisation Strategy (EZK 2018a). In the second half of 2018, we expect to see a number of further policy documents, for example in the field of horizontal privacy and AI in the administration of justice.

The National Digitalisation Strategy is a two-track process: 1) grasping societal and economic opportunities and 2) strengthening the foundations according to five spearheads. One of those five spearheads relates to the strengthening of the resilience of businesses and citizens. This refers specifically to privacy and digital security. In this field, the Cabinet has made the shift from agenda setting and policy development to political decision making.[185] The government has launched specific policy measures with regard to digital security, such as new bills, the creation of think tanks and improving cooperation.

Another spearhead from the National Digitalisation Agenda relates to fundamental rights and ethics in the digital age. New themes within this spearhead that have emerged since the start of 2017 include the spreading of disinformation, the protection of democracy and the significance of algorithms for fundamental rights. Within this spearhead, policy development is still very much in its infancy. The government is above all investing in the accrual of knowledge, and has announced studies across a broad scope, including research into the significance of AI and the protection of public values (request for advice from the WRR) and a study into digitalisation of democracy (request for advice from the Council for Public Administration, ROB).

[185] In the field of privacy, specific legislation and a series of policy measures have been in place for a considerable length of time. On 25 May 2018, the General Data Protection Regulation (GDPR) came into effect.

With regard to the spearhead ‘a dynamic digital data economy’, the Cabinet is, among other things, investigating the extent to which existing statutory frameworks are sufficient. The goal is to keep the markets competitive, and to clarify the question of the possible need for alterations to the set of instruments in the field of competition. In respect of each of these issues, the Cabinet has announced a series of studies. Here, too, policy is in its earliest stages. The Cabinet is also promoting self-regulation by platforms and cooperation between (local) government and platforms.

With regard to the digital data economy, to a large extent, policy setting is in the hands of the European Commission. The Commission will be issuing proposals about the relationship between businesses and platforms and the delivery of digital content. In other policy areas, too, policy setting is (in part) the responsibility of the European Commission that is currently modernising a series of legal frameworks and formulating new frameworks, for example in respect of data protection, ePrivacy, audio-visual and media services, copyright, consumer rights and cybersecurity.

Political decision making: Senate and House of Representatives

In the Dutch Senate and House of Representatives, privacy and digital security are clearly on the agenda. New societal themes that have also been placed on the agenda include control of technology (transparency of algorithms) and justice (discrimination due to algorithms), autonomy (about disinformation, political microtargeting and freedom of choice), and human dignity and balances of power (the position of sharing and gig platforms, employee conditions and the power of tech companies). Via round table discussions and expert meetings, both Houses are actively building up their knowledge of new societal and ethical aspects of digitalisation, for example in the field of AI in the administration of justice, data analytics and the sharing and gig economy.

Policy implementation: regulators

Among almost all regulators, the awareness of the societal and ethical aspects of digitalisation has grown. Many of these regulators are now assessing the significance of digitalisation for (new) aspects of their fields of study, and their role in that process. They are at work acquiring knowledge of new issues; take for example the investigations by the Authority for Consumers and Markets (ACM) and the Dutch Media Agency into the digitalisation of news. Among some regulators, these activities have led to new areas for attention in their supervision tasks, for example at the Authority for the Financial Markets (AFM), which has expressed its intention to more specifically examine the use of data in the financial sector.

There is also more collaboration between regulators. The Cabinet has announced a dialogue session for supervisory bodies active in the field of digital security, aimed at improving the effectiveness of supervision. In the period 1 January 2017 – 30 June 2018 we have also seen enlarged or adapted mandates for a number of regulators, in response to amended or new legislation, accompanied by larger budgets and increased capacity.

7.2.2 Broadening the debate

The most important message from *Urgent Upgrade* is that 'government, businesses and civil society must take action now to strengthen the governance system' (Kool et al. 2017, p12). We can now conclude that the first steps have been taken.

Both from a technological and societal perspective, the debate on the societal and ethical issues has been broadened. More digital technologies are now on the policy agenda, including AI, platforms and persuasive technology. There is greater attention for the societal and ethical aspects of freedom of expression, protection of democracy, equality and justice and the boundaries of the self-reliance of individual citizens (autonomy). Table 22 provides an overview of the societal and ethical issues we identified in *Urgent Upgrade.* In that report, privacy and security were on the agenda. These have now been joined by autonomy, control of technology and justice, and the balances of power. Within each of these topics a number of new subjects are now being discussed. These are printed in bold in table 22.

During the past eighteen months, awareness of the societal and ethical issues of digitalisation has grown. Numerous actors such as policy makers, politicians, civil society organisations, regional and local governments, professional associations and regulators now recognise the importance of protecting public values. They are at work considering the question what digitalisation means for their organisation, sector or practice. The central question for these parties is how they can successfully direct the digitalisation process. Many players recognise that the underlying principle behind all digitalisation activities must be the protection of public values and fundamental rights. This represents a turnaround in the debate on the use and influence of digital technology, from a focus on technology and the assumption that it will automatically result in social progress, to a focus on the interaction between digitalisation and values. On the one hand, digitalisation is seen as a means of tackling the challenges facing society, while on the other it is recognised as a power that could compromise the development of public values.

Table 22 Societal and ethical issues relevant to digitalisation. Subjects that have emerged since *Urgent Upgrade* (2017) are printed in bold.

Topic	**Societal and ethical issues**
Privacy	Data protection, privacy, mental privacy, surveillance, function creep
Autonomy	Freedom of choice, freedom of expression, manipulation (**spreading of disinformation, microtargeting), protecting democracy**, paternalism, **skills**, **boundaries of self-reliance**
Safety and security	Information security, identity fraud, physical safety
Control of technology	Control and transparency of algorithms, responsibility, predictability
Human dignity	Dehumanisation, instrumentalisation, de-skilling, de-socialisation, unemployment
Justice	Discrimination, exclusion, equal treatment, stigmatisation
Balances of power	Unfair competition, exploitation, relation between consumers and businesses, **relationship between businesses and platforms**

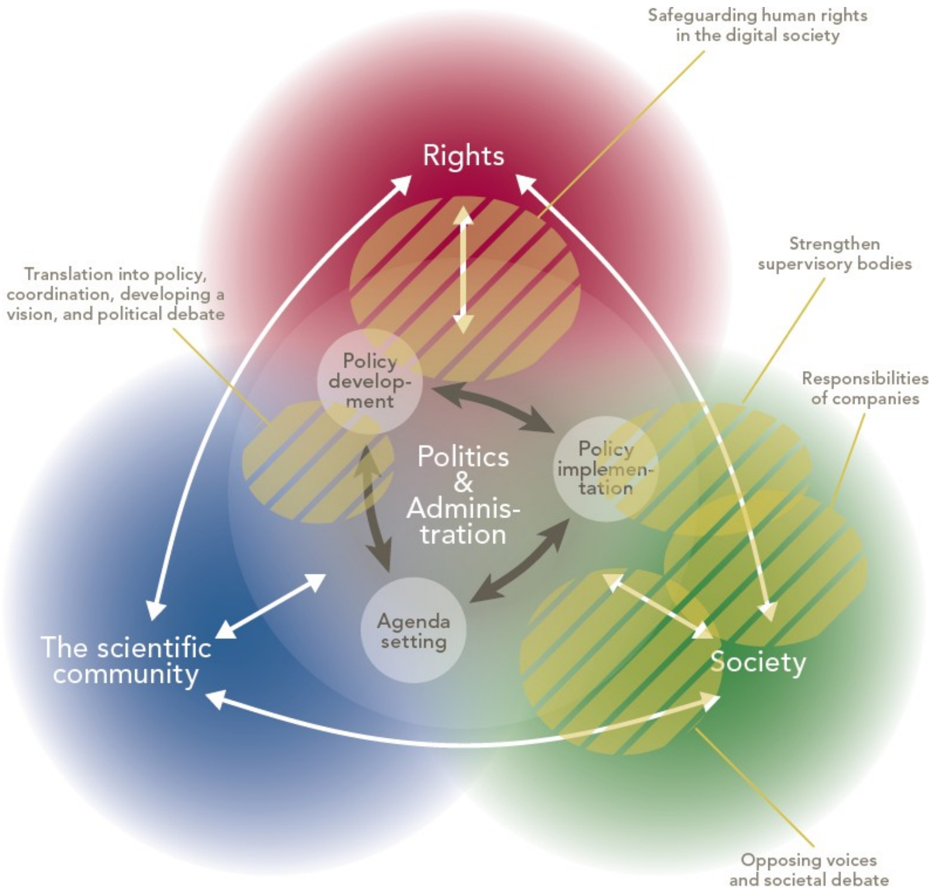
Source: Rathenau Instituut

7.3 Blind spots partially covered

At the start of 2017, we identified five blinds spots in the governance system regarding the ethical and societal aspects of digitalisation (see figure 4). Based on the recognition that the creation of an adequate governance system is a long-term process, the Rathenau Instituut called upon government, businesses and civil society organisations to take rapid steps in each of the five areas identified. This paragraph maps out for each of the five blind spots what actions have been initiated in the period 1 January 2017 - 30 June 2018. We also identify a number of shortfalls still existing in respect of each blind spot. Based on this analysis, in section 7.4, we issue five recommendations.

Figure 4 Five blind spots in the governance system with regard to the ethical and societal aspects of digitalisation, start of 2017

1. Translating emerging societal and ethical issues into policy. Inter-ministerial consultation and coordination of digitalisation and political debate on these emerging issues.
2. Safeguarding fundamental rights and human rights in the digital society.
3. Strengthening supervisory bodies and ensuring that they consult with one another.
4. New responsibilities for companies that develop digital products and services.
5. Organising opposing voices and societal debate: strengthening civil society, augmenting the public's knowledge and skills, and promoting public debate on digitalisation.


Safeguarding human rights in the digital society
Rights
Strengthen supervisory bodies
Translation into policy, coordination, developing a vision, and political debate
Responsibilities of companies
Policy development
Politics & Administration
Policy implementation
Agenda setting
The scientific community
Society
Opposing voices and societal debate

Source: Rathenau Instituut (Urgent Upgrade, 2017)

Blind spot 1: Translating emerging societal and ethical issues into policy. Interministerial consultation and coordination of digitalisation and political debate on these emerging issues.

Translation into policy

With regard to the topics privacy and digital security, the translation of the presence of societal and ethical issues on the agenda into policy has now started. Policy making on privacy and data protection had already been in progress for some time. For digital security and the IoT, a series of policy agendas with specific measures were laid down in the period 1 January 2017 - 30 June 2018 (including the National Cyber Security Agenda, the Roadmap for Secure Digital Hardware and Software and the imminent Defence cyber strategy). This does not mean that the protection of privacy and digital security is ‘complete’; technological and social developments are constantly leading to new issues, for example in the field of facial recognition. However, this topic is not yet on the policy agenda. To make the translation from new issues into policy, continuous monitoring of developments is needed, to identify whether, and if so where, new policy measures are required.

The translation from agenda setting into policy is less apparent in respect of emerging topics, such as the spreading of disinformation and the transparency of algorithms. These issues have been placed on the agenda, but the policy making process is still in the early stages. Although ‘Fundamental rights and ethics in the digital age’ are a spearhead within the National Digitalisation Strategy, that strategy does not yet specify clear policy measures. The Cabinet is currently investing particularly in building up the necessary knowledge, via research. We would add that a series of further policy documents are expected to be published in the autumn of 2018.

As concerns other subjects, the translation of presence of the agenda into policy is above all a task for the European Commission. The Commission is currently modernising a series of statutory frameworks with regard to privacy, copyright and consumer rights, among others. The Commission is also issuing new policy frameworks in the field of illegal content and competitive data economy. These new measures will require the Netherlands to make a timely translation from a presence on the agenda into policy, in order to determine the Dutch position.

Finally, a number of relevant themes are still barely present on the policy agenda at all, such as facial recognition, virtual and augmented reality, and the possible health effects of digital technology. In particular facial recognition is already being widely used in society; as such, this technology raises urgent fundamental questions for example about privacy.

Coordination and harmonisation of policy
At the start of 2017, we saw considerable difficulties in the translation of ethical and societal aspects of digitalisation into a coherent policy, capable of encompassing multiple domains. Policy discussions on these issues were often incident-based. In Urgent Upgrade, we therefore proposed the drawing up of an overarching Cabinet vision on the governance of the societal and ethical aspects of digitalisation.

With its National Digitalisation Strategy, the Cabinet has now laid down an overarching agenda for digitalisation. Societal and ethical aspects are an element of this agenda, with as its spearheads 'fundamental rights and ethics in the digital age', 'dynamic digital economy' and 'strengthening the resilience of citizens and organisations'. In mid-2018, an interdepartmental working group was also established to consider the societal and ethical aspects of digitalisation. In this field, therefore, greater harmonisation and coordination have been achieved within government. At the same time the policy remains mainly reactive, mostly driven by such incidents as the Cambridge Analytica scandal and the suspected Russian involvement in the American presidential elections.

Coordination and harmonisation of politics
Within the Dutch Senate and House of Representatives, too, attention for societal and ethical issues has grown, as reflected by the Parliamentary questions and motions submitted (see appendix 1). There is a clear need for an overarching understanding of the significance of digitalisation for the protection of public values; for example see the (suspended) motion by senator Duthler on the question 'whether and how the process of digital transformation requires further standardisation' (Parliamentary Papers I 2017-2018, 34 775 VI, V), and the parliamentary motion by Van Dam and Van der Molen in which the government is called upon to 'introduce a values-driven approach to digitalisation' and to inform and offer the House the 'opportunity to be involved in the development of these values' (Parliamentary Papers 2017-2018 32761, no. 120).

With its National Digitalisation Strategy (EZK 2018a) in June 2018 the Cabinet did introduce an overarching policy agenda. In that connection, on 20 September 2018, a general debate was held in the House of Representatives about digitalisation, under the auspices of the Permanent Committee for Economic Affairs and Climate Policy. The Digital Government Agenda (NLDigibeter) is also expected to be discussed within the Permanent Committee for the Interior. Within its Permanent Parliamentary Committees, the Dutch Senate is also involved in discussing a series of societal and ethical aspects of digitalisation.

Nonetheless, in neither House has space yet been created for discussing the societal and ethical aspects of digitalisation based on an overarching approach, that crosses the boundaries between the various relevant domains.

Blind spot 2:
Safeguarding fundamental rights and human rights in the digital society.
Our analysis reveals that the Cabinet is in the process of investigating the significance of digitalisation for the safeguarding of fundamental rights in a number of areas. The Ministry of the Interior and Kingdom Relations, for example, is concentrating particularly on algorithms and fundamental rights and the significance of digitalisation for democracy. This then represents a start on covering this blind spot. At the same time, it has become clear that safeguarding fundamental rights and human rights, and wherever necessary amending those rights, is a long-term development. Over the coming years, too, the Cabinet must remain active in these areas.

Algorithms and the protection of democracy are not the only subjects requiring attention. Within the Council of Europe, we are currently seeing a broad assessment of new areas of technology and societal and ethical issues. In Europe, the Council of Europe has the lead when it comes to investigating and shaping the significance of new technology for fundamental rights. A similar broad-based orientation is also essential for the Netherlands, and as such it is important to not restrict attention for digitalisation to the role of algorithms or AI.

Blind spot 3:
Strengthening supervisory bodies and ensuring that they consult with one another.
Attention for the societal and ethical aspects of digitalisation has grown among regulators. The mandate and budget for a number of these supervisory bodies have been extended. Investments are also being made in accruing expertise and cooperation with other supervisory bodies. These are essential developments in strengthening the governance system. Experience will show over the next few years whether this does in fact result in strong supervisory bodies capable of effective enforcement.

Blind spot 4:
New responsibilities for companies that develop digital products and services.
In the period under investigation 1 January 2017 - 30 June 2018, much attention was paid by the various umbrella and sector organisations to the introduction of the General Data Protection Regulation (GDPR). Various organisations introduced tools to assist businesses in preparing for this new regulation. A cautious start was also made on considering the ethical issues, for example in the form of ethical

codes and guidelines for developers of for example robotics and AI. On the other hand, there is little visible evidence within business of attention for other themes such as control of technology (transparency of algorithms), autonomy (persuasive technology) and justice, or for trends such as facial recognition and virtual and augmented reality.

Our analysis reveals that pressure from society, policy and politics on business to take its social responsibility in these areas is growing. Over the past few years, this has been particularly clear with regard to digital security and IoT, and in relation to the Cambridge Analytica scandal. In the Netherlands, policy makers are searching for possibilities for encouraging developers to take greater responsibility. The GDPR, for example, compels developers to comply with privacy by design. In the field of digital security, the Netherlands aims to impose compulsory security updates on manufacturers of consumer electronics.

In respect of the sharing and gig economy, too, the question of the responsibility of platforms has acquired a prominent position on the policy agenda. The crucial element is the demand for greater clarity about the role of platforms. At the end of 2017, the European Court of Justice finally clarified the nature of the responsibilities of a platform like Uber, in respect of taxi services.[186]

In other areas, for example countering the spread of disinformation, the Cabinet is initially relying on self-regulation by the private sector. In response to public controversy and requests from regulators, the major Internet platforms are taking the first cautious steps in this direction.

To a limited extent, therefore, a start has been made on covering this blind spot. At present, there is still no proactive attitude within the private sector to safeguard public values despite growing calls from politics and society to accept this responsibility. A number of bills are currently being prepared aimed at forcing business to accept statutory obligations, in these areas. It is important to carefully consider the importance of these responsibilities, and how they can or cannot be imposed on businesses. One current question, for example, is the role of social media platforms in the rapid deletion of hate-spreading content and material that may be in violation of copyright. There is however a clear concern that in the face of fears about liability, Internet companies themselves will determine what content may or may not be placed online, thereby restricting the freedom of expression.

[186] The European Court of Justice judged that the service offered by Uber via an app is a transport service as intended in EU law, and not a digital service. This means that the EU Member States are able to determine nationally the conditions according to which this service is provided. The case was brought before the court by Spanish taxi drivers.

Blind spot 5:
Organising opposing voices and social debate: strengthening civil society, augmenting the public's knowledge and skills, and promoting public debate on digitalisation.

In *Urgent Upgrade*, we saw a limited social debate on the societal and ethical significance of a digitalising society. As a result, one of our recommendations was to strengthen technological citizenship, for example through social dialogue and promoting digital skills. Technological citizenship means that the public has a better understanding of new technology and the skills to use it, has a command of the functioning and effects of digital technology on the individual and society, and is able to participate in democratic debate and political decision making on technology (Van Est 2016).

The limits of digital literacy

In the period 2017-2018, we saw greater attention for digital literacy, digital skills and resilience. Work is for example underway on a new curriculum for primary and secondary schools, with more attention for digitalisation, and plans for media literacy are due to appear in the autumn of 2018. In the National Digitalisation Strategy, within the spearhead 'Other work, new skills and lifelong learning', there is clear attention for (digital) skills acquisition.

At the same time, attention has grown for the limits of the self-resilience of individuals. Various advisory councils, the National Ombudsman, the Ministry of the Interior and Kingdom Relations and the implementing bodies such as the UWV and ICTU have all called for attention for these limits. The starting point is no longer by definition 100% digital; it is equally important that an analogue channel remains available and plans are more based on the idea of public facilitation. In healthcare, too, organisations are warning about the limits of self-reliance (Pluut & De Jong 2018; Niezen & Verhoef 2018).

Broader social debate

As regards involvement in the democratic debate and political decision making, a great deal has happened in a number of areas, in the period 1 January 2017 - 30 June 2018. Members of the public and civil society organisations clearly made their presence felt. Five students succeeded in enforcing a referendum on the Wiv Act, which resulted in a very active public debate. Civil society organisations responded to government policy with a series of lawsuits. Privacy, digital security, profiling (for example the lawsuit against the government system SyRI) and transparency and control of technology are key topics.

During the investigated period, the media played in particular an important role in bringing such issues as autonomy, balances of power and the effects on health, to the attention of a broad public. In particular the Cambridge Analytica scandal placed the relationship between digitalisation, democracy, media and citizenship – and as such technological citizenship – high on the political and public agenda. As a result, many parties became acutely aware that technological citizenship is an absolute precondition for a healthy democracy, and that there is still much to be achieved in that regard.

7.4 Recommendations

This report reveals that over eighteen months, the realisation has grown steadily among many players that digitalisation poses society with a massive transition challenge, with both negative and positive aspects. This transition perspective is of great importance for the governance of societal and ethical digitalisation issues in that it raises the crucial question: what sort of digital society do we want to live in? To be able to address that question, an integrated approach to innovation is called for that shapes and directs the digital transition and as a result our society, on the basis of public values.

The most important message from the Rathenau Instituut is therefore that government, businesses and civil society must take further action to strengthen the governance system so that a digital society can be shaped and directed based on public values, in which no one is excluded.

Below we list five actions that will help policy makers, businesses and civil society organisations further strengthen the governance system with regard to the ethical and societal aspects of digitalisation. The first action refers directly to the central challenge described above. Each of the action points refers to further actions aimed at even better addressing the blind spots within the governance system identified in 2017. Each action concerns the formulation of a specific ambition and the necessity for the long-term deployment of tools and resources in order to successfully bring about the digital transition.

Recommendation 1:
Invest in a values-based approach to innovation
It is important that ethical and societal issues are not viewed in isolation from the processes of innovation and digitalisation. There is a clear risk that ‘fundamental rights and ethics in the digital age’ as the final section in the Dutch National Digitalisation Strategy, could literally be an afterthought in the digitalisation agenda. To achieve the ambitions of the Netherlands for example with regard to mobility, healthcare, education and power supply, it is essential that a link be established between innovation programmes and ethical and societal issues. Bringing about a

a transition or finding a reply to the question ‘in what sort of society do we want to live’, means assuming and accepting values as the essential starting point. This turnaround in thinking ties in with the general development in thinking about innovation policy, in which the challenges facing society are acquiring an increasingly important, leading role in shaping innovation; the outcome is a mission-based innovation policy or decisive innovation systems (see Mazzucato 2018; Frenken & Hekkert 2017).

Against this background, the Rathenau Instituut calls for ‘meaningful digitalisation’ based on interaction between five innovation processes: , experimentation, grasping opportunities, mitigating risks and working together and learning (Van Est et al. 2018). In each of these processes, there is a central position for the role of public values. ‘Appreciation’ first and foremost relates to a clarification of the benefits and limits of digitalisation from the point of view of public values. Key elements are target values or innovation goals (such as quality of life, sustainability, social inclusion, vital economy, efficient service provision) and values closely related to fundamental rights and human rights (such as privacy, autonomy, security, human dignity, control of technology, justice and balances of power). The second vital element is the direction of technological and social innovation on the basis of public values. By setting down ethical guidelines for autonomous cars, the German government has offered developers clear handholds and guidelines for the further development of those autonomous vehicles. In the Netherlands, the Municipalities of Eindhoven and Amsterdam established four core principles for governing the processes of digitalisation in their cities (Municipalities of Eindhoven and Amsterdam, 2017). This essentially also means imposing requirements and setting ground rules, for example for interaction with businesses.[187] When it comes to ‘grasping opportunities’, it is essential to also consider the opportunities offered by digitalisation, and grasping those opportunities to address social challenges. To ‘mitigate risks’, it is also vital to focus on the risks of digitalisation, while specifically protecting public values via debate, policy and the development of technology.

Recommendation 2:
Establish a proactive, overarching agenda and activity plan for the societal and ethical aspects of digitalisation

Clearly, the societal and ethical aspects of digitalisation have acquired a significant place on the policy agenda. However, as yet there is no coherent picture and the steps taken remain mainly reactive. As regards privacy and digital security, the step from agenda setting to policy making has been taken, but this is not yet the case for new items on the agenda such as the significance of algorithms for fundamental rights, the importance of digitalisation for democracy, and persuasive technology.

[187] See: https://fd.nl/economie-politiek/1207927/een-sensor-op-elke-straathoek

To bring about a strong governance system, tangible, proactive policy agendas are also needed in these areas (such as the Roadmap for secure Digital Hardware and Software). This also demands attention for topics as yet barely present on the policy agenda, if at all, such as facial recognition, virtual and augmented reality, and the possible health risks of digital technologies. Any proactive agenda requires periodic monitoring of digital trends and the accompanying societal and ethical issues. An overarching agenda inherently includes a vision on how society can be involved in the digital transition (see also recommendation 5).

Recommendation 3:
Invest in a strong position for supervisory bodies
Regulators form a crucial link in strengthening the governance system for the societal and ethical digitalisation issues. Those regulators are currently investing in acquiring expertise and collaborating with other supervisory bodies. A number of regulators have also been given further tasks and authorities or increased budgets, or preparations are underway on similar proposals, for example with regard to digital security and the media. It is essential to monitor whether and to what extent these new supervisory authorities are sufficient.

The actions taken with a view to strengthening the regulators can be viewed as initial steps. We are only just starting to understand the meaning of a digital society. As part of the process of policy implementation, regulators are the hands and feet of policy makers, as well as their eyes and ears. As a result, for policy makers they fulfil a role in placing issues on the agenda, for example with regard to an adequate mandate or set of instruments. From a strategic viewpoint, it is therefore essential to continue investing in the capabilities and capacities of the regulators.

A strong position for supervisory bodies also includes the possibility of enforcement. Over the past few years, greater clarity has been achieved as concerns the relevant legal frameworks, for example with regard to platforms. Nonetheless, a number of questions are still unanswered, for example concerning the role and responsibilities of social media platforms in the provision of news. Over the coming period, these legal uncertainties must be clarified.

Because it runs right across sectors and legal frameworks, over the next few years, digitalisation will require intensive cooperation between various supervisory bodies. The spreading of disinformation, for example, affects the legal frameworks governing the processing of data, voting rights, competition law, media law and consumer law. Cooperation will probably reveal the presence of insufficient clarity on areas of authority, ‘gaps’ not covered by cooperation, and will help identify legal frameworks that require further adjustment. Policy makers must be ready to take account of such outcomes.

Recommendation 4: The private sector: recognise the importance of socially responsible digitalisation

> *I think a big mistake we have made, looking back on this, is viewing our responsibility as just building tools, rather than viewing our whole responsibility as making sure that those tools are used for good.”*
> Mark Zuckerberg, CEO Facebook[188]

Our analysis shows that the growing political and social sensitivity for the societal and ethical aspects of digitalisation is imposing further pressure on businesses to take these issues seriously. So far, businesses have only met these demands to a limited extent. Within the major tech businesses, for many years, attention was above all focused on developing and rolling out new technologies as quickly as possible, rather than considering how those technologies are used. Under pressure from society, this situation is slowly changing. The statement by Mark Zuckerberg quoted above, and which he made in April 2018 when he was called to account for the Cambridge Analytica scandal before the American Congress, is a clear reflection on this changing attitude.

Corporate social responsibility with regard to digitalisation calls for a proactive attitude from business: predicting and anticipating the potential societal and ethical implications of the technology developed by a company. An early understanding of the ethical and societal aspects, for example based on ethical impact assessments, could result in design changes.

The responsibility of businesses to protect human rights is for example laid down in the Guidelines for multinational businesses issued by the OECD. Businesses are called upon to actively undertake to recognise the risks of violations of human rights by themselves or parties in their supply chain, and wherever possible to prevent such violations. In other areas, too, for example in respect of security or data protection, businesses are now subject to a variety of duties of care.

It is now the turn of business to put those duties of care into practice. Sectoral organisations can play an important role in providing information about the existing duties of care, and satisfying international standards in practice, for example by introducing codes of conduct.

[188] During the hearing before the American Congress on 10 April 2018.

Recommendation 5:
Encourage technological citizenship

Engagement by society and citizens is a key component of the shaping and directing of innovation. It is important that citizens have an understanding of the possibilities and risks of new technology, possess the skills to handle those new technologies in their life, in an adequate manner, and are able to participate in democratic debate and the process of political decision making. This is referred to as ‘technological citizenship’ (Van Est 2016). Continuous encouragement of these three elements of technological citizenship is essential for any strong governance system. It also remains vitally important to take account of the limits of self-reliance of the public, and their willingness to participate.

The current renewal of the curriculum in primary and secondary education offers excellent opportunities for giving technological citizenship an adequate position in education. Attention must however also be focused on the third element: democratic participation by the general public. For the entire working population it is also vital that digital skills be acquired, to enable them to also retain meaningful employment in the future.

In increasing public involvement, two issues are of key importance: sound information provision and the opportunity to participate. In respect of information provision, independent media and research journalism play a central role. From a democratic viewpoint, safeguarding these elements of a digital society is vital.

‘Values-driven innovation’ means shaping and directing innovation on the basis of shared public values. This calls for social involvement and dialogue in determining the direction to be taken. Involvement is indeed desired at various points in our society: at project level, at sector level (for example healthcare, power supply, mobility and education) and at various administrative levels (national, provincial and local). We are seeing initiatives taken at numerous different locations. Think of local government involving local residents in smart city projects, or businesses that involve their employees in innovations on the shop floor.
In the framework of the ‘proactive, overarching agenda and activity plan for the societal and ethical aspects of digitalisation’, as referred to in recommendation 2, it is essential that national government develops a vision on promoting technological citizenship and strengthening social involvement in the digital transition.

7.5 Finally

A broad realisation has emerged that digitalisation is presenting society with a considerable transition challenge. Digitalisation is no longer seen as an issue exclusively affecting ICT. Over the past few years, we have experienced directly how digitalisation is influencing the world in which we live, our economy, our democracy; in short, our entire society. Digitalisation is constantly generating new ethical and societal questions.

This is reflected by two examples. Facial recognition is already a standard application in the new generation of smartphones, and raises urgent questions about the loss of anonymity and privacy protection. Even today, our smartphones, social media and other apps are exercising such an influence that there is more and more reference to potential mental and physical health effects. Former employees from Silicon Valley have compared the technology deployed in these digital media to the technology in gambling machines.

It seems likely that the digitalisation of society is set to accelerate over the coming years. Virtual and augmented reality applications are already invading the consumer market and other domains. The continued rollout of 5G networks will inevitably deliver a boost to the Internet of Things and the real-time ability to control objects and information (and even us). This clearly offers opportunities, for example for the energy transition, but also raises many questions about authority over data and a fair and competitive data economy. Across the world, businesses and countries are investing many billions in artificial intelligence. According to some, this AI race will determine the future economic and military power of many countries. Nonetheless, as yet, there is little discussion of the significance of these compelling technologies for ourselves, our relationships and our society.

The report *Urgent Upgrade* and this update to that report were published in response to the Gerkens Motion, in which the government was called upon to ask the Rathenau Instituut to investigate the desirability of a committee able to advise on the ethical aspects of the digitalising society. The motion itself refers to the Internet of Things and to the broader societal, socio-legal and socio-psychological effects of digitalisation. The Dutch Senate already suspected that digitalisation would generate huge challenges for society. The report *Urgent Upgrade*, and this update, confirm that suspicion. Although steps have been taken to strengthen the governance system, public values are still being compromised by digitalisation. There is an urgent need to actually base our thinking on the awareness that our society is experiencing nothing less than a digital transition, and to assign a pivotal role to values in shaping and directing an inclusive digital society. Now and in the years to come, that will place demands on all parties to accept their own responsibility, and to collaborate with other local, regional and international parties.

Bibliography

Adviescommissie voor Vreemdelingenzaken (2016). *Profileren en selecteren: advies over het gebruik van profilering in de uitvoering van het vreemdelingenbeleid*. Den Haag: Adviescommissie voor Vreemdelingenzaken

AFM (2017a). *Jaarverslag 2016: Scherp toezicht in een veranderend speelveld*.
Amsterdam: AFM. Available online: https://www.afm.nl/nl-nl/verslaglegging/jaarverslag

AFM (2017b). *AFM waarschuwt voor grote risico's bij Initial Coin Offerings*. (13 november 2017). Available online: https://www.afm.nl/nl-nl/consumenten/nieuws/2017/nov/risico-ico

AFM (2018a). *AMF Agenda 2018*. Available online: https://www.afm.nl/nl-nl/verslaglegging/agenda

AFM (2018b). AFM *zet in 2018 vol in op data-analyse om belegger te beschermen*. (24 januari 2018). Available online: https://www.afm.nl/nl-nl/consumenten/nieuws/2018/jan/agenda-2018

Agentschap Telecom (2017). *Staat van de Ether, 2016*. Groningen: Agentschap Telecom. Available online: https://magazines.agentschaptelecom.nl/staatvandeether/2017/01/index

Authority of the House of Lords (2018). *AI in the UK: ready, willing and able?* London: House of Lords

Autoriteit Consument & Markt (2017). *Geen dominante marktmacht bij online video-streaming platforms* (22 augustus 2017) Available online: https://www.acm.nl/nl/publicaties/publicatie/17573/Geen-dominante-marktmacht-bij-online-video-streaming-platforms

Autoriteit Consument & Markt (2018). *Position Paper Autoriteit Consument & Markt.*
Rondetafelgesprek over de marktdominantie van internet- en technologiebedrijven. 31 januari 2018. Available online: https://www.acm.nl/sites/default/files/documents/2018-02/positionpaper-acm-over-marktdominantie-grote-tech-bedrijven.pdf

Autoriteit Persoonsgegevens (2017a). *Agenda 2017*. Den Haag: Autoriteit Persoonsgegevens.

Autoriteit Persoonsgegevens (2017b). Adviesontwerp besluit tot wijziging van het Besluit BRP. Den Haag: Autoriteit Persoonsgegevens (21 maart 2017)

Available online: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_wijziging_besluit_brp_sila.pdf

Autoriteit Persoonsgegevens (2017c). *Wetgevingsadvies conceptwetsvoorstel Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven*. Den Haag: Autoriteit Persoonsgegevens (28 april 2017) Available online: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_pnr.pdf

Autoriteit Persoonsgegevens (2017d). *Advies wetsvoorstel Implementatiewet herziene richtlijn betaaldiensten*. Den Haag: Autoriteit Persoonsgegevens (22 augustus 2017) Available online: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_psd2.pdf

Autoriteit Persoonsgegevens (2017e). *Adviesverzoek concept-Cybersecuritywet*.
Den Haag: Autoriteit Persoonsgegevens (25 oktober 2017) Available online: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/z2017-04917_advies_cybersecuritywet.pdf

BEUC (2018a). *Automated decision making and Artificial Intelligence – A Consumer Perspective*. BEUC Position Paper. 20-06-2018. www.beuc.eu/publications/beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf

BEUC (2018b). *Plugging the gap in consumer rights. What a new deal should look like in 2018*. Brussels: BEUC. Available online: www.beuc.eu/publications/beuc-x-2018-023_what_a_new_deal_for_consumers_should_look_like_in_2018.pdf

BEUC (2018c). *Cybersecurity Act - Consumers need mandatory security by design and by default*. Brussels: BEUC. Available online: http://www.beuc.eu/publications/beuc-x-2018-024_cybersecurity_act_consumers_need_mandatory_security_by_design_and_by_default.pdf

BMVI (2017). *Ethics Commission Automated and Connected Driving*. Berlin: BMVI.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B, Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G.C., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., Lyle, C., Crootof, R., Evans, O., Page, M., Bryson, J., Yampolskiy, R. & Amodei, D. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Available online: https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

Centraal Planbureau (2017). *Scientia potentia est: de opkomst van de makelaar voor alles*. Den Haag: Centraal Planbureau.

Centraal Planbureau (2018). *Risicorapportage Financiële Markten 2018*. Den Haag: Centraal Planbureau

College voor de Rechten van de Mens (2017a). *Onbeperkt stemmen - Rapportage over de toegankelijkheid van verkiezingen voor mensen met een beperking*. Utrecht: College voor de Rechten van de Mens. Available online: https://mensenrechten.nl/publicaties/detail/37739

College voor de Rechten van de Mens (2017b). *Brief aan de minister van BZK over internetconsultatie conceptwetsvoorstel Generieke digitale infrastructuur*. Utrecht: College voor de Rechten van de Mens. Available online: https://www.mensenrechten.nl/publicaties/detail/37468

COMEST (2017). *Report of COMEST on robotics ethics* (14 September 2017).
Paris: UNESCO. Available online: http://unescoblob.blob.core.windows.net/pdf/UploadCKEditor/REPORT%20OF%20COMEST%20ON%20ROBOTICS%20ETHICS%2014.09.17.pdf

Commissie van Ministers (2017). *Reply to Recommendation* | *Doc. 14432* (19 October 2017). Brussel: Commissie van Ministers. Available online: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24236&lang=en

Cultureel Planbureau (2018). *CPB Risicorapportage Financiële Markten 2018.* Den Haag: Cultureel Planbureau.

CTIVD (2017). *Jaarverslag 2016*. Den Haag: CTIVD.

Commissariaat voor de Media (2017a). *Jaarverslag 2016*. Hilversum: CvdM. Available online: https://jaarverslag.cvdm.nl/2016/wp-content/uploads/2017/02/Commissariaat-voor-de-Media-Jaarverslag-2016-webversie.pdf

Commissariaat voor de Media (2017b). *YouTubers ontwikkelen met hulp van Commissariaat voor de Media een code om transparanter te zijn over reclame*. (17 november 2017). Available online: https://www.cvdm.nl/nieuws/youtubers-ontwikkelen-hulp-commissariaat-media-code-om-transparanter-reclame/

Commissariaat voor de Media (2017c). *Commissariaat voor de Media en Agentschap Telecom tekenen samenwerkingsprotocol* (6 december 2017) Available online: https://www.cvdm.nl/nieuws/commissariaat-voor-de-media-en-agentschap-telecom-tekenen-samenwerkingsprotocol/

Commissariaat voor de Media (2017d). *Samenwerking Stichting Reclame Code en Commissariaat voor de Media* (23 november 2017) Available online:

https://www.cvdm.nl/nieuws/samenwerking-stichting-reclame-code-en-commissariaat-media/

Commissariaat voor de Media (2017d). *Samenwerkingsprotocol Consumentenautoriteit – Commissariaat voor de Media*. Available online: https://www.cvdm.nl/wp-content/uploads/2013/04/Samenwerkingsprotocol-ACM-en-CvdM.pdf/

Cyber Security Raad (2016). *European Foresight Cyber Security Meeting 2016. Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care*. Den Haag: Cyber Security Raad. Available online: https://www.cybersecurityraad.nl/binaries/Report%20European%20Foresight%20Cyber%20Security%202016_tcm56-102235.pdf

Cyber Security Raad (2017a). *Ieder bedrijf heeft digitale zorgplichten*. Nijmegen: Xerox/OBT. Available online: https://www.cybersecurityraad.nl/binaries/20170405_CSR_Handreiking2017_CompleetDEFweb_tcm56-253718.pdf

Cyber Security Raad (2017b). *Naar een landelijk dekkend stelsel van informatieknooppunten*. Den Haag: Cyber Security Raad. Available online: https://www.cybersecurityraad.nl/binaries/CSR-advies%202017%20nr.%202%20-%20Naar%20een%20landelijk%20dekkend%20stelsel%20van%20informatieknooppunten_tcm56-269317.pdf

Cyber Security Raad (2017c). *Naar een veilig verbonden digitale samenleving*. Den Haag: Cyber Security Raad. Available online: https://www.cybersecurityraad.nl/binaries/CSR%20Advies%20IoT%20digitale%20versie%20DEF%20NED_tcm56-298518.pdf

Cyber Security Raad (2018). *'Naar een open, veilig en welvarend digitaal Nederland': Advies inzake de Nederlandse Cybersecurity Agenda (NCSA)*. Den Haag: Cyber Security Raad. Available online: https://www.cybersecurityraad.nl/binaries/CSR_Advies_NCSA_NED_tcm107-334926.pdf

De Waard, P. & K. Haegens (2018). AFM-voorzitter: *'Financieel beleggen begint op gokken en gamen te lijken'*. (24 januari 2018) Available online: https://www.volkskrant.nl/4561537

DH BIO (2017). *Information document concerning the DH-BIO*. Brussel: Raad van Europa. Available online:https://rm.coe.int/inf-2017-5-e-info-doc-dh-bio/168077c578

ECP (2018). *Artificial Intelligence: Gespreksstof en handvatten voor een evenwichtige inbedding in de samenleving*. Whitepaper. Leidschendam: ECP.

Europese Commissie (2018a). *Multi-dimensional approach to disinformation. Report of the independent High Level Group on fake news and online disinformation*. Brussels: Europese Commissie.

Europese Commissie (2018b). *Bestrijding van online-desinformatie: Commissie stelt EU-brede praktijkcode voor* (26 April 2018). Available online: http://europa.eu/rapid/pressrelease_IP-18-3370_nl.htm.

Europese Commissie (2018c). Communication from the Commission to the European Parliament, European Council, the Council, the European Economic Social Committee and the Committee of the Regions. *Artificial Intelligence for Europe.* COM (2018) 237. 25.4.2018. Brussels: European Commission.

European Group on Ethics in Science and New Technologies (2018). *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*. Brussel: European Commission.

European Political Strategy Centre (2018). *The Age of Artificial Intelligence. Towards a European Strategy for Human-Centric Machines*. Brussel: EPSC

European Political Strategy Centre (2018). *The Age of Artificial Intelligence. Towards a European Strategy for Human-Centric Machines*. Brussels: EPSC. Available online: https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategicnote_ai.pdf

Europese Toezichthouder voor gegevensbescherming (2015). *The EDPS Strategy 2015-2019*. Brussel: ETGB. Available online: https://edps.europa.eu/sites/edp/files/publication/15-07-30_strategy_2015_2019_update_en.pdf

Europese Toezichthouder voor gegevensbescherming (2017a). *Recommendations on specific aspects of the proposed ePrivacy Regulation*. Brussel: ETGB. Available online: https://edps.europa.eu/data-protection/our-work/publications/opinions/recommendations-specific-aspects-proposed-eprivacy_en

Europese Toezichthouder voor gegevensbescherming (2017b). *Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation).* Brussel: ETGB. Available online: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

Europese Toezichthouder voor gegevensbescherming (2017c). *Opinion 7/2017 on the new legal basis of the Schengen Information System*. Available online: https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_en.pdf

Europese Toezichthouder voor gegevensbescherming (2017d). *Opinion 11/2017 on the proposal for a regulation on ECRIS-TCN*. Available online: https://edps.europa.eu/sites/edp/files/publication/17-12-12_opinion_ecris_tcn_2017_0542_en.pdf

Europese Toezichthouder voor gegevensbescherming (2018a). *Ethics Advisory Group Report 2018*. Brussel: ETGB. Available online: https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf

Europese Toezichthouder voor gegevensbescherming (2018b). *Opinion 3/2018 on online manipulation and personal data*. Available online: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

FRA (2018). #Big Data: *Discrimination in data-supported decision making*. Vienna: FRA. Available online: http://fra.europa.eu/en/publication/2018/big-data-discrimination

Freese, C. & Dekker, R. (2018). *Samen werken met robots*. Amsterdam: De Burcht

Freese, C., Dekker, R., Kool, L., Dekker, F. & Est, R. van (2018). *Robotisering en automatisering op de werkvloer – bedrijfskeuzes bij technologische innovaties*. Den Haag: Rathenau Instituut

Frenken, K., Van Waes, A., Smink, M. & Van Est, R. (2017). *Eerlijk delen - Waarborgen van publieke belangen in de deeleconomie en de kluseconomie*. Den Haag, Rathenau Instituut.

Gemeente Eindhoven en Amsterdam (2017). ‘Spelregels voor de digitale infrastructuur in de stad’. Brief wethouders Depla en Ollongren.

Eindhoven/Amsterdam.

Geonovum (2017a). *Verkenning locatiegegevens en sociale platforms*. Amersfoort: Geonovum. Available online :https://www.geonovum.nl/sites/default/files/2017%20Rapport%20locatiegegevens%20en%20platforms.pdf

Geonovum (2017b). *Whitepaper Geo-standaarden*. Available online: https://docs.geostandaarden.nl/wp/basis-wpgs-20171222/

Heck, W. (2016). *Beperking opslag van data is tegenslag voor terreurbestrijders*. In NRC. Available online: https://www.nrc.nl/nieuws/2016/12/22/eu-hof-beperkt-opslag-van-data-tegenslag-voor-terreurbestrijders-5891446-a1537920

High Level Expert Group (2018). *A multi-dimensional approach to disinformation.*

Report of the independent High level Group on fake news and online disinformation. Luxembourg : Europese Commissie.

Hof van Justitie van de Europese Unie (2017). *Asociación Profesional Élite Taxi v Uber Systems Spain SL*. Available online: https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp- content/uploads/2017/12/European-Court-of-Justice-Uber-ruling-December- 20-2017-POLITICO.pdf

IBC (2017). *Report of the IBC on big data and health*. Paris: UNESCO. Available online: http://unesdoc.unesco.org/images/0024/002487/248724e.pdf

Kool, L., Timmer, J., Royakkers, L. & Van Est, R. (2017). *Opwaarderen. Borgen van publieke waarden in de digitale samenleving*. Den Haag: Rathenau Instituut.

Korthagen, I. & Van Keulen, I (2017). *Online meebeslissen - Lessen uit onderzoek naar digitale burgerparticipatie voor het Europees Parlement*. Den Haag: Rathenau Instituut.

Ladikas, M., S. Chaturvedi, Y. Zhao & D. Stemerding (red.) (2015). *Science and technology governance and ethics: A global perspective from Europe, India and China*, Heidelberg: Springer

Meulen, van der, B. & A. Rip (1998). Mediation in the Dutch science system. In: *Research Policy* 27(8) pp. 757-769.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2018a). NL DIGIbeter. Agenda Digitale Overheid. Den Haag: BZK.

Ministerie van Binnenlandse Zaken en Koninkrijksrelatie (2018b). *Digiprogramma 2018. Digitaliseren met vertrouwen*. Den Haag: BZK.

Ministerie van Buitenlandse Zaken (2018). *Mensenrechtenrapportage. Actualisering buitenlands mensenrechtenbeleid en resultaten*. Den Haag: BZ

Ministerie van Economische Zaken en Klimaat (2017). *Navigeren met wind in de zeilen. Voortgangsrapportage Bedrijvenbeleid 2017*. Den haag: Ministerie van Economische Zaken en KlimaatMinisterie van Economische Zaken en Klimaat (2018a) *Nederlandse Digitaliseringsstrategie*. Den Haag: EZK

Ministerie van Economische Zaken en Klimaat (2018b). *Roadmap Digitaal veilige hard- en software*. Den Haag: EZK

Ministerie van Justitie en Veiligheid (2018a). *Nederlandse Cybersecurity Agenda: Nederland digitaal veilig*. Den Haag: Ministerie van Justitie en Veiligheid

Ministerie van Justitie en Veiligheid (2018b). *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming*. Den Haag: Ministerie van Justitie en Veiligheid

Ministerie van Onderwijs, Cultuur en Wetenschappen (2018). *Aanbieding brochure Doorbraakproject en report Berenschot Toets SIVON*. Den Haag: OCW.

Ministerie van Sociale Zaken en Werkgelegenheid (2017). *Kamerbrief Kabinetsreactie SER-verkenning 'Mens en Technologie: samen aan het werk'*. Den Haag: SZW.

Ministerie van Sociale Zaken en Werkgelegenheid (2018). *Motie van de leden Verhoeven en Buitenweg, nr 118. 8 juni 2018*. Den Haag: Ministerie van Sociale Zaken en Werkgelegenheid

Ministerie van Veiligheid en Justitie (2017). *Reactie op het ACVZ-advies: "Profileren en selecteren".* Den Haag: Ministerie van Veiligheid en Justitie

Muller, C. (2017). *Kunstmatige intelligentie - De gevolgen van kunstmatige intelligentie voor de (digitale) eengemaakte markt, de productie, consumptie, werkgelegenheid en samenleving*. Brussel: Europees Economisch en Sociaal Comité

Munnichs, G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race - Over cyberdreigingen en versterking van weerbaarheid*. Den Haag: Rathenau Instituut.

Nationaal Cyber Security Centrum (2017a). *Cybersecuritybeeld Nederland 2017*.
Den Haag: NCSC. Available online: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2017.html

Nationaal Cyber Security Centrum (2017b). Wet gegevensverwerking en meldplicht cybersecurity. Den Haag: NCSC. Available online: https://www.ncsc.nl/actueel/nieuwsberichten/wet-gegevensverwerking-en-meldplicht-cybersecurity.html

Nationaal Cyber Security Centrum (2017c). ICT-beveiligingsrichtlijnen voor mobiele apps. Den Haag: NCSC. Available online: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-mobiele-apps.html

Nationale ombudsman (2017). *Digitalisering mag mensen niet uitsluiten*. Available online: https://www.rathenau.nl/nl/blog/nationale-ombudsman- digitalisering-mag-mensen-niet-uitsluiten

Nationale ombudsman (2018). *Onderzoeksagenda 2018*. Available online: https://www.nationaleombudsman.nl/system/files/bijlage/onderzoeksprogramma%202018%20DEF_0.pdf

Niezen, M. en P. Verhoef (2018). Digitale gezondheidsregie - Meer gegevens, meer grip? Den Haag: Rathenau Instituut

OESO (2018). *Tax Challenges Arising from Digitalisation: More than 110 countries agree to work towards a consensus-based solution*. Paris: OESO. Available online: http://www.oecd.org/newsroom/tax-challenges-arising-from-digitalisation-more-than-110-countries-agree-to-work-towards-a-consensus-basedsolution.htm

Onderwijsraad (2017). *Doordacht Digitaal*. Den Haag: Drukkerij Excelsior.

OSCE (2016). *UN Human Rights Council resolution on protection of human rights on the Internet a milestone for free speech, says OSCE Representative*. Wenen: OSCE. Available online: http://www.osce.org/fom/250656

Parlementaire Assemblee van de Raad van Europa (PACE). (2015) *Technological convergence, artificial intelligence and human rights (Motie 24 June 2015).* Brussel: PACE. Available online: http://www.assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=21951&lang=en.

Parlementaire Assemblee van de Raad van Europa (PACE) (2017).

Recommendation 2102 Provisional version (28 April 2017) Technological convergence, artificial intelligence and human rights. Brussel: PACE. Available online: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23726&lang=en

Planbureau voor de Leefomgeving (2017). *Mobiliteit en elektriciteit in het digitale tijdperk. Publieke waarden onder spanning*. Den Haag: Uitgeverij PBL.

Pluut, B. & M. de Jong (2018). E-health experts: Denk niet te gemakkelijk over zelfredzaamheid. Blogserie Beschaafde Bits. Den Haag: Rathenau Instituut.

Privacy International & Article 19 (2018). *Privacy and Freedom of Expression In the Age of Artificial Intelligence*. London: Privacy International & Article 19. Available online: https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf

Raad van Cultuur (2018). *Zicht op zo veel meer*. Den Haag: Raad voor Cultuur. Available online: http://toekomst-cultuurbeleid.cultuur.nl/sectoradviezen/audiovisueel

Raad van Europa (2018). *Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*. Strasbourg: Council of Europe.

Raad van Europa (1997). *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (Oviedo, 4.IV.1997)*. Brussel: European Treaty Series - No. 164

Raad voor de leefomgeving en infrastructuur (2015). *Verkenning technologische innovaties in de leefomgeving*. Den Haag: Raad voor de leefomgeving en infrastructuur

Raad voor de leefomgeving en infrastructuur (2017). *Technologie op waarde schatten – een handreiking*. Den Haag: Rli.

Raad voor de leefomgeving en infrastructuur (2018). *Stroomvoorziening onder digitale spanning*. Den Haag: Rli

Raad voor Volksgezondheid en Samenleving (2017). *Implementatie van e-health vraagt om durf en ruimte*. Den Haag: RVS

Rathenau Instituut & SER (2017). *Naar een verantwoorde digitale samenleving: van kwesties naar acties: Deel I, 6 december 2017*. Available online: https://www.rathenau.nl/sites/default/files/inline-files/Verslag%20conferenties.pdf en https://www.rathenau.nl/nl/digitale-samenleving/acties-voor-een-verantwoorde-digitale-samenleving

Royakkers, L., Timmer, J., Kool, L. and Van Est (2018) Societal and ethical issues of digitization. In: *Ethics and Information Technology* Vol 20, nr. 2, p.127-142

VVD, CDA, D66 en ChristenUnie (2017). *Vertrouwen in de toekomst. Regeerakkoord 2017 – 2021*. Available online: https://www.rijksoverheid.nl/regering/documenten/publicaties/2017/10/10/regeerakkoord-2017-vertrouwen-in-de-toekomst

SER (2015). *Werkloosheid voorkomen, beperken en goed verzekeren*. Den Haag: SER. Available online: https://www.ser.nl/~/media/db_adviezen/2010_2019/2015/werkloosheid-voorkomen.ashx

SER (2016). *Mens en technologie. Samen aan het werk*. Den Haag: SER. Available online: https://www.ser.nl/nl/publicaties/adviezen/2010- 2019/2016/mens-technologie.aspx

Sociaal en Cultureel Planbureau (2017). *De sociale staat van Nederland 2017*. Den Haag: SCP. Available online: https://www.scp.nl/Publicaties/Alle_publicaties/Publicaties_2017/De_sociale_staat_van_Nederland_2017

Staatscommissie parlementair stelsel (2017). *Probleemverkenning*. Den Haag: Staatscommissie. Available online: https://www.staatscommissieparlementairstelsel.nl/opdracht-en-aanpak

Staatscommissie Thomassen (2010). *Report Staatscommissie Grondwet. Den Haag: Staatscommissie Grondwet*. Available online: https://www.rijksoverheid.nl/documenten/rapporten/2010/11/11/rapport-staatscommissie-grondwet

Stemerding, D. & L. Kater (2005). *Public bio-ethics bodies as intermediary organisations*. Paper presented at the workshop on Intermediary Organisations, PRIME, University of Twente, 6-7 October.

Studiegroep Informatiesamenleving en Overheid (2017). *Maak Waar*. Den Haag: Studiegroep Informatiesamenleving en Overheid. Available online: https://www.rijksoverheid.nl/documenten/rapporten/2017/04/18/rapport-van-de-studiegroep-informatiesamenleving-en-overheid-maak-waar

UN General Assembly, Human Rights Council: resolution 20/08 adopted by the General Assembly, The promotion, protection and enjoyment of human rights on the Internet, 29 juni 2012, A/HRC/20/L.13, available online: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A.HRC.20.L.13_en.doc

UN General Assembly, Human Rights Council: resolution 26/13 adopted by the General Assembly, The promotion, protection and enjoyment of human rights on the Internet, 20 juni 2014, A/HRC/26/L.24, available online: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G14/059/67/PDF/G1405967.pdf?OpenElement

UN General Assembly, Human Rights Council: resolution 32/13 adopted by the General Assembly, The promotion, protection and enjoyment of human rights on the Internet, 27 June 2016, A/HRC/32/L.20, available online: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

V2_(2018). *Jaarverslag 2017*. Rotterdam: V2. Available online: http://v2.nl/organization/annual-reports

Van Eck, B.M.A. (2018). *Geautomatiseerde ketenbesluiten en rechsbescherming. Een onderzoek naar de praktijk van geautomatiseerde ketenbesluiten over een financieel belang in relatie tot rechtsbescherming*. Tilburg: Tilburg University

Van Est, R., Timmer, J., Kool, L., Nijsingh, N., Rerimassie, V. & Stemerding, D. (2017). *Regels voor het digitale mensenpark. 'Telen' en 'temmen' van de mens via kiembaanmodificatie en persuasieve technologie*. Den Haag: Rathenau Instituut. Available online: https://www.rathenau.nl/nl/publicatie/regels-voor-het-digitale-mensenpark

Van Est, R. & J.B.A. Gerritsen, met medewerking van L. Kool (2017). *Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality – Expert report written for the Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe (PACE).* Den Haag: Rathenau Instituut

Van Est, R. (2017). *Technologisch burgerschap: dé democratische uitdaging van de eenentwintigste eeuw*. (21 december 2017) Den Haag: Rathenau Instituut. Available online: https://www.rathenau.nl/nl/publicatie/technologisch-burgerschap-dé-democratische-uitdaging-van-de-eenentwintigste-eeuw

Van Est, R., E. de Bakker, J. van den Broek, J. Deuten, P. Diederen, I. van Keulen,

I. Korthagen en H. Voncken (2018). Waardevol digitaliseren – Hoe lokale bestuurders vanuit publiek perspectief mee kunnen doen aan het 'technologiespel'. Den Haag: Rathenau Instituut.

Van Keulen, I., Korthagen, I., Diederen, P. en Van Boheemen, P. (2018).

Digitalisering van het nieuws – Online nieuwsgedrag, desinformatie en personalisatie in Nederland. Den Haag: Rathenau Instituut

Hof, C. van 't, J. Timmer & R. van Est (red.) (2012). Voorgeprogrammeerd: Hoe het internet ons leven leidt. Den Haag: Boom Lemma uitgevers.

Vetzo, M., J. Gerards & R. Nehmelman (2018). *Algoritmes en grondrechten*. Utrecht: Universiteit Utrecht

Villani, C (2018). *For a meaningful artificial intelligence. Towards a french and european strategy*. Available online: https://www.aiforhumanity.fr/en

VN Mensenrechtenraad (2016).*The promotion, protection and enjoyment of human rights on the Internet. 27 Juni 2016 (A/HRC/32/L.20)*. Available online: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

Wetenschappelijke Raad voor het Regeringsbeleid (1976). *Instellingswet WRR, art.*
2a (30 juni 1976). Available online: http://wetten.overheid.nl/BWBR0003043/1998-01-21

Wetenschappelijke Raad voor het Regeringsbeleid (2016). *Big Data in een vrije en veilige samenleving*. Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid. Available online: https://www.wrr.nl/publicaties/rapporten/2017/04/24/weten-is-nog-geen-doen

Wetenschappelijke Raad voor het Regeringsbeleid (2017). *Weten is nog geen doen. Een realistisch perspectief op redzaamheid*. Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid.Available online: https://www.wrr.nl/publicaties/rapporten/2017/04/24/weten-is-nog-geen-doen

Widlak, A. & Peeters, R. (2018). *De digitale kooi. (On)behoorlijk bestuur door informatiearchitectuur*. Den Haag: Boombestuurskunde.

Parliamentary Papers

Appendix Proceedings II, 2016-2017, no. 2075

Appendix Proceedings II, 2017-2018, no. 1612

Proceedings II 2017-2018, 9

Parliamentary Papers I 2014-2015, CVIII, E Parliamentary Papers I 2014-2015, 33 750 XIII, E

Parliamentary Papers I 2016-2017, 34372

Parliamentary Papers I 2017-2018, 34775 VI, V

Parliamentary Papers II 2010-2011, 31570, no. 20

Parliamentary Papers II 2015-2016, 33009, no. 16

Parliamentary Papers II 2016-2017, 26643 and 32761, no. 426

Parliamentary Papers II 2016-2017, 32034, no. 22

Parliamentary Papers II 2016-2017, 34741, no. 2

Parliamentary Papers II 2017-2018, 26643 and 32761, no. 537

Parliamentary Papers II 2017-2018 32761, no. 120

Parliamentary Papers II 2017-2018, 32827, no. 126

Parliamentary Papers II 2017-2018, 32827, no. 127

Parliamentary Papers II 2017-2018, 34388, no. G

Parliamentary Papers II 2017-2018, 34851, no. 23

Parliamentary Papers II 2017-2018, 34861, no.2

Parliamentary Papers II 2017-2018, 26643, no. 488

Parliamentary Papers II 2017-2018, 26643, no. 490

Parliamentary Papers II 2017-2018, 26643, no. 496

Parliamentary Papers II 2017-2018, 26643, no. 508

Parliamentary Papers II 2017-2018, 29023, no. 228

Parliamentary Papers II 2016-2017, 33009, no. 39

Parliamentary Papers II 2016-2017, 33009, no. 42

Parliamentary Papers II 2017-2018, 33009, no.47

Parliamentary Papers II 2017-2018, 33009, no. 48

Parliamentary Papers II 2017-2018, 34588, no. 70

Parliamentary Papers II 2017-2018, 34775 VI, no. 88

Parliamentary Papers II 2017-2018, 34775 VII, no. 52

Parliamentary Papers II 2017-2018, 34775, no. 88

Parliamentary Papers II 2017-2018, 26643, no. 527

Parliamentary Papers II 2017-2018, 26643, no.529

Appendix 1 Parliamentary questions and motions

Via *desk research,* we mapped out which written Parliamentary questions and motions submitted in the period between January 2017 and June 2018 called for attention for the ethical and societal issues relating to the areas of technology we discussed in the introduction. We classified the submitted questions and motions according to the seven values from *Urgent Upgrade*: privacy, digital security, autonomy, control of technology, human dignity, justice and balances of power. In many cases, the questions and motions share interfaces with a series of different public values, but we have classified each with a single value (the one which seems much central with regard to the questions).

Privacy – House of Representatives

	2018 (27 Parliamentary questions)
1	Het bericht dat twee derde van 150 populaire websites de privacywet overtreedt
2	Ontoegankelijkheid van Amerikaanse nieuwssites door EU regels
3	Het bericht ‘Mkb kan uitzondering op nieuwe strenge privacywet wel vergeten’
4	Het bericht ‘ABN Amro wil klantdata gebruiken voor advertenties’
5	Het bericht ‘Gegevens huisdieren en hun baasjes op straat’
6	Wetgeving voor particulier en professioneel dronegebruik
7	De Algemene verordening gegevensbescherming (AVG) en de Belastingdienst
8	Het bericht ‘Privacywet of niet, Kadaster deelt privégegevens’
9	Het bericht ‘Jouw medicijnen worden straks misschien wel door een drone gebracht’
10	Het bericht dat Meld Misdaad Anoniem gegevens doorverkoopt
11	Gebruik informatie uit het Handelsregister voor facebook-targeting
12	Het gebruik van gegevens uit het handelsregister voor direct marketing aan ZZP’ers en kleine ondernemers
13	Het bericht dat informatie van de Kamer van Koophandel gebruikt wordt voor reclamedoeleinden
14	Het bericht dat tientallen medewerkers van het Hagaziekenhuis ongeoorloofd een medisch dossier hebben ingekeken
15	Het bericht ‘Tientallen snuffelden ongeoorloofd in medisch dossier Barbie’
16	Privacyschendingen door Facebook
17	Het report van de CTIVD over de AIVD en het gebrek aan privacy bij informatie-uitwisseling
18	Het bericht 'Hoe de digitale halsband van Magister de privacy van schoolkinderen nekt'
19	Privacyschendingen door Facebook
20	Gestolen politie-uniformen
21	Het bericht ‘Gemeente harkt te veel persoonsgegevens binnen’
22	De veiligheid van vrouwen op het internet
23	Het sociale mediagebruik van de politie
24	Kloksystemen op basis van vingerafdrukken
25	Locatiebepalingen bij 112 meldingen
26	Het delen van persoonsgegevens van gebruikers van Valys
27	Cambridge Analytica

	2017 (34 Parliamentary questions)
1	Het bericht “Sollicitant niet meer vogelvrij op internet.”
2	Het gebruik van spyware in China
3	Verhandelbare spionagesoftware en de persoonlijke levenssfeer
4	Het bericht dat de AIVD en het kabinet burgers misleiden
5	Gestolen data van Übergebruikers
6	Naming and shaming op internet
7	Het bericht dat de vingerafdruk op het Nederlandse paspoort nooit wordt gecontroleerd
8	Het bericht dat bedrijven ongevraagd klantgegevens delen met Facebook
9	Een droneverbod vanwege privacy
10	Het op straat belanden van gevoelige gegevens van 1800 kwetsbare leerlingen
11	Het bericht dat op station Amsterdam Centraal slimme reclameborden worden ingezet
12	Het bericht ‘reclameborden op Amsterdam CS weten wanneer en hoelang jij kijkt’
13	Het bericht dat het project met de slimme camera’s in de haven van Rotterdam stil ligt
14	Ov-chipkaartbedrijf Translink dat de reisgegevens van honderden studenten heeft doorgegeven aan de Dienst Uitvoering Onderwijs
15	Het overdragen van sociale media data van gewone Nederlanders aan de Amerikaanse overheid, de Muslimban en de onderhandelingen over de Amerikaanse preclearance faciliteiten op Schiphol
16	Patiënten die onder druk gezet worden om bijzondere persoonsgegevens af te staan in de geestelijke gezondheidszorg
17	Het artikel ‘Dubieuze gluurcamera gewoon te koop via Amazon’
18	Het bericht dat Google gebruikersgegevens in buitenlandse datacentra moet overhandigen aan de VS
19	Het bericht dat er camera’s hangen in de kleedkamers van fitness keten ‘Fit For Free’
20	Betalen door data te delen en de verkoop van consumentendata aan bedrijven en de overheid
21	Het bericht dat er een camera in een toilet in een café is geplaatst
22	De aanbesteding van mobiele telefonie
23	Het bericht 'Privacy van leerlingen groeit scholen boven het hoofd' en het report 'Doordacht Digitaal' van de onderwijsraad
24	Het bericht dat Google gebruikersgegevens in buitenlandse datacentra moet overhandigen aan de VS
25	Het bericht dat er in Almelo per app gestemd kan worden
26	De verkoop van browsergegevens
27	Het toestemmingsvereiste voor de verwerking van ROM gegevens
28	Het artikel ‘Een ongeluk. 112 aan de lijn, maar waar zit je precies?’
29	Mogelijke privacy risico's in de online belastingaangifte
30	Het bericht “Consumentenbond wil Bel-me-niet-Register ook voor ex-klanten”
31	Het onderzoek van de Consumentenbond over het Bel-me-niet Register
32	Inzage in e-mails van het ministerie van Algemene Zaken inzake de Teevendeal
33	Het herkenbaar uitzenden van beelden ten behoeve van de opsporing
34	De uitspraak van de Hoge Raad dat vergaand onderzoek in smartphones privacy-rechten schendt

	2018 (8 motions)
1	Motie van de leden Van Kooten-Arissen en Hijink over privacy- en burgerrechtenorganisaties actief betrekken bij het Informatieberaad Zorg
2	Motie van het lid Van Nispen over standaardmodellen voor het vragen van toestemming voor gegevensverwerking
3	Motie van het lid Kuiken over een beter Europees privacytoezicht

4	Motie van de leden Van Raak en Arissen over een voorstel waarin de sleepnetfunctie uit de wet wordt gehaald
5	Motie van het lid Van Nispen over meer geld voor de Autoriteit Persoonsgegevens
6	Motie van de leden Verhoeven en Van Nispen over de uitvoering van de additionele taken door de AP
7	Motie van het lid Koopmans c.s. over ervaringen en voornemens inzake de AVG
8	Motie van de leden Van der Staaij en Van Toorenburg over duidelijke richtlijnen voor de functionaris gegevensbescherming
	2017 (21 motions)
1	Motie van de leden Diertens en Van den Berg over ROM-data
2	Motie van het lid Kooiman over ROM gegevens
3	Motie van het lid Arissen over een verbod op het delen van ongeëvalueerde gegevens
4	Motie van het lid Arissen over de privacy van burgers in relatie tot de Wet op de inlichtingen- en veiligheidsdiensten
4	Motie van het lid Arissen over het vrijstellen van medische informatie
5	Motie van het lid Arissen over geen gegevens verzamelen en bewaren van burgers die geen doelwit zijn van de diensten
7	Motie van het lid Özdil over geen reisgegevens van studenten meer opvragen
8	Motie van de leden Özütok en Van Engelshoven over een heldere richtlijn over welke medewerkers welke gegevens mogen inzien
9	Motie van het lid Helder over knelpunten in de privacywetgeving wegnemen
10	Motie van het lid Van Oosten over de mogelijkheden en beperkingen in de privacyregelgeving voor informatiedeling tussen professionele partijen
11	Motie van het lid Van Dam over alleen transacties via derdenrekeningen
12	Motie van het lid Van Oosten over de mogelijkheden en beperkingen in de privacyregelgeving voor informatiedeling tussen professionele partijen
13	Motie van de leden Lodders en Geurts over cameratoezicht in relatie tot de huidige capaciteit van de NVWA
14	Motie van de leden Lodders en Geurts over nog niet overgaan tot vrijwillig cameratoezicht
15	Motie van het lid De Groot over monitoren van het gebruik van camerabeelden door de NVWA
16	Motie van het lid Grashoff over camerabeelden zonder restricties ter beschikking stellen aan de NVWA
17	Motie van het lid Verhoeven over een aanvullende grondwettelijke bescherming tegen inmenging door derden
18	Motie van de leden Van Toorenburg en Kuiken over het gebruik van camerabeelden bij de opsporing van drugscriminelen
19	Motie van de leden Omtzigt en Bashir over een extern en onafhankelijk onderzoek naar databeveiliging bij de Belastingdienst
20	Motie van het lid Schouten over risico's bij uitwisseling van data met buitenlandse diensten
21	Motie van het lid Koser Kaya over gratis toegang tot relevante contactgegevens van ambtenaren

Privacy – Dutch Senate

	2017 (1 motion)
1	Motie-Wezel (SP) c.s. over het uitsluitend verstrekken van no-hit gegevens voor opsporingsdoeleinden en de inlichtingendiensten (EK 33.542, H)

Digital security – House of Representatives

	2018 (16 Parliamentary questions)
1	Driekwart van de 500 duizend websites van het MKB die privacygevoelige informatie verwerken is kwetsbaar voor digitale inbraak.
2	Onveilige telefoons van Samsung
3	Het bericht ‘Agentschap Telecom slaat alarm over hackbare apparaten’
4	Het bericht ‘Luchtmacht klaar voor bewapende drone’
5	De risico's die de overbelasting van de elektriciteitsvoorziening brengt voor de digitale koppositie van Nederland
6	Het bericht dat mbo- en hbo-studenten onvoldoende cybersecurity kennis en vaardigheden aanleren
7	Het bericht ‘IT-controleurs: te weinig investeringen in cyberbeveiliging’
8	Het bericht 'Gevaarlijk pedohandboek ongestoord verspreid via internet'
9	Het bericht 'Een database om miljardenfraudes te voorkomen: in het VK kan ’t wél’
10	Onlineoplichting via datingsites
11	Exportcontrole op cybersurveillancegoederen
12	De overname chipbedrijf NXP door Qualcomm
13	De aanhoudende DDoS aanvallen op Nederlandse banken en de Belastingdienst
14	DDoS-aanvallen op banken
15	Het bericht ‘Nederland is niet up-to-date’
16	De berichten ‘Spionnenjacht blokt 5G’ en ‘Arena geen proeftuin voor nieuwste generatie mobiel internet’
	2017 (27 Parliamentary questions)
1	Nederlanders die probeerden omstreden spionagesoftware te verkopen aan Ecuador
2	Het bericht ‘Merendeel gemeenten mailt onveilig’
3	Het bericht ‘Cybersecurity hoogleraren vrezen dat Nederland digitaal onder water komt te staan’ en het bijbehorende position paper
4	De onveiligheid van “Internet of Things” in Nederland
5	Het bericht dat de smartphones van NAVO-troepen gehackt proberen te worden
6	Het bericht ‘Fox IT houdt zeggenschap staat af’
7	Het bericht dat het bedrijf Fox-IT de zeggenschap van de staat afhoudt
8	Het feit dat er een groei van 122% is geconstateerd in varianten van ransomware
9	Het bericht dat DNB het beheer van vertrouwelijke data wil uitbesteden
10	Nationale veiligheidseisen bij aanbestedingen van cruciale communicatiediensten van de overheid
11	Het bericht dat ziekenhuizen getroffen zijn door ransomware-aanvallen
12	Het bericht dat malware mogelijk energiebedrijven kan platleggen
13	Nationale veiligheidseisen bij aanbestedingen van cruciale communicatiediensten van de overheid
14	Het bericht dat de gemeente Groningen de ICT-voorzieningen privatiseert
15	De internationale cyberaanval en de ICT van de Overheid
16	De ICT-storing in het systeem van Amadeus waardoor overal ter wereld reserveringssystemen voor de luchtvaart uitvielen
17	Het bericht dat er binnen de gehele overheid is informatieveiligheid nodig is
18	Het bericht dat bedrijven nog te weinig doen aan digitale veiligheid
19	De beveiliging van websites van Nederlandse ambassades
20	Het bericht dat de CIA kwetsbaarheden in met het internet verbonden apparaten misbruikt

21	The berichten ‘Datalekken bij gemeenten; het is een beetje een zooitje’ en ‘Organisaties worstelen met nieuwe privacy wetgeving’
22	Het bericht ‘Overheid eist invloed bij cyberbeveiliger Fox-IT’
23	Het bericht dat een Brits bedrijf het IT-beveiligingsbedrijf dat Nederlandse staatsgeheimen beveiligd heeft overgenomen
24	Russische hackers die gebruikmaken van Nederlandse server
25	Het bericht dat meerderheid van de zorgsites onbeveiligd is
26	Het onderzoek dat een meerderheid van de zorgwebsites geen veilige HTTPS-verbinding heeft
27	De verdubbeling van het aantal datalekken door ziekenhuizen

	2018 (12 motions)
1	Motie van Kuiken en Van Der Staaij over een digitaal gebiedsverbod voor haatzaaien
2	Motie van de leden Van Oosten en Buitenweg over naming and shaming bij niet verwijderen van kinderpornografie
3	Motie van het lid Van Toorenburg c.s. over internetbedrijven die zich niet committeren aan de notice-and-take-down-procedures
4	Motie van het lid Paternotte c.s. over oplossingen voor de Sigint-functie
5	Motie van het lid Van Helvert over de app WeChat
6	Motie van het lid Diks over de capaciteit voor cyberdefensie
7	Motie van het lid Buitenweg over instelling van een EU-cybersecuritywerkgroep
8	Motie van het lid Verhoeven over doorgeven van onbekende kwetsbaarheden
9	Motie van het lid Alkaya over zorgaanbieders aanwijzen als aanbieder van essentiële diensten
10	Motie van het lid Van der Lee over de screening van buitenlandse investeringen
11	Motie van het lid Paternotte c.s. over certificering van op internet aangesloten apparaten
12	Motie van de leden Kuiken en Arno Rutte over een "digitaal gebiedsverbod"
	2017 (17 motions)
1	Motie van het lid Bruins Slot c.s. over investeren in cyber
2	Motie van het lid Amhaouch c.s. over digitalisering door het brede mkb
3	Motie van het lid Arissen over een verbod op hacken
4	Motie van de leden Von Martels en Amhaouch over de risico's van cyberaanvallen
5	Motie van het lid Hijink over hacktests op IoT-apparatuur
6	Motie van het lid Diks over het in EU-verband samenbrengen van militaire expertise op het gebied van cybersecurity
7	Motie van de leden Bruins Slot en Van Engelshoven over de betrouwbaarheid en veiligheid van de Ondersteunende Software Verkiezingen
8	Motie van de leden Hijink en Verhoeven over maatregelen om consumenten te beschermen tegen slecht beveiligde apparatuur
9	Motie van het lid Verhoeven c.s. over een mandaat voor het NCSC om (semi-)publieke instellingen te helpen bij cyber security
10	Motie van de leden Buitenweg en Verhoeven over een jaarlijkse test van de vitale ICT-infrastructuur
11	Motie van het lid Krol over het proactief delen van kennis over digitale veiligheid
12	Motie van het lid Hijink over het oprichten van een digital trust centre
13	Motie van het lid Aukje de Vries c.s. over het voor eind 2017 wegwerken van onvolkomenheden op het gebied van informatiebeveiliging
14	Motie van de leden Schouten en Omtzigt over het op orde brengen van de informatiebeveiliging en het beheer van het financiële systeem van de Tweede Kamer

15	Motie van het lid Amhaouch over een adequate beveiliging van hard- en software voor het verkiezingsproces
16	Motie van het lid Van Engelshoven over bevorderen dat mensen met tweestapsidentificatie inloggen via DigiD
17	Motie van het lid Schouten over extra middelen voor de CTIVD

Digital security – Dutch Senate

	2018 (2 motions)
1	Motie-Strik (GroenLinks) c.s. over de instelling van een onafhankelijke toetsingscommissie (EK 34.372, J)
2	Motie-Bredenoord (D66) c.s. over de AMvB waarin misdrijven kunnen worden aangewezen waarvoor een bevoegdheid tot binnendringen in geautomatiseerde werken wordt gecreëerd (EK 34.372, I)

Autonomy – House of Representatives

	2018 (10 Parliamentary questions)
1	Het bericht ‘Populaire games overtreden gokregels’
2	Het bericht 'Medische gegevens in eigen beheer op je computer of telefoon: vanaf volgend jaar is het mogelijk'
3	Het bericht 'Gegevens miljoenen Facebook-gebruikers gestolen voor politieke reclame'
4	Beïnvloeding door buitenlandse entiteiten van democratische verkiezingen
5	Nepnieuwsbestrijders van de EU die Nederlands nieuws beoordelen maar geen Nederlands spreken
6	Nepnieuws
7	Het bericht 'Online burgerinspraak kan leiden tot teleurstelling in politici'? en het report van het Rathenau instituut 'Online meebeslissen'?
8	Het door ‘EU vs Disinfo’ bestempelen van journalistieke verslaggeving tot nepnieuws
9	Het bericht ‘Meer gemeenten ruilen e-mail om voor online formulier’
10	Het verdwijnen van pinautomaten en de verminderende toegankelijkheid tot contant geld
	2017 (4 Parliamentary questions)
1	Massasurveillance door de Oezbeekse overheid
2	Onvoldoende mobiel bereik in delen van Brabant
3	Het niet tijdig beschikbaar zijn van digitale leermiddelen
4	Het bericht dat volgens de rechter een datavrije muziekbundel niet in strijd is met netneutraliteit
	2018 (15 motions)
1	Motie van het lid Becker over een centraal informatiepunt
2	Moties van het lid Verhoeven c.s. over pleiten voor keuzevrijheid voor gebruikers
3	Gewijzigde motie van de leden Kwint en Yesilgöz-Zegerius over het opheffen van EU versus Disinfo (t.v.v. 21501-34-286)
4	Motie van het lid Westerveld over een andere strategie voor EU versus Disinfo
5	Motie van de leden Sneller en Verhoeven over een Europese strategie tegen ondermijnende desinformatie

6	Motie van het lid Yesilgöz-Zegerius over afschaffing van EU versus Disinfo
7	Motie van de leden Kwint en Leijten over het opheffen van EU versus Disinfo
8	Motie van het lid Tielen over verbeteren van digitale vaardigheden
9	Motie van het lid Den Boer over de consequenties van activeren zonder e-mailaccount
10	Motie van het lid Omtzigt over de Berichtenbox van de Belastingdienst
11	Motie van het lid Özütok over het verbeteren van de Berichtenbox
12	Motie van het lid Paternotte over 5G-uitrol in buitengebieden
13	Motie van het lid Alkaya over behoud van netneutraliteit
14	Motie van de leden Van Raan en Paternotte over nummerportabiliteit verankeren in de Bankenwet
15	Motie van het lid Leijten over een actieve keuze voor digitale post
	2017 (14 motions)
1	Motie van de leden Voortman en Recourt over toegankelijker en transparanter ingerichte internetconsultaties
2	Motie van het lid Van der Molen over uitbreiding van de reikwijdte van de richtlijn door toevoeging van social media als uitstel niet haalbaar is
3	Motie van de leden Paternotte en Ellemeet over aandringen op uitstel van besluitvorming over de reikwijdte van de richtlijn ten aanzien van social media c.q. video sharing platforms
4	Motie van de leden Van der Molen en Verhoeven over vergroting van de weerbaarheid
5	Motie van het lid Baudet over een concreet plan voor een individueel digitaal stemsysteem
6	Motie van het lid Sienot c.s. over innovatieve oplossingen voor bereikbaarheid
7	Motie van het lid Verhoeven c.s. over beïnvloeding van democratische processen door nepnieuws
8	Motie van de leden Westerveld en Van den Hul over de mediawijsheid onder senioren en volwassenen
9	Motie van de leden Ellemeet en Yesilgöz-Zegerius over onderzoek naar de staat van de Nederlandse onderzoeksjournalistiek
10	Motie van de leden Ellemeet en Yesilgöz-Zegerius over inzicht in middelen van de publieke omroep voor onderzoeksjournalistiek
11	Motie van het lid Bouwmeester c.s. over een lange termijndoel opstellen dat leidt tot een digivaardig Nederland
12	Motie van het lid Omtzigt over belastingbrieven zowel digitaal als op papier versturen
13	Motie van de leden Kuiken en Verhoeven over oneigenlijke beïnvloeding van verkiezingen
14	Motie van het lid Öztürk over een fonds voor de aanpak van nepnieuws

Control of technology – House of Representatives

	2018 (3 Parliamentary questions)
1	Het bericht ‘Algoritme voorspelt wie fraude pleegt bij bijstandsuitkering’
2	De berichtgeving over het proefschrift van Marlies van Eck van de Tilburg University
3	De ontwikkeling en het gebruik van ‘killer robots’
	2017 (1 Parliamentary question)
1	Feitelijke vragen n.a.v. de Zembla-uitzending "Belastingdienst overtreedt willens en wetens privacywet"

	2018 (3 motions)
1	Motie van het lid Verhoeven c.s. over openbaarheid van de werking en de broncode van algoritmen en analysemethoden
2	Motie van de leden Verhoeven en Buitenweg over openbaarmaking van databestanden, algoritmes en analysemethodes van SyRI
3	Motie van het lid Buitenweg over verruimen van de mogelijkheden voor collectieve procedures bij de rechter
	2017 (0 motions)

Human dignity – House of Representatives

	2018 (6 Parliamentary questions)
1	Het bericht 'Computer zegt nee. Hoe Saskia twintig jaar vastliep in het systeem'
2	Een vorm van slavernij bij PostNL
3	Het bericht 'Blussen? Dat doen we straks met een robot'
4	Stress veroorzakende klantbeoordelingssystemen
5	Het bericht ‘Callgirl voor Albert Heijn’
6	Misstanden met arbeidsmigranten bij distributiecentra van Albert Heijn
	2017 (0 Parliamentary questions)
	2018 (0 motions)
	2017 (1 motion)
1	Motie van het lid Marcouch over vergroten van de capaciteit bij de douane voor toezicht, handhaving en opsporing

Justice – House of Representatives

	2018 (4 Parliamentary questions)
1	De berichten 'Debacle met digitale rechtspraak was voorzienbaar' en 'Digitalisering blijft steken'
2	Het bericht ‘Robotrechter e-Court is een groot en niet-transparant zwart gat?’
3	E-Court
4	Achterstanden bij de digitalisering van de rechtspraak
	2017 (0 Parliamentary questions)

	2018 (1 motion)
1	Motie van het lid Buitenweg over vormen van digitale arbitrage
	2017 (1 motion)
1	Motie van de leden Segers en Van Dam over Duitse boetewet socialmediabedrijven

Balances of power – House of Representatives

	2018 (10 Parliamentary questions)
1	Maaltijdbezorger Deliveroo ronselt minderjarigen
2	De pakketsorteerders die via een schijnconstructie worden ingehuurd bij PostNL
3	De ongevallenverzekering voor Deliveroo bezorgers
4	Het omgaan met de mogelijkheden om deelplatforms te kunnen onderwerpen aan nationale regels
5	Validatie van 80%-norm arbeidsovereenkomst postsector
6	De mogelijkheid van een Airbnb-hypotheek
7	De gevolgen van dalende postvolumes voor de postbezorging
8	Dat Schiphol Deliveroo inzet voor bezorging aan de gate
9	16 miljard belastingontwijking van Google via Nederland
10	De uitspraak van het Europese Hof van Justitie dat Uber een taxibedrijf is
	2017 (4 Parliamentary questions)
1	De eenzijdige opgelegde commissieverhoging door Thuisbezorgd.nl
2	Een gemeentelijke meldplicht voor verhuur van woningen via digitale platforms
3	Het bericht dat maaltijdbezorger Deliveroo alle koeriers in loondienst gaat vervangen door (schijn)zelfstandigen
4	Het bericht dat maaltijdbezorger Deliveroo alle koeriers in loondienst gaat vervangen door (schijn)zelfstandigen
	2018 (5 motions)
1	Motie van de leden Paternotte en Wörsdörfer
2	Motie van de leden Van der Lee en Paternotte over vakantieverhuur van woningen via digitale platforms
3	Motie van de leden Van Ojik en Asscher over het belasten van digitale activiteiten
4	Motie van de leden Asscher en Van Ojik over belastbaarheid van internetgiganten
5	Motie van de leden Alkaya en Moorlag over de onlinemarkt voor aan huis bezorgde maaltijden
	2017 (6 motions)
1	Motie van het lid Pieter Heerma c.s. over de situatie op de markt voor maaltijdbezorging
2	Motie van het lid Nijboer c.s. over digitale diensten betrekken in de belastingheffing
3	Motie van het lid Van der Lee over het gebruik van convenanten in de deeleconomie
4	Motie van het lid Hijink over de juridische status van deeleconomieplatforms
5	Motie van het lid Gijs van Dijk c.s. over de fietskoeriers van Deliveroo
6	Motie van de leden Wiersma en Van Weyenberg over de toekomst van de arbeidsmarkt

Balances of power – Dutch Senate

	2018 (1 motion)
1	Motie-Duthler (VVD) c.s. over digitale transformatie (EK 34.775 VI, V)

Appendix 2 The significance of public governance

Governance as social control

Etymologically, the term 'governance' is related to the Greek term *kubernein*, which means steering a boat or wagon. The philosopher Plato was the first to use the word to describe deliberately controlling the actions of large groups of people to achieve desired results and avoid risks and unwanted outcomes (Hoppe 2010, 10). Public governance is therefore essentially all about setting direction in society.

Governance is an ambiguous concept, and it is easy to lose one's way in the extensive literature on the subject. Below we introduce a number of insights and concepts from that literature, which can help us to consider the governance of the societal and ethical aspects of science and technology.

Governance of public issues

Governance serves to deal with public issues. By this we mean social problems that can only be solved by taking collective action (according to Hoppe, 2010). In this way, governance practices and processes are formed around certain issues in a communal struggle with political problems, and the search for potential solutions. The free exchange of arguments in society and a means of exercising power, in other words reason and power, play a role (Jaspers 1974).

On the one hand, it is about identifying and addressing problems and on the other hand solving them. Hoppe (2010, 17-18) distinguished three processes:

6. underpinning the problem (*puzzling)*;
7. seeking political support (*powering*); and
8. political participation (*participation)*.

The first process, for example, involves using scientific knowledge to properly assess the problem, and to ascertain the extent to which it has an impact on the public, and requires government action.

The second process is about obtaining political support: can sufficient political pressure and influence be drummed up to place the problem on the political and policy agenda? The problem is after all constantly competing for the state's limited attention and problem solving capacity.

The third process concerns participation: who is involved and especially who is not involved in defining the problem and determining the solutions, the instruments and shaping the institutions? Which public interests or values are better articulated and represented?

From the perspective of a democratic state subject to the rule of law, governance must necessarily satisfy a number of conditions. In recognising that there are numerous failing or fragile states across the world, the World Bank developed the concept of *good governance* in 1994:

> 'Governance is epitomized by predictable, open, and enlightened policymaking (i.e. transparent processes); a bureaucracy imbued with a professional ethos; an executive arm of government accountable for its actions; and a strong civil society participating in public affairs; and all behaving under the rule of law.' (World Bank 1994, vii).

This definition is still valid today. Its central element is how government interacts with society.

Governance for designing interactions between government and society

The concept of governance implies that the government is not seen as the only guardian of public interests and that the control of society does not just take place through formal instruments such as legislation and regulation. Public services are delivered by a network of actors in the public and private sector (Van Kersbergen & Van Waarden 2001). In other words: the responsibilities for providing public services are spread over a network of public and private entities.

The government is a network partner and exercises control in interaction with other parties, applying a very diverse and extensive combination of formal and informal practices. Alongside traditional forms of coercion, command & control, this may also involve encouraging public debate, negotiations, collaboration, joint vision forming and the establishment of alliances (see Van Kersbergen & Van Waarden 2004: 151-152).

Governance can also be a response to public opposition, lack of support, institutional distrust or the complexity of issues. The Dutch government has for many years cooperated with various actors in society. However, in recent decades, the desire for governance has grown in response to digitalisation, privatisation and internationalisation (Hajer et al. 2004).

There are a number of governance concepts circulating that refer to specific types of interaction between the government and civil society actors.

In the case of multi-stakeholder governance, actors from industry, society and government together develop a joint approach to issues that affect them all, but which are too complex to tackle effectively without cooperation. One such issue, already mentioned above, is internationalisation.

Alongside interaction between public and private actors, many issues also require discussions between various layers of administration, for example at European, national, regional and local level. These dynamic administrative processes are contained in the term multi-level governance:

> ‘The sharing of policy-making competencies in a system of negotiation between nested governments at several tiers (supranational, national, regional and local) on the one hand and private actors (NGOs, producers, consumers, citizens, etc.) on the other’ (Van Tatenhove & Liefferink, quoted in Hajer et al. 2004: 18).

When describing the specific interaction between government parties, citizens and civil society groups, the term ‘deliberative governance’ is often used. Key factors are democratic values and the quality of the exchange of visions and interests. Deliberative practices are mostly formed in a reaction to the laborious political-administrative handling of sensitive social problems, and in situations where there is mutual distrust and limited exchange of arguments (Hajer et al. 2004). Deliberation can be a means of building up institutional trust and seeking workable solutions.

Meta-governance of the governance system

Governance, then, is the collective control of our society. Referring to the original meaning of the word, Kooiman defines governance as a ‘hypercomplex socio-cybernetic system’ (quoted in Blatter 2012, 14). In other words, today it is no longer relevant to simply view governance as how these issues are dealt with by government. It is equally essential to keep a watchful eye on the entire system of governance arrangements in society in order to recognise, discuss, investigate and address public concerns, and to find, implement and evaluate possible solutions for them. The legitimate and effective organisation of such procedures often requires the involvement of a diverse range of institutes and administrative and social processes. Together, these form what we call a governance ecosystem.

The issue with governance, therefore, is whether the current governance ecosystem, representing the entire governance arrangement surrounding a particular public problem, is functioning well.

According to Hoppe (2010), two search processes play a role in improving a governance ecosystem.

1. The first concerns the institutions. Certainly when new problems arise, there is often a lack of institutional structure. Hajer & Wagenaar (2003) speak of an 'institutional void', where shared normative frameworks and organisational competences are lacking, and it is unclear who is responsible for what. Sociologist Ulrich Beck refers to this as 'organised irresponsibility' (Beck 1988), which he sees as a key feature of our high-tech risk society (Beck 1992).

   The establishment of institutions from the bottom up, or the expansion and improvement of existing institutions requires among other things institutional entrepreneurship. Hoppe (2004) uses the term meta-governance, since it is a question of controlling the governance of problems, or rather the structuring of the governance ecosystem in which collective problems can be identified and addressed.

2. The second search process refers to the organisation of social involvement, and alignment with the perceptions of ordinary citizens.

Relevant questions from a governance perspective

The above brief introduction raises numerous questions concerning the definition of governance, as well as the meta governance of problems (how the governance ecosystem is structured and how it works).

Questions regarding the governance of problems include:

- Which public problems have been identified?
- Which interests or values are well or less well articulated?
- How do the various actors in society and politics discuss these problems?
- How are problems placed on the political or other agendas?
- Which parties have been involved in the debate and the shaping of policy?
- Which solutions have been put forward and institutionalised?
- The questions relating to the meta governance of problems include:
- What institutions are in place to discuss public problems and raise them at a political level?
- How does consultation take place between public and private actors, and between governments, ordinary citizens and civil society organisations?
- How are public values institutionally safeguarded?
- Which institutions have been established over the years to bring this about?
- What does the governance system for a particular issue look like?

Bibliography accompanying this appendix

Beck, U. (1988). Gegengifte. Die Organisierte Unverantwortlichkeit. Frankfurt/Main: Suhrkamp.

Beck, U. (1992). Risk Society. Towards a New Modernity. London: Sage.

Blatter, J. (2012). Forms of political governance: Theoretical foundations and ideal types. Lucerne: University of Lucerne.

Hajer, M.A. & H. Wagenaar (red.) (2003). Deliberative policy analysis: Understanding governance in the network society. Cambridge: Cambridge University Press.

Hajer, M.A., J.P.M. van Tatenhove & C. Laurent (2004). Nieuwe vormen van governance: Een essay over nieuwe vormen van bestuur met een empirische uitwerking naar de domeinen van voedselveiligheid en gebiedsgericht beleid. Bilthoven: RIVM.

Hendriks, F. & F. Drosterij (2010). Goed bestuur in de stad: wat staat op het spel?

In: Bestuurskunde 19(4), pp. 6-18.

Hoppe, R. (2010). The governance of problems: Puzzling, powering and participation. Bristol: The Policy Press.

Jaspers, K. (2012/1965). Kleine Schule des philosophischen Denkens. München: Piper.

Kersbergen, K. van & F. van Waarden (2001). Shifts in governance: Problems of legitimacy and accountability. Den Haag: NOW.

Kersbergen, K. van & F. van Waarden (2004). ‘Governance’ as a bridge between disciplines: Cross-disciplinary inspiration regarding shifts in governance and problems of governability, accountability and legitimacy. In: European Journal of Political Research 43, pp. 143-171.

O’Toole, L.J. (2000). Research and policy implementation: Assessment and prospects. In: Journal of Public Administration Research and Theory 10, pp. 263-288.

World Bank (1994). Governance: The World Bank’s experience. Washington D.C.: World Bank.

Open Access
The Rathenau Instituut has an Open Access policy. Reports, background studies, scientific articles and software are freely available. Research data will be available, subject to the legal provisions and ethical standards for research on third-party rights, privacy and copyright.

Contact details
Anna van Saksenlaan 51 P.O. Box 95366
2509 CJ The Hague
The Netherlands +31(0)70-342 15 42
info@rathenau.nl www.rathenau.nl

The Rathenau Instituut stimulates public and political opinion forming on social aspects of science and technology. We perform research and organise debate relating to science, innovation and new technologies.

Rathenau Instituut