Rathenau Instituut

Urgent Upgrade

Protect public values in our digitized society

Report

Urgent Upgrade

Protect public values in our digitized society

Linda Kool, Jelte Timmer, Lambèr Royakkers and Rinie van Est

Urgent Upgrade

Protect public values in our digitized society

Linda Kool, Jelte Timmer, Lambèr Royakkers and Rinie van Est

Rathenau Instituut
Anna van Saksenlaan 51
PO Box 95366
2509 CJ The Hague
Telephone: 070-342 15 42
E-mail: info@rathenau.nl
Website: www.rathenau.nl
Publisher: Rathenau Instituut

Editor: Science stories
Translation: Val Kidd
Illustrations: Rikkers Infographics
Cover photo: iStock
Design: Rathenau Instituut
Printing: Rathenau Instituut

Preferred citation:
Kool, L., J. Timmer, L. Royakkers en R. van Est, *Urgent Upgrade - Protect public values in our digitized society*. The Hague, Rathenau Instituut 2017

Rathenau Instituut has an Open Access policy. Published 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.

Foreword

My diary had a lock on it. I could write down whatever I liked because no-one else ever read it. Digitization has put an end to that. Your e-reader is looking over your shoulder, monitoring which passages interest you most. And your childrens’ toys are nowadays so *smart* that the manufacturer is listening in via the Internet. Is that bad? Yes.

The current study 'Opwaarderen – safeguarding public values in the digital society' describes how the far-reaching digitization of society is raising fundamental ethical and societal issues. It reveals that governments, regulators, industry and society are not yet fully equipped to deal with this new set of challenges. At stake are important public values and human rights such as privacy, equal treatment, autonomy and human dignity.

Rathenau Instituut carried out this study as a result of a motion tabled in the Dutch Senate on 23 September 2014, asking the government to investigate the desirability of a committee that can advise on the ethical aspects of the digitization of society. The motion surmised that digitization is compromising some important values. Our investigation confirmed this is the case.

Rathenau Instituut was established three decades ago to investigate new science and technology and their impact on society. The key issue at that time was automation. Currently we are looking at digitization. Having analysed the effects of this development on the labour market, last year we presented our findings on big data, data in the field of medicine and digital coaches.

Now we are comprehensively investigating which technologies are expected to shape the digital society in the coming years, which societal and ethical challenges the process will evoke, and to what extent these challenges are already part of the societal and political agenda and also institutionally embedded. We identify blind spots, draw up a list of necessary actions and look at what role a committee could play.

I am grateful to the Senate for their knowledge question. I would also like to thank staff at the Ministry of the Interior and Kingdom relations and the supervisory committee: Corien Prins, Jeroen van den Hoven, Inez de Beaufort, Victor Bekkers, Heleen Janssen and Meine Henk Klijnsma. We hope that our study will help to both enlighten and energize future discussions.

Our diaries are now digital. The locks are gone. But we are not powerless. If government, industry and society take the right actions, we can further shape digitization in a responsible way.

Melanie Peters
Director Rathenau Instituut

Summary

The far-reaching digitization of society raises fundamental ethical and societal issues. The government, industry and society are not yet adequately equipped to deal with these new issues. This challenges important public values and human rights such as privacy, equity and equality, autonomy and human dignity. Great efforts need to be made at all levels of government and society to steer the digitization of society in the right direction. We are by no means powerless, however. Provided that the government, industry and society take appropriate action, we can provide the digital society with a sensible upgrade.

Motion by the Dutch Senate: explore the desirability of appointing a committee

In September 2014, the Senate tabled a motion requesting the government to ‘ask Rathenau Instituut to explore the desirability of appointing a committee that could advise on the ethical aspects of the digitization of society’ (see Box 1). The motion was signed by a large number of political parties. In accordance with the Senate’s request, the Dutch Ministry of the Interior and Kingdom Relations has asked Rathenau Instituut to formally investigate this matter. The present report is the result of that investigation.

The motion refers to the emergence of the Internet of Things, which presents both opportunities and threats. The motion reflects the Senate’s concern that important values are being impacted by digitization. This is indicated by the fact that the motion refers not only to the technological effects of digitization, but also to the ‘*social, socio-legal and socio-psychological impacts*’. The motion also expresses a deeper, underlying concern, that existing political and administrative institutions may not be sufficiently equipped to address new challenges arising from the digitization of society. The Rathenau Instituut’s investigation supports the concerns expressed by the Senate.

Box 1 Motion by Senator Gerkens presented on 23 September 2014

The Senate, having heard the deliberations, concludes that the digital technology involved in *the Internet of Things* will connect everything and everyone with each other; it further concludes that this unstoppable development will present opportunities for society, but also poses threats; it considers that the impact of this digital development on society is not just technological, but also societal, socio-legal and socio-psychological; it asks for the government to request that Rathenau Instituut investigates the desirability of a committee which can advise on the ethical aspects of the digitizing society, and proceeds with the day’s agenda.

Signed by Senators Gerkens, Franken, K.G. de Vries, Strik, Duthler, Van Boxtel.

The questions addressed

The central question of this study concerns the desirability of appointing a committee to advise on the ethical aspects associated with the digitization of society. To answer that question, three sub-questions are examined in this report:

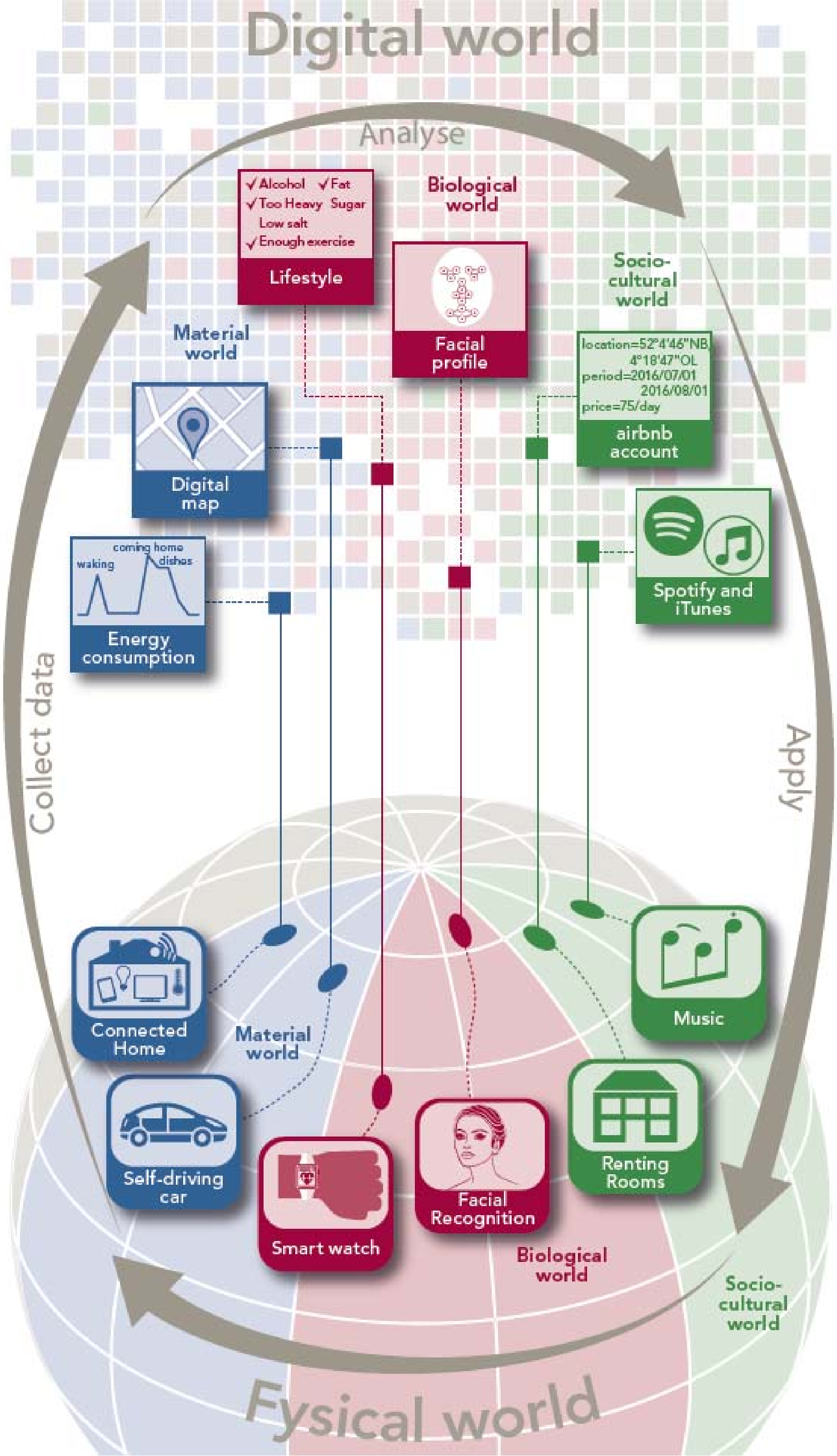
1. On which specific technologies is the digitization of society based (both in the past and in the coming 5 to 10 years)?
2. What kind of societal and ethical issues does the digitization of society raise?
3. To what extent do these issues challenge the current governance system? That is, which issues are – or are not – being placed on the political agenda? Which issues are – or are not – being addressed by existing Dutch institutions? Are there any blind spots, in terms of how emerging ethical and societal issues are being handled? What role could a committee play in this context?

The new wave of digitization

The concept of digitization refers to a large cluster of digital technologies such as robotics, the Internet of Things, artificial intelligence and algorithms, big data, digital platforms, biometrics, persuasive technology, augmented reality and virtual reality. Together they are generating a new wave of digitization. Through these technologies, ever more aspects of our physical world are being digitized: 1. the material world (our streets, buildings, homes, production processes), 2. the biological world (our bodies and minds) and 3. the socio-cultural world (our social environments including our work). For instance, virtual representations are entering the physical world: the digital world is growing, and technologies such as artificial intelligence and automated algorithms are increasingly being used to process the data in that world.

This study finds that the physical world and the digital world are becoming ever more closely intertwined. There are continuous feedback-loops between them. People, objects or processes in the physical world are first measured in bits and bytes and then analysed (or profiled) in the digital world. These analyses in turn are then immediately used to modify products and services in the physical world. For example, smart homes measure the temperature in the dwelling, analyse the preferences of their occupants, and automatically adjust the thermostat to the desired temperature, at the desired time. Then there are smart cars, which measure the physical world around them via numerous sensors and cameras, while maintaining continuous connections with internet servers that process this information and retrieve map details or traffic updates. The cars then use the results of these analyses to find their way to their destination (see Figure 1). The emergence of these continuous, *cybernetic*, feedback loops, appears to represent a new phase in the digitization of society.

Figure 1 New phase in the digital society



Public values at stake

The new wave of digitization is, therefore, leading to a world in which continuous feedback and real-time management and control are increasingly important principles for a range of services. This is exerting a strain on important public values such as equity and equality, privacy, autonomy and human dignity. We have clustered these into seven topics (see Table 1). This view is supported by recent news reports. For instance, the software used by judges in the United States to calculate the chances that a suspect will re-offend has been found to involve an element of discrimination in some cases. The use of software to determine where extra police presence is needed can create a self-fulfilling prophecy. In any given area, an increase in police numbers is reflected by a rise in the number of offences recorded (many eyes see more than one pair of eyes). This data is then incorporated into computer analyses, causing the software to predict a rise in the crime rate at that location. Data surveillance can unconsciously influence a user's identity, and lead to 'filter bubbles', in which the system only suggests news, information and contacts that match the user's previous behaviour, choices and interests. Finally, there is the use of robots and software in healthcare, law, banking and other sectors. The question here, which we need to address as a matter of urgency, is what things do we want to leave to robots and what would be a minimum level of human involvement consistent with humane care or with taking on meaningful responsibility. Another issue is that public services are increasingly dependent on software (including self-learning software) developed by private parties. This makes it difficult to track the choices made by such software, and the resultant effects. Might judges or doctors who use system X reach different verdicts or diagnoses than their counterparts who use system Y?

Table 3.1 Overview of ethical and societal issues related to digitization

Central topic	Issues
Privacy	Data protection, privacy, mental privacy, spatial privacy, surveillance, function creep
Autonomy	Freedom of choice, freedom of expression, manipulation, paternalism
Safety and security	Information security, identity fraud, physical safety
Control over technology	Control and transparency of algorithms, responsibility, accountability, unpredictability
Human dignity	Dehumanization, instrumentalization, deskilling, desocialization, unemployment
Equity and equality	Discrimination, exclusion, equal treatment, unfair bias, stigmatization
Balances of power	Unfair competition, exploitation, shifting relations consumers and businesses, government and businesses

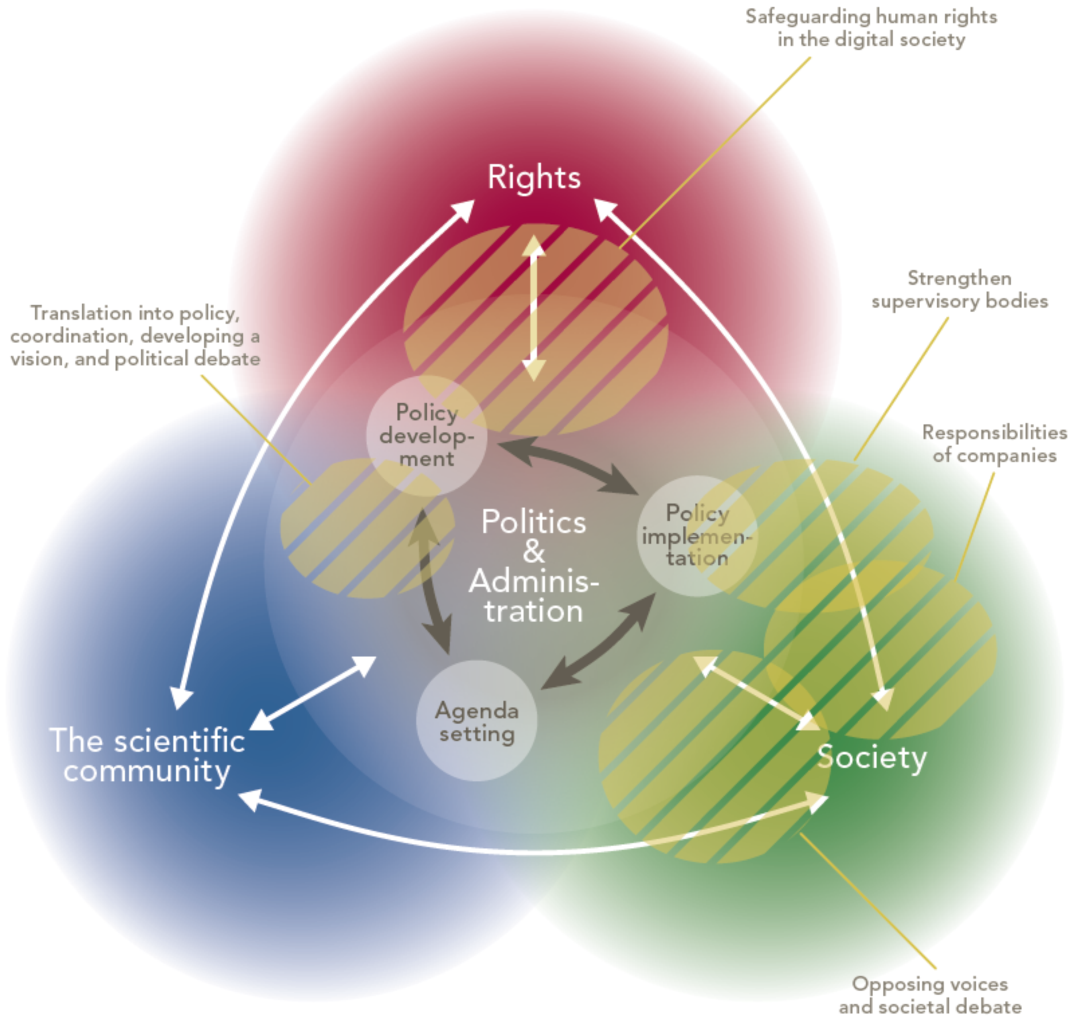
Blind spots in the governance landscape

Thus, various ethical and societal challenges are emerging in the wake of the new wave of digitization. Important public values are at stake here, values that are closely related to fundamental rights and human rights. That raises the question of whether our current regulatory frameworks and supervisory arrangements have the powers needed to adequately protect these fundamental rights. In this study, Rathenau Instituut explored the ethical and societal challenges of digitization and the challenges of the current governance landscape. We conducted a comprehensive analysis to determine which actors and institutions are demanding attention for which issues, and what actions they are taking to address these challenges. This analysis involved an examination of the role of the scientific community and knowledge institutions (what issues are they flagging up?), the role of institutions responsible for protecting human rights, the role of civil society and the roles of policy makers and politicians in agenda setting, in political decision making, and in the implementation of policy.

Our analysis of the governance landscape shows that the protection of public values currently leaves much to be desired. Digitization leads to conceptual confusion about which rules are relevant, and about how these should be applied. In some cases, this results in an initial reluctance to use existing frameworks, even where these are applicable. In other cases, we see that digitization is creating a need for new frameworks capable of protecting important values in the digital society. We conclude that five important blind spots have emerged (see Figure 2) in the current governance system for ethical and societal issues raised by digitization:

- Translating emerging societal and ethical issues into policy, inter-ministerial consultation and coordination on digitization, and the political debate on these emerging issues.
- Safeguarding fundamental rights and human rights in the digital society.
- Strengthening supervisory bodies and seeing to it that they consult one another.
- New responsibilities for companies that develop digital products and services.
- Strengthening ‘opposing voices’ and societal debate: strengthening civil society, augmenting the public’s knowledge and skills, and promoting public debate on digitization.

Figure 2 Blind spots in the governance landscape



Rathenau Instituut

These blind spots mainly involve emerging and urgent societal and ethical issues evoked by the use of artificial intelligence, robotics and the Internet of Things in relation to topics such as equity and equality, autonomy, human dignity, responsibility, and imbalances of power between consumers and businesses, or between members of the public and government bodies. Take, for instance, digital service providers (e.g. in the sharing economy or social media) with a dominant market position. With few alternatives, users are increasingly dependent on such providers for their income or for information. Our research shows that governance structures have yet to emerge in these areas. The associated public debate needs to become more clearly defined. In addition, issues identified in the political domain are not being translated into tangible policy actions.

The governance system is more highly developed in the areas of privacy, the protection of personal data and security. Although, here too, some fundamental questions are still unresolved, there is a growing awareness of the importance of privacy protection among members of the public, the government and the business community. Supervisory bodies are being granted greater powers. At the European level, too, the regulations are being strengthened. A range of government programmes and civil society programmes have been established to encourage people to acquire digital skills and to adopt safe digital practices.

Upgrading: Action programme for a responsible digital society

Digital innovations are developing at a breath-taking pace. Digitization has penetrated the very fabric of society. The continuous stream of technical upgrades is creating many new opportunities for the economy and for society at large. At the same time, however, it is raising fundamental societal and ethical questions. The digitization of society is exerting a strain on essential public values. In the coming years, society will have to deal with digitization issues and with the associated ethical and societal challenges. It is time to recognize the fact that digitization is having a major impact on the very foundations of society, and to ensure that public values and fundamental rights in the digital age are properly safeguarded. That requires an upgrade of the governance system, involving systematic strengthening by means of structural safeguards for societal and ethical values.

A key requirement of this upgrade is that all parties within society must take action to steer digitization in the right direction. It would be irresponsible of the government, the business community and society to turn a blind eye to the fundamental impact of digitization. All of these actors have responsibilities in terms of dealing with the societal and ethical aspects of digitization. It is up to the government to formally launch this action programme. However, government cannot solve the issues on its own, industry and civil society need to act as well.

Accordingly, our key conclusion is that the Senate's concerns **about the ethical and societal impact of digitization**, as formulated in the motion tabled by Senator Gerkens, **are justified**. In this motion, the Senate reflects on the desirability of establishing a committee to advise on the ethical aspects of the digital society. Our analysis shows that, **to safeguard essential public values, the governance landscape needs to be substantially strengthened at several points in the area of societal and ethical aspects of digitization**.

By its very nature, a committee would be unable to resolve the blind spots in the governance landscape. The complex task of strengthening the governance landscape demands that all parties live up to their responsibilities and make a collective effort to safeguard public values in the digital society. One of the attendant risks of appointing a committee is that societal and ethical issues will be 'parked' with the committee, while parties in the field and those at political-governance level take a 'wait and see' attitude. Moreover, the present study has already completed much of the groundwork that would normally be carried out by a committee of this kind. The study has identified the societal and ethical digitization issues we are facing. To tackle these issues, it has also pinpointed various blind spots in the governance landscape. It also suggests a range of actions that each of the parties involved could pursue, to strengthen their individual roles within the governance system.

Accordingly, Rathenau Instituut's key message is 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.

We are putting forward a five-part proposal that will enable policymakers, businesses and civil society organizations to responsibly upgrade the governance landscape:

1. Appoint an interdepartmental working group charged with shaping a government vision on how to deal with the societal and ethical significance of digitization, and with ensuring coordination in the political-governance domain.
2. Strengthen the role and position of supervisory bodies.
3. Draw up a 'Digitization Agreement' formulating the commitments 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 digitization, 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 digitization issues.

Each action is subdivided into a number of specific action points, which are explained below.

1. Appoint an interdepartmental working group charged with shaping a government vision on how to deal with the societal and ethical significance of digitization.

Action points for the interdepartmental working group:

- Coordinate the various activities and develop an overarching vision of the societal and ethical impact of digitization and of how public interests can be safeguarded.
- Explore ways of safeguarding fundamental rights in the digital age. In this context, it is important to seek links with initiatives at European level, in the Council of Europe for example.

Coordination and developing a vision

The process of translating ethical and societal issues into a coherent and cross-domain policy is progressing very slowly. An interdepartmental working group is needed to shape a government vision on the governance of societal and ethical digitization issues, and to incorporate this into structures of government in an integrated and strategic manner. The working group can ensure the coherence of any cross-domain policy issues. The working group can also raise awareness, within the government, of the implications of digitization in terms of safeguarding public values. It can also encourage various ministerial departments to address and reflect on the significance of emerging societal and ethical questions in their fields.

Safeguarding fundamental rights

The political-governance domain has the responsibility of monitoring the implications of digitization in terms of safeguarding fundamental rights. Discussions in the Netherlands have focused on the question of whether, and how, the right to privacy, confidential communication and freedom of expression should be modified in the light of digitization. Various projects have recently been initiated at European level (e.g. by the Council of Europe and by the European Parliament). The goal of these projects is to explore the potential impact of technologies such as AI, robotics, and the Internet of Things on the protection of fundamental rights (Van Est & Gerritsen, forthcoming). The Netherlands should explore the significance of digitization in terms of fundamental rights. It should also take note of European initiatives in this area. This, too, is a task for the interdepartmental working group.

2. Strengthen the role and position of supervisory bodies

Action points:

- Supervisory bodies: take note of emerging societal and ethical issues.
- Supervisory bodies: based on the current mandate, explore ways of addressing these emerging issues: what rules apply, what tools do regulators have at their disposal, what capacity/knowledge is required?
- Supervisory bodies: in the context of collective consultations, agree on who is responsible for what, and take collective action where necessary.
- Government: incorporate conditions, and take on the role of launching customer.

All regulators are facing with emerging digitization issues, whether these involve privacy, discrimination, new balances of power, or human dignity. All regulators should familiarize themselves with the question of how, in their own fields and within the scope of their current mandate, they can address emerging ethical and societal digitization issues in practical terms. In addition, close coordination is important. As digitization spans a wide range of sectors, the different regulators' enforcement domains will often overlap. Regulators should therefore update each other on the details of the digitization issues they are facing, on how regulation is organized, and on the focus of their individual areas of responsibility.

Familiarization with digital issues does not necessarily mean that a new regulator, or a new regulatory framework, is needed. Existing regulatory frameworks may provide adequate scope. For instance, the General Data Protection Regulation provides a framework for scrutinizing decisions taken automatically by algorithms. Sometimes, a regulator's current mandate and tools will suffice, on other occasions adjustment may be required.

The regulators' position can only be strengthened if existing conditions provide sufficient leeway for this purpose. It is important that the government imposes conditions on the purchase and design of IT systems. These conditions could then be used by enforcement agencies to assess the systems in question. For example, governments could determine transparency requirements for automated and complex algorithms, in order to hold software developers accountable for the operation of such systems. This would enable software developers to incorporate such features into their system design at an early stage. There is an even greater need to specify requirements in the case of public (and semi-public) services and digital systems in healthcare, education, the legal system and the like. In situations like this, it is the government's responsibility to act as the guardian of public interests. Due to increasing servitization, systems in public services are increasingly in the hands of private parties. As a result, the government, the regulators and the enforcement agencies often have insufficient information and powers to monitor the operation and impact of these systems. It must be possible to monitor the layout of the system and its effects. The government should establish conditions to be observed when procuring new systems.

3. Draw up a 'Digitization Agreement' formulating the commitments and responsibilities of businesses, government, and civil society actors with regard to safeguarding public values in the digital society.

Action points for the 'Digitization Agreement':

- Businesses: give priority to duty of care, to protect human rights in the context of digital products and services.
- Businesses and trade associations: develop practical ways of addressing duty of care through codes of conduct.
- Businesses, trade associations and the scientific community: explore and learn from existing tools and structures that can help the business community deal with ethical impacts. Privacy impact assessments can serve as models for an ethical impact assessment.
- The government and the scientific community: invest (by means of research funding and innovation policy) in exploring and tackling the societal and ethical implications of new technology.
- The government: explore ways of strengthening opposing voices from non-governmental organizations and members of the public (e.g. through class actions, or by exploring the pros and cons of revoking the prohibition on constitutional scrutiny).
- The government, businesses and civil society: greater commitment to digital skills in the educational system (young people and professionals).
- The government, businesses and civil society: expand media literacy (understanding the impact of new technology on their daily lives).

Industry, civil society and members of the public should cooperate with the government in taking steps to safeguard public values in the digital society. This could take the form of a 'Digitization Agreement', in which the various parties set out details of how they propose to jointly give the digital society a 'human face'. When drawing up a Digitization Agreement, support from businesses and participating stakeholders is vital. The process can be modelled on the approach taken in the Netherlands when reaching previous agreements, such as the Energy Agreement.

The Importance of a Digitization Agreement

For the Netherlands, it is vital that such an agreement is concluded and implemented. As with biotechnology, societal and ethical issues become key success and failure factors for innovation. Any failure to take timely action to protect public values may undermine the trust of consumers and members of the public, and lead to failed innovations and costly processes. If the Netherlands was able find an appropriate way to safeguard public values in future IT innovations, it could serve as a model for other countries. This approach could also create opportunities for Dutch industry.

Action points in the Digitization Agreement

Any 'Digitization Agreement' should define and document the responsibilities of various parties. The responsibilities of businesses are an important element of any such agreement. IT developers should be fully aware of their products' societal and ethical impact, and should actively endeavour to protect human rights and fundamental rights. Businesses' corporate responsibilities to respect human rights are enshrined in a variety of documents, including the OECD's Guidelines for Multinational Enterprises. Businesses should take action to identify situations in which they (or parties in their supply chain) might be at risk of human rights violations and, where possible, to prevent such violations.

These international standards can be translated into everyday practice by means of trade association codes of conduct, which provide guidance on how to deal with societal and ethical issues. We can learn from existing tools and structures in the field of data protection, such as privacy impact assessments and privacy by design. For example, ethical impact assessments could be used to identify and discuss societal and ethical issues, other than those relating to privacy, at an early stage of product development. The government can encourage such actions, by creating sufficient scope in innovation policy and research funding to address the societal and ethical ramifications of new technology.

In addition, the Digitization Agreement should focus on promoting 'technological citizenship', by, amongst other things, encouraging the acquisition of digital skills (see also action 4 Strengthen societal dialogue). This could be achieved by expanding media literacy in the educational system, and by creating sufficient scope for programming and other digital skills. This not only applies to the primary and secondary education of future citizens, but also for educating and training professional people today. From healthcare to the judicial system, it is important for professionals to take note of the impact that the new wave of digitization is having on public values.

Finally, it is important for the Digitization Agreement to document ways in which the counter-arguments of non-governmental organizations (NGOs) and members of the public can be more effectively supported (for example by means of class actions).

4. Strengthen societal dialogue

Action points:

- The government, businesses and civil society: support technological citizenship by holding a national debate on emerging societal and ethical digitization issues.

The public debate on the societal and ethical significance of the new wave of digitization is still limited, particularly with regard to emerging issues such as equity and equality, human dignity, autonomy, and new balances of power between businesses and consumers, between businesses and governments, and between members of the public and government bodies. It is, therefore, important to hold a national debate on these developments. It is up to the government to launch such a debate. At the same time, a societal dialogue can only be successful if it involves cooperation with parties in the field. While the government will not have executive responsibility for holding the debate, it needs to be the initiator and driving force behind these events. The experience gained from holding previous debates in the Netherlands, such as the societal debate on nanotechnology, will prove useful in this regard.

Together with encouraging people to acquire digital skills (see above), this debate lies at the very heart of technological citizenship. Technological citizenship means that members of the public are aware of the technological culture in which they live, and that they understand the ways in which technology influences their lives (Van Est 2016). 'Technological citizens' are informed about the significance of technology and they participate in democratic decision-making about new technology. They are able to critically review technologies and their relevance to everyday life. On that basis, they are able to decide which technologies they can (or want to) or cannot (or do not want to) use. For example, this means that people understand how profiling and self-learning algorithms work and could affect them. Such individuals are also able to shield themselves from unwelcome influences, and to choose alternative options. Technological citizenship thus calls for increasing societal awareness, while encouraging the formulation of opinions about the influence and significance of the new wave of digitization.

5. Schedule regular political debates in the Senate and in the House of Representatives of the Netherlands on the governance of societal and ethical digitization issues.

Action points:

- Regular debates on the governance of societal and ethical digitization issues.

One knock-on effect of an overarching government vision on dealing with the societal and ethical significance of digitization is that this subject will regularly feature on the political agenda. This will address the request from parliament that a periodic and systematic debate be held on societal and ethical digitization issues. That request is reflected in regular calls from the Senate and the House of Representatives in the Netherlands, asking the government to formulate an integrated vision in areas such as privacy, or the role of ethics in innovation policy. The motions by Senator Gerkens and Senator Ester (Parliamentary Papers I, 2013-2014, 33750 XIII) are examples of this. The motion by Senator Ester requests the Ministry of Economic Affairs to report annually on the role of ethics in innovation policy. It also endeavours to facilitate a systematically recurring political-ethical debate on this topic in the Senate. To date, the political debate has mainly been driven by incidents. By ensuring that this topic regularly features on the Senate's agenda (preferably in a context that is not limited to a single committee), the debate will transcend the limitations of its current fragmentary and sporadic nature. It will then be possible to determine whether the actions taken to strengthen the governance landscape have actually borne fruit: has the landscape been adequately strengthened? Have any new blind spots developed? And is any further action needed?

Table of Contents

1 Introduction

1.1 The Senate's request

The Dutch Senate requested in a motion on 23 September 2014 that the government 'ask Rathenau Instituut to explore the desirability of a committee that can advise on the ethical aspects of the digitization of society' (see Box 1). The Socialist party (SP) tabled the motion, which was then signed by the parties D66, VVD, CDA, GroenLinks and PvdA. As requested, the Ministry of the Interior and Kingdom relations (BZK) asked Rathenau Instituut in September 2015 to investigate the issue stated in the motion. Consequently, Rathenau Instituut has conducted this study, thereby charting the societal and ethical issues around the digitization of society and investigating to what extent the identification and monitoring of these issues are imbedded in Dutch institutions.

Box 1.1 Motion by Senator Gerkens presented on 23 September 2014
The Senate, having heard the deliberations, concludes that the digital technology involved in *the Internet of Things* will connect everything and everyone with each other; it further concludes that this unstoppable development will present opportunities for society, but also poses threats; it considers that the impact of this digital development on society is not just technological, but also societal, socio-legal and socio-psychological; it asks for the government to request that Rathenau Instituut investigates the desirability of a committee which can advise on the ethical aspects of the digitizing society, and proceeds with the day's agenda.

Signed by Senators Gerkens, Franken, K.G. de Vries, Strik, Duthler, Van Boxtel.

1.2 The context of the motion

The Gerkens motion was tabled during a debate in the Senate on the privacy and monitoring of intelligence and security services in September 2014. This debate was taking place about a year after the NRC newspaper reported on documents obtained via Edward Snowden concerning Dutch Intelligence Services procedures.[1] At the same time, the motion refers to the Internet of Things and the wider social, socio-legal and socio-psychological implications of digitization developments.

The motion request for a committee, is what we regard as a meta-question (see section 1.3 Research questions and approach). It expresses concern whether the current institutional and legislative frameworks and forms of supervision are sufficiently equipped to meet the challenges of

[1] On 30 November 2013, NRC published an article on an internal NSA report revealing that the AIVD had hacked several internet fora servers, thereby intercepting all the particpants' data. NRC.nl: *AIVD hackt internetfora, 'tegen wet in'*, 30 November 2013.

the digitizing society. This underlying concern is the leading factor in the approach to our study and the conclusions of this report.

The motion calls for the government to request that Rathenau Instituut investigates the ethical aspects of digitization. The issue raised ties in with Rathenau Instituut's objectives and substantive expertise. For thirty years, Rathenau Instituut has been identifying the ethical and social meaning of automation – later called digitization.[2] The precise reason Rathenau Instituut is carrying out this task for the government is to enable political judgement.[3] In recent years, digitization has been a highly important topic for Rathenau Instituut, featuring on its agenda in numerous ways. The various developments it has addressed include The Internet of Things, robotics, biometrics, smart mobility, big data, digital platforms, digitization in healthcare, the world of insurance and farming.[4] Thus the motion issue integrates a major part of Rathenau Instituut's research over the past years.

1.3 Research questions and approach

The key question raised by the Ministry of the Interior and Kingdom relations is: to what extent is it desirable to set up a committee that can advise on the ethical aspects of the digitization of society? In order to answer this question, we establish the various sub-questions. These relate to digitization, ethical and social issues and their *governance*. In this section we explain our approach to each research question.

Digitization:
The motion refers to the *digitization of society*. Therefore the first step in our investigation is to gain more insight in the concept of digitization. We do this by posing two research questions:

- On which specific technological developments is the digitization of society based?
- In what way will the digitization of society be shaped by new technologies in the coming 10 to 15 years?

Based on literature research, we outline how digitization has materialised over the past six decades. To demonstrate how more and more aspects of 'analogue' society have become digitized, we examine this shift in three different spheres: the material world, the biological world and the socio-cultural world. We then describe the expanding 'digital world'. For each sphere we select two fields of technology (eight in total) which we anticipate will shape digitizing society in the coming 10 to 15

[2] The Institute was established as a result of the 'Rathenau Commission' which in 1979 had the mandate to advise the government on the social impact of automation. The Commission, chaired by Gerhart Rathenau, former Director of Philips Natlab, recommended from then on to identify systematically the impact of new technology. That recommendation was heeded with the founding of NOTA, the Netherlands Organisation for Technology Assessment, later renamed the Rathenau Instituut.

[3] See the established decree, wetten.overheid.nl/BWBR0026157/2009-07-24, 24 July 2009, which states: '*Het instituut heeft als taak bij te dragen aan het maatschappelijke debat en de politieke oordeelsvorming over vraagstukken die samenhangen met of het gevolg zijn van wetenschappelijke en of technologische ontwikkelingen waaronder de ethische, de maatschappelijke, de culturele en de wettelijke aspecten daarvan. Het instituut levert in het bijzonder bijdragen aan de politieke oordeelsvorming in de beide Kamers van de Staten-Generaal en in het Europese parlement.*'
The Institute contributes to all the aspects by offering among other things context and policy options.

[4] See e.g. Beyond control: Consumer privacy in the Internet of Things (2016), Digitalisering van dieren (2016), De meetbare mens (2016), De robotsamenleving (2015), Verzekeren in de data-gedreven samenleving (2015), Dicht op de huid (2015), De data-gedreven samenleving (2015), Eerlijk advies (2014), De Kracht van platformen (2014), Tem de robotauto (2014), Intieme technologie (2014), Op advies van de auto (2013), Voorgeprogrammeerd (2012), Overal robots (2012), Check-in, check-out (2010), Databases (2010), Het glazen lichaam (2008), Van privacyparadijs tot controlestaat (2007).

years: robotics, biometrics, persuasive technology, digital platforms, augmented reality, virtual reality and social media, artificial intelligence, algorithms and big data. We decided to focus on these eight areas because they best illustrate a wide range of the impact of the new wave of digitization. The fields of technology are the starting point for our next research sub-question.

Ethical and social issues:

Once it is clear which technologies will shape the digital society in the years to come, we can investigate what ethical and social issues these technologies raise. Thus the subsequent research question is:

- What social and ethical issues does the digitization of society raise?

Here we are talking about ethical and social issues. Senator Gerkens' motion refers to the *ethical* aspects of the digitizing society. We get a clear picture of the Senate's meaning in the explanatory text (see box 1): it speaks about the 'social, socio-legal and socio-psychological effects of digital developments. This explanation expresses a broad definition of ethics – which is why we also adopt a broad approach. In this study we define ethics as the systematic reflection of morals, that is to say the entire framework of standards and values that actually exist in a society. Thus we view ethics as something that does not merely play a role at an individual level, but also at a societal level. For that reason, our research consistently considers the ethical *and* social issues brought about by the digitization of society. We chart these by comprehensively studying the relevant scientific literature. We will show which issues play a role in each field of technology and how they manifest themselves.

Governance:

The motion asks if it is desirable to have a committee that can advise on the ethical aspects of the digitalizing society. As mentioned above, that question points to an underlying concern in the Senate whether the current legal framework, supervisory systems and social resilience are sufficient to cope with emerging ethical and societal issues surrounding digitization. We therefore address the motion question based on this underlying query.

We investigate how the *governance* of ethical and societal issues becomes established in the digitizing society and whether it is adequate. Our aim is to discover which issues the existing institutions do or do not address, and in what way: are there blind spots regarding how to handle (new) ethical and societal issues? The follow-up question is what role a committee could play. We should therefore also gain insight in what types of committees typically deal with ethical and social issues in the context of technology and how we see the role of a committee.

The final sub-questions are therefore:

- How do we understand the governance of social and ethical issues in technological developments, and what role do committees play in these?
- How is the governance of ethical issues in the digitized society currently established? Which issues are addressed well or not so well and can we identify blind spots?
- What role can a committee play in digitizing society's broader governance eco-system?

Governance is a complex concept. In Appendix B we present a number of insights and definitions from the literature which can be useful for considering the governance of social and ethical aspects in science and technology. For our approach it is vital that we distinguish the *governance* and *meta-governance* of ethical and social problems.

In general terms, governance is about collectively controlling social problems in our society (for a more detailed definition, see Appendix B). The real issues here are:

- What public problems have been identified and put on the political agenda?
- Which interests or values are well or less well articulated?
- How do various actors in society discuss these problems?
- Who is and who is not involved to a greater or lesser extent?

Meta-governance shows that the collective control of public problems takes place in a *governance ecosystem*, or rather with a group of institutes, administrative and social processes and actors. Meta-governance represents the structure, framework and functioning of the governance ecosystem and deals with questions such as:

- Which institutions exist to discuss problems and address them politically?
- In what way do public and private actors come to an agreement with each other?
- How are public values institutionally protected?
- Which institutions have developed over the years to ensure this?

In this study we want to learn more about the governance and the meta-governance of the societal and ethical issues that arise from digitalisation. Our approach is two-fold. Firstly we look at whether we can generally understand the governance ecosystem in the Netherlands concerning social and ethical issues in technology. To do this, we define a general conceptual framework, based on a review of governance mechanisms that have arisen in the Netherlands over the past half century, in four fields of technology: biotechnology, ICT, research involving human subjects and animal trials. This historical overview also illustrates what kind of committees have been set up in the past to deal with ethical and societal issues in these fields and what role they played within the governance ecosystem.

We then apply the general conceptual framework to gain insight in how the governance ecosystem for ethical and social issues concerning digitization materialises. Desk research enables us to analyse which parties make up the ecosystem, which public problems they are (or not) aware of, to what extent these problems feature on the political agenda and how the identified problems are handled from a policy perspective. Our analysis covers activities up till October 2016. On this basis we can surmise where there are possible blind spots in the current governance eco system and what role a committee could play.

We note that Rathenau Instituut makes up part of the governance ecosystem involving societal and ethical issues in technology as well as in digitization. As stated above, the Institute’s mission is to foster public and political opinion-forming on science and technology. For that reason we mention Rathenau Instituut’s activities in our analysis of the ecosystem.

Besides literature and desk research, this study involved discussions with various experts and stakeholders (Appendix C has an overview of the experts we consulted). We also presented and discussed the results of our study with a supervisory committee, consisting of six people with scientific and political-administrative experience (see also Appendix C). Rathenau Instituut is responsible for the findings in this report. Finally, in accordance with Rathenau Instituut's quality procedures, the report was submitted for an internal review.

1.4 Reader's guide

The following chapters will elaborate step by step on the research questions relating to digitization, social and ethical aspects.

Chapter 2 traces the development of digitization over the past 50 years, examining which areas of technology are likely to affect our digital society in the coming years. These areas have fuelled a new technological wave, ushering in another phase in our digital world. Initially consisting of the large-scale collection of data on the physical, biological and social world, digitization is now focused on the large-scale analysis and application of that data. This makes real-time intervention and (re)directing possible. Take for example social media users' newsfeeds, which social media companies are now 'customizing' based on their monitoring and analysis of these same users' surfing behaviour. This *cybernetic loop* is characteristic for the current phase of digitization.

This new wave of technology is currently giving rise to several social and ethical concerns, which we outline in Chapter 3. We highlight the most urgent issues in each area of technology, and illustrate these with actual examples. It becomes apparent that the social and ethical issues surrounding digitization not only relate to privacy and security, but also evoke new fundamental issues concerning factors such as justice, equal treatment, autonomy and human dignity. Who, for example, has insight in what choices the social media companies' filtering software makes to show certain news items or not? Which tasks would we rather leave to robots, and which not?

Chapter 4 explains the concept of a governance ecosystem for societal and ethical issues in technology. Looking back over half a century, we see how we in the Netherlands have dealt with ethical and social issues surrounding biotechnology, ICT, clinical trials and animal experiments. The review shows which committees were in charge of these areas and what type of committees they were. Based on this historical review, we can draw up a general conceptual framework of the Dutch governance ecosystem for societal and ethical issues in technology. Within this framework, we distinguish four domains: fundamental and human rights, science, society, and politics and governance.

In Chapter 5 we then apply this conceptual framework to gain insight into how the governance ecosystem for ethical and social issues to do with digitization is currently taking shape. The analysis focuses on the Netherlands but includes relevant developments in other countries. Based on desk research, we outline which activities the various organizations and actors are proposing, preparing, initiating or conducting, in order to meet the social and ethical challenges surrounding digitization.

We also establish which committees are still covering this area or which have been proposed by various organizations. We identify the blind spots in different parts of the governance landscape.

Chapter 6 summarizes the main findings of this study. Our conclusion is that the far-reaching digitization of society is raising fundamental ethical and societal issues. Currently, government and society are not adequately equipped to deal with these issues. In order to safeguard our public values and fundamental rights in the digital age now and in the future, the governance system needs to be upgraded. Such upgrading requires that all parties – government, business and civil society – take action to keep digitization on the right track. We propose an action programme that will shape the digital society in a responsible way.

2 The new digital wave

2.1 Introduction

This chapter guides us through the continual digitization of society. What has been digitized over the past 60 years, what are the effects of that digitization, and what will the future digital society look like. We are not attempting to paint the whole picture of all things digital, but rather give readers an idea of what digitization actually means. We look both to the past (the relevant technological developments that have underpinned the process of digitization) as well as to the future (the relevant technological developments that will shape the digital society over the next five to ten years). These latter developments represent a selection of eight areas of technology. In the next section, these areas form the starting point for analysing the ethical and societal issues that arise in the digital society.

We start with a concise historical review of developments in micro-electronics and telecommunications: important techniques, or *resources* for digitization (section 2.2). We show how more and more areas in the ‘analogue’ society are becoming digital, and divide these into three ‘worlds’ that are the *object* of that digitization: the material world, the biological world, and the socio-cultural world (section 2.3). For each of these worlds, we highlight the significant digitization milestones. Then we turn to the ever-expanding digital world (section 2.4), in which we select two technology areas for analysing social and ethical issues. In section 2.5 we bring these four worlds together: what new stage in the development of the digitizing society do we see? Finally, section 2.6 sums up the main findings of this chapter.

Box 2.1 Digitization

According to the dictionary, digitization literally means converting something (such as data or an image) to digital form (Merriam-Webster). Think for example of digitally transferring a VHS video tape so that you can play it on a computer. Or scanning a photo that is then converted to digital pixel dimensions. Currently, we have a continually growing number of digital products and services such as digital music, streaming services and the digital bank account.

It is already apparent that digitization is not just about converting analogue signals into bits and bytes. Converting information into digital form gives that information other properties, and enables other things. In 1995 Nicholas Negroponte wrote *Being Digital* in which he indicated that digitization makes information easier to transport, manipulate and integrate. Around this time, several scientists including Manuel Castells in his classic *The Rise of The Network Society,* began to see digitization (of the network) as the dominant organizational structure for a society that is about to change the existing ways of creating and experiencing power and culture (Castells 1995; Van Dijk 1997). A decade later, Benkler (2006) described in *The Wealth of Networks* how information technology enables new forms of collaboration that lead to fundamental changes in the economy and society.

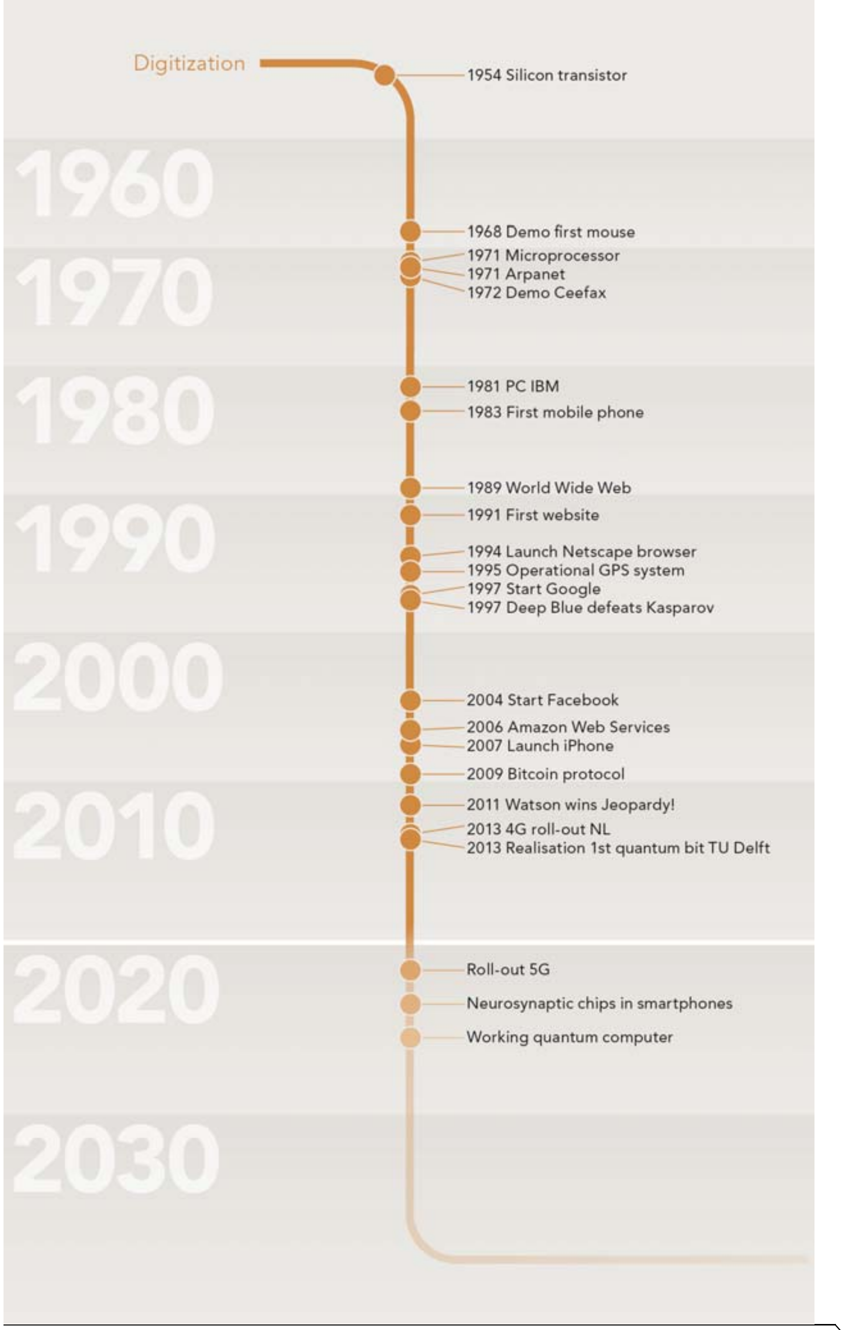
ICT, and the resulting digitization – just like steam or electricity – are applied in countless ways. That is why we also speak of a generic technology (*general purpose technology*) (Bresnahan & Trajtenberg 1995). This technology not only enables the creation of many new products, but also has a long term effect on numerous societal processes.

2.2 Resources to digitize[5]

In this section we illustrate how digitization has taken shape over the past half century. We examine the underlying techniques that enable digitization, for example the equipment (hardware), software, telecommunications and infrastructure; in short, information and communication technology (ICT). Our examination starts by providing a concise historical overview of the developments in micro-electronics and telecommunication (see Figure 2.1). You can read about the various positioning statements and theories on the term digitization in Box 2.1. They indicate that digitization is not just a matter of instrumental change – fundamental changes are taking place in our economy and in society.

[5] This section provides a condensed historical overview of developments in micro-electronics and telecommunication. For a more extensive overview, see for example works by Van den Bogaard et al. (2008): De eeuw van de computer: de geschiedenis van de informatietechnologie in Nederland.

Figure 2.1 An overview of digitization resources



Rathenau Instituut

The breakthrough in microelectronics and telecommunications of the 1940s and 1950s laid an important technological foundation for digitization. Those breakthroughs included the first programmable computer (1941) and the first silicon-based transistor (1954). A transistor serves to strengthen or switch electronic signals. As it is the fundamental building block for each chip, the transistor therefore forms the basis of every ICT application. Over the last fifty years, the number of transistors on a chip has doubled roughly every 18 months to two years. This trend of miniaturization and the rate at which innovation is taking place, is called Moore's Law, and in the past six decades it has led to ever smaller, more powerful and more affordable computers.[6]

The first computers in the 1950s were colossal and used mainly by the defence industry and for complex calculations in science. Banks also started to use these '*mainframe computers'*. The 1960s saw computers gradually becoming smaller and smaller and marked the arrival of the 'mini-computer' – as big as a refrigerator. A breakthrough came in 1971 with Intel's microprocessor. Despite being only a few millimetres in size, it was just as powerful as its giant cousins of the Fifties. Thus Apple and Microsoft, still small companies back then, were able to design even smaller-sized computers that could sit on a desk separate from a mainframe. But it was not until the 1980s that information technology entered society on a wide scale, with the advent of IBM's Personal Computer (PC). The PC swiftly appeared in many workplaces, its main applications being word processing and spreadsheets, and in the following years also in the family home.

Mobile telephony and the Internet emerged in the 1990s. This coincided with the start of digitization and convergence of existing infrastructures like cable and ether for telephony, radio and TV services. The consequences of this digitization process soon became evident everywhere: in business services like the music trade, the travel industry, logistics and retail; also in semi-public sectors such as education, mobility and healthcare. The growing availability of the Internet worldwide reinforced globalization. This made it possible to *outsource*, *offshore* and automate initially production work and later also knowledge work (Van Est & Kool 2015).

By the end of the twentieth century, the Internet was changing from a passive, information-providing medium (web 1.0) to an interactive platform to which users can contribute in an abundance of ways (web 2.0): via commenting, posting their own content and *tagging* as well as reviewing others' content. The web has become a 'platform for data management ', especially through the input of users' social connectedness and collective intelligence (O'Reilly 2005). Social networking sites like MySpace, Hyves and Facebook appeared, and other social media like YouTube and Twitter. With the emergence of smartphones and other mobile devices like tablets, along with the continuing development of fast, wireless internet connections and *cloud* applications, it is no longer possible to imagine the economy and society without the Internet and the associated online services.

After 2010 we saw 4G networks being rolled out, the emergence of the Internet of Things (see section 2.3) and more and more online applications using a form of artificial intelligence, such as speech recognition, or better search functionality. In 2011, IBM's supercomputer won the TV game 'Jeopardy' for the first time and in 2016, Google's AlphaGo programme won the highly complex

[6] Moore's Law is based on a prediction by Gordon Moore in 1965. He predicted that the number of transistors on a microchip, and thus the processing power of computers, would double every two years, while the cost would remain the same. Fifty years on, his prediction is still valid. However, it is debatable how long Moore's Law will still apply. The expectation is that chips will have reached their physical limit once they are about five nanometers in size. Manufacturers will then probably switch to 3D chips (stacked chips). The next step will be chips no longer based on silicone, but on optical, nano or biological principles. IBM presented for example a neurosynaptic chip, TrueNorth in 2015.

game ‘Go’ from a human expert.[7] For 2020 and beyond, the expectations are the roll-out of the 5G network, new types of faster chips and breakthroughs in the field of quantum computing.[8] In Figure 2.1 we have clustered these expectations under uncertain future milestones.

2.3 Objects of digitization

Currently, ICT and digitization are ubiquitous in our society. ICT is also linked with other technology fields, such as nanotechnology, biotechnology and neurotechnology. This so-called NBIC convergence has become increasingly visible since the late 1990s. Digitization penetrates every aspect of our lives: the technology nestles itself *in* us (for example through brain implants), *between* us (through social media like Facebook), knows more and more *about* us (via big data and techniques such as emotion recognition), and is continually learning to behave more *like* us (robots and software exhibit intelligent behaviour and can mimic emotions). In 2014, Rathenau Instituut referred to this as the intimate technological revolution (Van Est 2014).

The interweaving of ICT with other technologies demonstrates that all sorts of aspects of our lives are digitizing. As we cannot cover all these different aspects in detail here, we have decided to look at three distinct ‘worlds’:

1. the *material* world (e.g. the production process, public space and our home)
2. the *biological world* (the human body, the brain and our behaviour)
3. the *socio-cultural world* (communication, cultural products and organizations).

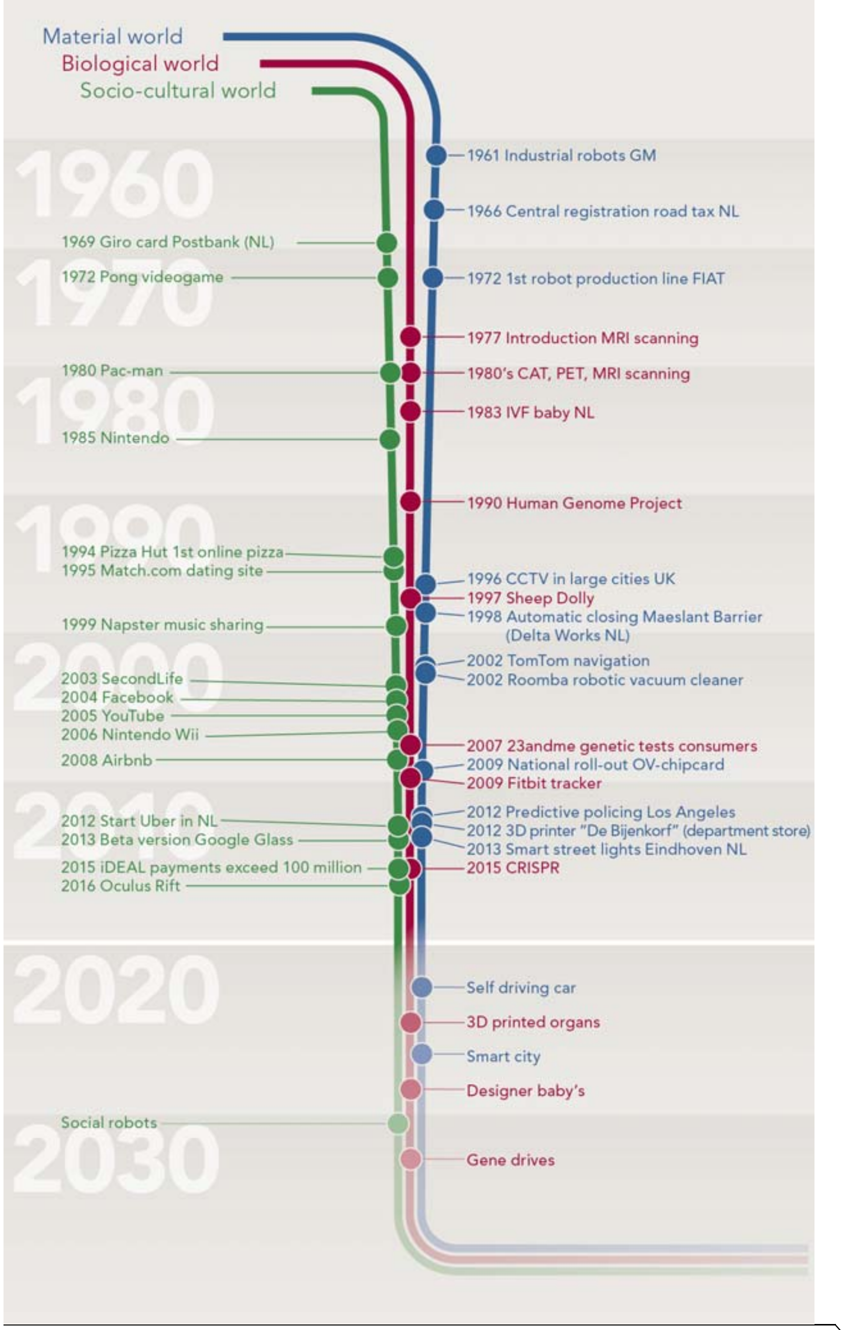
For each world, we highlight the significant digitization milestones, and the future technological innovations anticipated for 2020 and 2030 (see Figure 2.2). Based on this information, we select two technology areas in each world that are expected to shape the digital society in the next five to ten years. The worlds are all virtually represented in the growing digital world, which we describe in section 2.4.

The distinction between the three worlds is a conceptual one. In practice, these worlds are strongly interwoven and overlap each other. That is why when describing them, we always focus on *the object of digitization*. This means, for example, that we deal with the digitization of music in the socio-cultural world; we consider music as a cultural product, an object of digitization. That does not alter the fact that music has physical carriers and instruments, and a physical production and distribution process. Music therefore also has a place in the material world. Digitization of the material process has not only had a huge impact on the music industry; it also affects our cultural experience of music. We explain that influence in the socio-cultural world. Also human behaviour overlaps the biological and the socio-cultural world. From the above mentioned research perspective, we place behaviour in the biological world; we see behaviour as part of our ‘being human' that is now digitizing. Nevertheless, in addition to biological and psychological factors, behaviour also has social and cultural influences.

[7] bbc.com/news/technology-35785875,

[8] A quantum computer uses the laws of quantum physics and calculates with so-called qubits. Unlike the bits in a normal computer, qubits can be both 0 and 1 at the same time. Thus it is possible to carry out a calculation, which normally consists of sequential steps, in one go. This opens up radical new options for quantum computers and unprecedented processing speeds.

Figure 2.2 An overview of milestones in the digitization of the material, biological and socio-cultural worlds


Material world
Biological world
Socio-cultural world
1960
1961 Industrial robots GM
1966 Central registration road tax NL
1969 Giro card Postbank (NL)
1970
1972 Pong videogame
1972 1st robot production line FIAT
1977 Introduction MRI scanning
1980 Pac-man
1980's CAT, PET, MRI scanning
1980
1983 IVF baby NL
1985 Nintendo
1990 Human Genome Project
1990
1994 Pizza Hut 1st online pizza
1995 Match.com dating site
1996 CCTV in large cities UK
1997 Sheep Dolly
1998 Automatic closing Maeslant Barrier (Delta Works NL)
1999 Napster music sharing
2000
2002 TomTom navigation
2002 Roomba robotic vacuum cleaner
2003 SecondLife
2004 Facebook
2005 YouTube
2006 Nintendo Wii
2007 23andme genetic tests consumers
2008 Airbnb
2009 National roll-out OV-chipcard
2009 Fitbit tracker
2010
2012 Start Uber in NL
2012 Predictive policing Los Angeles
2012 3D printer "De Bijenkorf" (department store)
2013 Beta version Google Glass
2013 Smart street lights Eindhoven NL
2015 iDEAL payments exceed 100 million
2015 CRISPR
2016 Oculus Rift
2020
Self driving car
3D printed organs
Smart city
Designer baby's
Social robots
2030
Gene drives

Rathenau Instituut

The material world

The material world digitizes in all sorts of ways. Nowadays we come across robots not just in factories but also elsewhere. Cameras monitor highways, streets and stations. Appliances in our homes (smart TVs, smart energy meters) are constantly connected to the Internet and we have our smartphones with us day and night. In this section we illustrate the digitization of the material world by examining: 1) the production process, 2) the environment and public space, and 3) our home.

Production process

An important step in the digitization of the production process was the introduction of mechanical robotic arms in the manufacturing industry in the late 1970s. Later on, in the 1980 and 1990s, ICT broke through as the means to optimize the production process and prevent for example wasting materials.[9] The use of ICT went hand in hand with the globalization of the economy. It became increasingly important to optimize not just the production process, but also the entire value chain. The further breaking down of production jobs into subtasks led to both specialization (outsourcing) as well as relocation (offshoring). Customization also became possible. Customers can now design more and more products themselves, like sport shoes, and order them online. The products are only made after the customer has ordered them; ICT, in the form of flexible computer-controlled production processes, enables *just-in-time* production and mass personalization (or *mass customization*), see Van Est & Kool, 2015.

Since the beginning of the 21st century, new digital resources can monitor production and service processes increasingly accurately. There is more insight into consumer behaviour and how products are applied once they leave the factory gate. For example, the use of RFID, GPS and video cameras has led to *high-resolution management* (Subirana et al. 2006, p.11), or precision management. At its heart are data collection as well as techniques for monitoring and analysis. Under the influence of big data, more and more information is becoming available about every part of the value chain, which we can consequently control even more efficiently. Through the continuous monitoring of car or train parts for instance, maintenance costs can be reduced. The result is a smart fleet of cars or trains. The potential uses of data collection, monitoring and analysis are combined in futuristic images and put under the heading of 'smart' or Internet of Things, to promote an *Internet of Everything*: smart energy networks, *smart mobility* (including the self-driving car), digital oil extraction, robotic mining, *smart farming* and smart cities.

The deployment of a new generation of robots is another means of further optimizing the production process. Robots’ capacities are increasing thanks to improved vision systems (using for example 3D cameras), better navigation systems and advances in artificial intelligence. Robots have become indispensable in the manufacturing industry; the autonomous factory is now a reality in Japan, where the FANUC factory robots can operate for a month without supervision (Rahul & Velez 2015). We see more and more robots appearing outside the factories, for instance in unmanned aircraft (drones), self-driving vehicles, robots in healthcare and catering sectors, or household robots such as the robot vacuum cleaner. There are ongoing worldwide debates about how robotics and artificial intelligence will affect people’s jobs in the future (Ford 2015; Van Est & Kool 2015; Went et al. 2015; Brynjolfsson & McAfee 2014).

Digital manufacturing technologies such as 3D-printing are blurring the dividing lines between digital and material production processes even further. Advanced 3D scanning technologies make it possible to transform physical objects into digital 3D models that are infinitely reproducible. The scale at which materials can be created is shifting from micro to nano and atomic level: “We're on the threshold of the third digital revolution, one in which matter and information merge,” according to

[9] The so-called *lean management* principle, originally developed in Japan.

MIT Professor Gershenfield (Anthes 2006). Scientists are carrying out research projects experimenting with printing blood vessels and organs. In 2013, a design for a 3D-printable gun was posted online.[10]

Environment and public spaces

Our environment is digitizing in all kinds of ways. In the late 1990s, municipalities and companies introduced security cameras in public areas and business estates. The first municipality in the Netherlands that placed these cameras was Ede. In the years thereafter, cameras were monitoring our road network, public transport and private spaces such as shops and businesses. At the same time as cameras, other digital equipment entered the public arena such as navigation devices, the chip card for public transport and digital station gates (Vincent et al. 2010).

Through smartphones, mobile internet and social media, the physical and virtual world are becoming ever more closely intertwined. Social media, dating sites and other services are going to actively use location as part of their services, for example with *geo-tagging*, and ‘checking in' at locations, or for games based on geographical elements (*geo-caching*). This intertwining gets a new dimension with the introduction of techniques such as *virtual reality* and *augmented reality* (see below on the socio-cultural world).

Under the ‘Smart City’ banner, our environment is set to keep on digitizing over the coming years: governments, businesses and residents can get detailed insight into processes in the city through all sorts of sensors. Telecom companies can provide insight into how people move through cities based on the connections that phones make with their transmitter mast. Citizens can use home-made sensors to measure whether traffic flows are affecting the local air quality. The Smart City promises to be a sustainable and comfortable living environment without traffic jams, energy wastage or dodgy alleyways. ‘Smart’ in this context means that ICT – software, sensors and the Internet – overlay the city with a digital layer. This layer provides continuous data streams, with which municipalities can monitor or re(direct) residents, road users or even burglars.
Other potential applications are a smart sewer that monitors which bacteria, biomarkers or viruses are present, so that a possible disease outbreak can be predicted before people actually become ill,[11] or a smart streetlight that automatically determines when to switch itself on, with light colours that can influence the state of mind of those passing by and prevent potential aggression, and with cameras monitoring passing traffic.[12]

Home

Our home cannot escape digitization either. All kinds of household appliances are given an internet address via the Internet of Things. They are ‘hung on the net’ and get sensors, computing power and communication capabilities. Examples include smart thermostats connected to the energy supplier, thus providing digital insight into our energy consumption compared to others, or a smart

[10] ‘The liberator’ was made available online by the company Defense Disbtributed, however after 2 days it was removed by the US government (but can be be found again on the Internet via p2p sites).

[11] Currently developed by MIT Senseable City Lab, see: underworlds.mit.edu

[12] As created in the Living Lab Stratumseind 2.0 in Eindhoven, see: brainport.nl/high-tech-systems-materials/living-lab-laat-ander-licht-schijnen-op-stratumseind

TV that analyses our viewing behaviour and on that basis sends us tips for other programmes. Even Barbie already has a microphone and an internet connection.[13]

The concept Internet of Things dates back to early 2000, when electronics manufacturer LG presented a fridge that made an inventory of its contents and automatically contacted the supermarket to order new stock.[14] The term attracted worldwide attention when the United Nations International Telecommunications Unit (ITU 2005) published a report on the subject. A decade later, the vision of the Internet of Things started to become reality. Marketing agencies predicted a huge growth of products related to the Internet. Gartner (2015) projected that, compared to the 3 billion objects linked (on the consumer market) to the Internet in 2015, there would 13.5 billion objects by 2020. The OECD also estimated that consumers in Western countries would have 14 billion *connected devices* in their homes by 2022. That works out at around fifty objects per household (OECD 2013).

Main technology areas

This section highlights two main technologies that are expected to play an important role in shaping the digital society in the coming years: developments in robotics and the Internet of Things/smart environments (see table 2.1).

Table 2.1 Various areas of technology in the material world

Technology area	Description
Robotics	Robots can carry out ever more complex tasks. They can view things better (3D image), navigate and move better, and interact smarter with people. Robots are now found in factories, it is expected that social robots will play a role in offices, school buildings, hospitals, restaurants and the home environment.
Internet of Things and smart environments	Devices are increasingly equipped with an internet connection, sensors, processing power and communication capabilities. It this way the device collects data about its environment, which it can share with other objects (*machine 2 machine* communication) to steer processes, or analyses information in the *cloud* in order to provide 'customized' information or services.

Rathenau Instituut

Biological world

Over the past six decades the biological world has also been digitizing. The way we capture behaviour, emotions, body functions and the human DNA in bits and bytes and have it analysed by software has improved. Human genetic material has been digitally mapped in recent years, and can also be deliberately adjusted. Through *Smart wearables,* users and businesses gather biological

[13] The doll records calls and sends them to the cloud. Artificial intelligence helps to analyze the conversation, and on that basis chooses an appropriate response. At the end of 2015 Barbie got some negative press because it appeared to be possible to hack the recorded conversations.

[14] The concept that LG proposed in 2000 became a reality in 2016. At the CES exhibition, Samsung presented the smart fridge for the consumer market that will in fact be available in 2016 (including associated services) in South Korea.

data such as heart rate, respiration rate, body temperature or dietary and sleep patterns. And in the future, our outer ear, gait, voice, posture, breathing, heart rate and even the way we type, will be new ways to identify people. In this section, we illustrate the digitization of the biological world by looking at 1) the human body, 2) the brain and 3) human behaviour.

Body

The digitization of the body started decades ago with the application of medical equipment that could ‘digitally read' the human body. Initially this involved techniques such as x-rays and CT scans, or blood glucose monitors for diabetics. An important development for the digitization of the body’s ‘code’ was the Human Genome Project. This project, which began in 1990, charted the structure of the human DNA. At the start, they estimated the process would take about 15 years. However, thanks to the enormous progress in DNA analysis techniques – partly enabled by the rapid developments in computing power and storage capacity – a first rough map was completed in 2000 already. In the following years, it also became possible to adapt DNA material. This has recently become cheaper, faster and easier through the CRISPR gene editing technique (see Box 2.2). The technique brings controversial futuristic visions of designer babies a step closer.

Box 2.2 CRISPR

In the past few years, it has become easier to ‘read’ the human genome thanks to developments in *genome-sequencing* technology. Adjusting genetic information, however, was still a difficult task up until recently. The development of CRISPR-Cas9 technology (often abbreviated to CRISPR) has caused a stir. CRISPR technology makes use of the fact that bacteria have their own natural or innate immune system. When bacteria are infected with a virus, they build a part of that virus into their own DNA in order to be able to recognize it in the future. Scientists adapt the system in such a way that they can select which piece of DNA to incorporate and where that happens in the DNA. In addition to bacteria, the technique can also be applied to animals and humans. In this way CRISPR makes it easier, faster and cheaper to adapt genes in bacteria, plants, animals and people.

The digitization of the body is also visible outside the laboratory. Health care uses the technique to read DNA quickly and cheaply (Next Generation Sequencing). The technique helps clinical genetics centres to find the cause of a clinical picture. There are high expectations for providing health tailored by more knowledge about one's DNA profile, but for the time being, this is still a pipe dream (Vrijenhoek & Radstake 2016). Since 2006, via commercial services such as 23andMe, people can learn about their own genetic profile and possible hereditary predisposition to diseases and conditions such as baldness or blindness. Alongside genetic information, we see the digitization of the body in all sorts of areas. The current generation of smartphones and apps assist people to monitor their blood pressure, glucose, heart rate variability and stress responses. We anticipate that with the help of smaller and better sensors, the future generation of digital coaching will be able to constantly monitor the psychophysiological state of its users (Kool et al. 2014).

Brain

Our human brain, at least parts of it, also digitizes. In this way *neuro-imaging* technology in the lab helps to chart cognitive processes. Scientists are using *deep brain stimulation* (DBS) in brain implants, for example, to reduce the shaking in people with Parkinson's disease. An implanted neuro-stimulator sends electrical pulses to an electrode that is surgically implanted in the brain, at a specific spot, depending on the symptom. By 2011, already more than 70,000 Parkinson's sufferers had undergone this procedure (Bronstein et al. 2012). Scientists are also working on other applications of DBS, for example to help depression. In the consumer domain, *brain-computer interfaces* are coming on the market that enable users to analyse their own brain waves and attempt to improve their cognitive skills. Using electric waves, *do-it-yourself* neuro-enhancers try to boost brain power or train concentration using feedback on patterns in brain waves (Burkeman 2014).

Emotion recognition technology is getting better at recognising our emotions. The purpose-built software has advanced so much in recent years that computers are on average better than people at recognizing a false emotion (Andrade 2014; Li et al. 2015). Also facial recognition technology is improving at a fast rate. The best algorithms already recognise faces as well as people do (Harris 2015). Face and emotion recognition is part of a series of new identification possibilities based on the human body, in addition to the well-known methods like fingerprint and iris scan (Janssen et al. 2014).

Behaviour

In recent years scientists and companies have discovered that all kinds of information can be inferred from our digital surfing behaviour. This is due to the combined presence of large volumes of digital, personal data, plus smart software to analyse that data. For example Facebook profiles divulge information about sexual orientation or political affiliations (Kosinski et al. 2013). Watson, IBM’s smart computer, only needs a sheet of A4 text to analyse the author’s personality. Recruitment company Entelo scouts for talented programmers based on what they post on the Internet (Peck 2013). We will now take a closer look at how big data and smart software are applied in the digital world.

After recognizing and analysing human behaviour, the next step is influencing that behaviour (see box 2.3). Think of Facebook's emotion study, which revealed that showing users positive or negative information affects their mood. Consequently, users post more positive or negative things. The study caused quite a commotion among users when they realised that they had unwittingly been part of an experiment (Adam et al. 2014). The inconspicuous personalizing of search behaviour by search engines such as Google is an example of subtle influencing (Vincent et al. 2012).

Box 2.3 Persuasive technology

Persuasive technology uses insights from psychology, behavioural sciences and human-computer interaction, to design systems that encourage users to change their behaviour (Fogg

2002). This type of technological behaviour influencing – also called *nudging* – is becoming more and more sophisticated. Personalized influencing strategies are thus being studied, whereby users are influenced by the kind of argumentation to which they are sensitive (Kaptein 2015; Kaptein & Eckles 2012). Researchers use *ambient feedback* to observe how people at a lower cognitive level of consciousness are influenced by elements in their surroundings, such as light or colour. Research on low cognitive influence with colour proves this can be an effective strategy. Systems that use colour when providing feedback on energy consumption seem more effective than feedback based on figures (Maan et al. 2011; Ham et al. 2009).

Overview of technology areas
This section highlights the various technologies that are expected to continue shaping the digital society over the coming years. We will discuss in detail a number of these in the medical ethical and bio-ethical domain, including CRISPR and *deep brain stimulation* (see for example Van Est et al. 2014 and 2016). The focus here is areas outside the medical world, namely: 1) the rapid improvements in face recognition and other physical characteristics (multimodal biometrics), and 2) the growing use of persuasive technology in the consumer domain (see table 2.2). We also discuss technologies relating to analysing human behaviour through *data analytics*. Our review of these techniques is in section 2.4 (The digital world).

Table 2.2 Fields of technology in the biological world

Field of technology	Description
Persuasive technology	Persuasive technology is aimed at influencing and changing human behaviour. The methods for influencing are becoming more and more subtle.
Multimodal biometrics	Biometrics is a way to identify people uniquely, using various *identifiers* in the human body: fingerprint, iris, voice, face, ears, heart rhythm or gait. The expectation is that by combining different modalities, it will be easier to identify people. The technology also has other applications such as security.

Rathenau Instituut

Socio-cultural world

The growing use of ICT also means digitizing the interaction between people, as well as between people and organizations. Digitization penetrates our social and cultural life: shopping, listening to music, contacting friends, taking action and finding a date are things we do increasingly online. Even after death, our digital profiles on services as LivesOn[15] continue to speak for us. The distinction between offline and online is becoming more difficult to make. Also organizations are digitizing: more and more customer contact is entirely digital; and the new, digitally disruptive

[15] liveson.org/connect.php

organizational models mean organizing and providing access to products and services is more important than making or owning those products or services yourself. The now-famous quote from Tom Goodwin, vice president of Havas Media, depicts the success of these new organizational models: “Uber, the world's largest taxi company, owns no vehicles. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate. Something interesting is happening,” Goodwin (2015). In this section, we illustrate the digitization of the socio-cultural world by looking at 1) the digitization of communication and culture, and 2) the digitization of organizational models.

Communication and culture

The advent of social media and other online services in the late 1990s and at the turn of the century have had a huge impact on the way we communicate. Services have acquired an increasingly important role in our culture and for forming our identity. See for example, Boyd (2014), about the lives of the networked youth, work by Turkle on the impact of the screen on our lives and relationships (Turkle 2015; 2011), or Carr who writes about potentially other (more superficial) functioning of our brain through the Internet (2010). Our lives are interwoven with our smartphone, which forms the connection between the real and virtual world. Floridi et al. (2014) refer to this as *onlife*: the distinction between offline and online life is now completely blurred; they have become one.

Recent developments in *virtual reality* and *augmented reality* also contribute to this fusion. *Virtual reality* (VR), can make users’ virtual experiences feel better or ‘more real’. Game makers apply the technique to get gamers more into their game. Other domains use VR, such as rehabilitation care for the physically handicapped, or to train soldiers in the army. Via *augmented reality* (AR), users can get additional real-time information. For example, the app Layar gives home seekers on-the-spot information about a particular house they have seen in the area. The technology is also beneficial for professionals. For example, while a mechanic is working, via his smart glasses he can check and remind himself if he is carrying out a procedure correctly; or a surgeon can continuously get information on his patient’s vital signs.

Cultural products and services also jumped on the digital bandwagon: music, books, films and games can all be made digital, in order to distribute, listen to, read, watch and play. Smart recommendation technology, using big data and insights from artificial intelligence, helps people to make their choice from the huge selection on offer. The rapid development of artificial intelligence has resulted in software being able to do things that until recently we considered exclusively ‘human'. Thus software (to a limited extent) can write journalistic articles for domains like sport or the stock exchange. IBM’s Watson wins language games, and as chef, won the 2015 Horecava Innovation Award. Software also composes symphonies that experts cannot distinguish from leading composers (Steiner 2012).

Organizational models

The interaction between organizations and consumers is also becoming an increasingly digital process. Consequently, the organizational models are also changing. There are more and more online stores with no physical shop and organizations are increasing their efforts to connect with customers through digital channels (Twitter, chat, mail, apps). Also the Dutch government's guideline for the last couple of years is: "digital if possible, personal if necessary" [*digitaal als het kan, persoonlijk als het moet*] (BZK 2013).

From the turn of the century, digital organization models played a major role in organizing and facilitating transactions in the economy and society (Kreijveld et al. 2014). Similarly, the app stores provided an innovative boost because software development via this platform became accessible for small independent actors. Part of this success involved taking up a strategic position between the seller and the buyer, like Apple set up with iTunes, between the artists, record companies and consumers (Kreijveld et al. 2014). Through these digital platforms, radically new organizational forms began to appear after 2010. Examples are Airbnb and Uber that in a few years have become major economic players, drastically disrupting their respective branches. Ismail et al. (2014) describe them as exponential organizations that want to have as few as possible permanent employees and as many as possible on-call workers, make optimal use of the free services of a digital community, make maximum use of automated algorithms and own a minimum amount of capital goods. Another example of a digital platform is blockchain technology. This technology enables the development of so-called autonomous organizations – consisting entirely of bits and bytes. As the technology can automate a series of appointments and tasks, it can therefore take over the function of a certain organization (see box 2.4).

Box 2.4 Blockchain

The *blockchain* is known as the underlying technical protocol on which the virtual currency *Bitcoin* is based. To put it simply, the blockchain acts a virtual ledger, recording every transaction between users. The ledger is on all the computers that make up the blockchain network and is encrypted with smart cryptography. Each new transaction is spread throughout the network and verified by all the computers in the network. The principle behind the blockchain protocol is that it can record all kinds of agreements. Thus it is possible to automate contracts or even entire organizations – *Distributed Autonomous Organisations* (DAOs). One example is a web hosting company that sells website domains: the software records that if at a certain time, a certain party pays a certain amount on a specific account, the ownership of domain name X then passes to that party. Or in insurance: the blockchain could automate the agreement that people deposit a certain amount in a pot and get compensation in the event of an accident.

Overview of technology areas

We now turn to two major area of technology that are most likely to shape the digital society in the coming years: 1) the further development of social media, via techniques such as virtual reality and augmented reality, and 2) digital platforms including blockchain technology (see table 2.3).

Table 2.3 Overview of technology areas in the socio-cultural world

Technology area	Description
Social media (incl. VR and AR)	Social media and our smartphone fuse the virtual and physical world. The next step in this fusion is applying virtual reality and augmented reality.
Digital platforms (incl. blockchain)	Digital organization models play an increasingly greater role in arranging and facilitating transactions in the economy and in society. New digital platforms are emerging everywhere, disturbing the 'old' organization models.

Rathenau Instituut

2.4 The digital world

The previous section showed that many aspects of our material, biological and socio-cultural lives are already represented digitally. This has steadily expanded our digital world. There are other key technologies in that digital world, which we will illustrate here: 1) big data and algorithms, and 2) artificial intelligence.

Big data and algorithms

In 2011, consultancy company IDC calculated that the digital omniverse consisted of 1.8 'zettabytes'. Converted into Apple iPads, that boils down to enough tablets to build a Chinese wall twice as high as the original (IDC 2011). Since then, the extent of the digital world has grown exponentially and seems to have its own 'Moore's law': every two to three years, the amount of data doubles (Mayer-Schonberger & Cukier 2013b; IDC 2014); a phenomenon that is now known as 'big data'.[16] The data comes from cameras, smartphones, tablets or other portable devices, or from browsers and social networks. Users download more than 10 million new photos to Facebook every day. Other data sources are cloud services, and the growing application of sensors in products and machines connected non-stop to the Internet.

That ever-expanding digital world also means that we are becoming increasingly dependent on smart algorithms (software) to extract information from all the bits and bytes. Data collections and data analyses are becoming more complex. Companies and governments use (self-learning) software more frequently to make processes more efficient, for example on the stock market, when providing credit, detecting fraud, or regulating content on social media.[17] That is not always successful and it can be tricky to ascertain on the basis of what information the software reached a particular insight. The more often software makes decisions automatically, the more crucial it becomes to control these systems. Technology also plays a role here. With WatsonPaths for

[16] There is no single definition of big data. Some refer to its core characteristics: volume, variety and velocity (the 3Vs) (Gartner 2011). For others, besides quantity, big data is also about the combination of quantities of data and software that can find unexpected – valuable – correlations based for example on pattern recognition.

[17] In regulating content on websites and forums, the software automatically determines what is permissible and what is not (such as discriminatory texts or snide remarks). The Russian internet critic Yevgeni Morozov suggested in 2014 that in this way the Silicon Valley software is imposing a new kind of conservatism on society, where algorithms determine what is culturally acceptable or not (Morozov 2014).

example, IBM is trying to create a medical decision system that can explain what information sources the system has consulted, and what paths it has explored to come up with an option (IBM 2013).

Artificial intelligence

Data mining techniques (*data analytics*) and artificial intelligence (especially techniques such as *deep learning*) benefit immensely from the large amounts of data that have become available in recent years (see Box 2.5). Self-learning software is trained with these data: the more data the software gets, the smarter it becomes. Companies like Facebook and Google have facial recognition software that is improving quickly thanks to the many photos that users upload every day. Translation software is also improving because it can draw on a large number of officially translated documents from the United Nations and the European Commission (Mayer-Schonberger & Cukier 2013).

Box 2.5 Deep learning

Deep learning, a form of machine learning that leans heavily on statistical calculations and neural networks, has been partly enabled by the emergence of big data (The Economist 2015). Instead of attempting to define what rules a computer must apply to ‘understand’ for instance language, computer scientists are making use of the increasing amounts of data to allow software links or rules to be discovered.

Via *deep learning,* computers abstract information based on various layers of neural networks. In image processing, the first layer is shown raw images. It may for instance try to identify contrast and colours. A second layer combines that information and makes more abstract observations such as borders or shadows. The next layer looks to see if it can thereby identify eyes, lips or ears, enabling it to recognise random faces (The Economist 2015). These models are now still learning with the help of people, who indicate whether an image is a face or not, but work is also being carried out on *unsupervised learning* whereby the software learns on the basis of self-exploration and auto-correction.

Overview of technology areas

This section has shown that big data and algorithms as well as artificial intelligence, are key areas of technology expected to shape the digital society. Many of the technology areas discussed in the previous sections depend on progress in artificial intelligence and big data (table 2.4).

Table 2.4 An overview of technology areas in the digital world

Technology area	Description
Big data and algorithms	Algorithms are becoming more and more important for extracting information (connections and patterns) from the expanding digital world.
Artificial intelligence (*deep learning*)	Artificial intelligence – giving a system a form of intelligence – supports all kinds of technological processes (for example in robotics, language processing or smart environments), and is finding its way into increasingly more software applications.

Rathenau Instituut

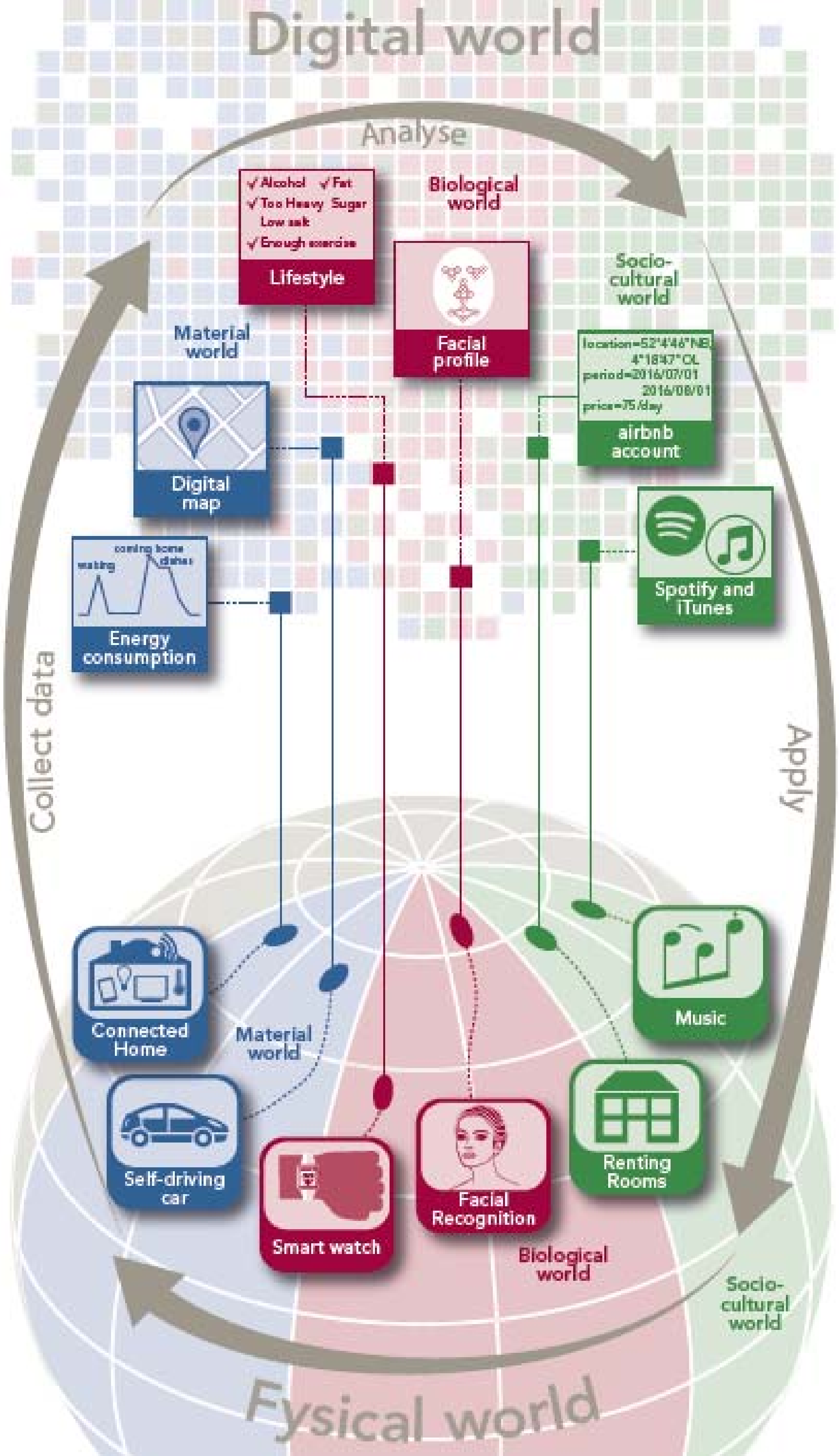
2.5 The four worlds in one: a new phase in the digital society

In the previous sections we looked at the *objects* of digitization. Whereas digitization was initially about the collection of data on (parts of) the material, biological and social world, nowadays we can analyse this data on a large scale and apply the acquired knowledge directly in the real world. For example by using sensors, train manufacturers can monitor their train fleet, carry out preventative maintenance and at the same time coordinate their technicians. Or the self-driving car that makes use of digital maps that with every meter it drives, adds information to that digital map, thus improving it. Or data surveillance, whereby companies track user actions, profiling them and on that basis show real-time ‘appropriate’ information, products or prices (see Figure 2.3).

The interconnection of the four worlds leads to continuous feedback loops between the physical and the digital world that manifest themselves in many areas: the production process, the environment, our bodies and our behaviour. Although digitization has been going on for decades, it has recently become easier to intervene real time in the physical world at an increasingly detailed level. This seems to have ushered in a new phase in the development of the digital society; a phase in which a cybernetic loop exists between the physical and the digital world (as shown in Figure 2.3). It means that processes in the physical world are measured, the resulting data is analysed, and then real time intervention takes place based on that data analysis. The impact of the intervention can subsequently be measured, analysed and adjusted, before rejoining the following cybernetic loop cycle.

We see in this a return to the so-called ‘cybernetic thinking’ that attracted interest in the 1950s and 1960s. The basic idea of cybernetics is that biological, social and cognitive processes can be understood in terms of information processes and systems, and thus digitally programmed and controlled (de Mul 1999). Meanwhile, ICT control is right back in the spotlight. Everywhere we see futuristic visions emerging about smart environments focused on digital control: smart cities, smart energy networks, smart factories, hospitals, offices, houses and so on. Digital control offers society and the individuals in that society a multitude of opportunities: from cheaper or more sustainable production, to early detection or prevention of diseases. But it also causes concern, for example about manipulating human behaviour and what makes us human. In the next chapter we will delve deeper into these ethical and societal issues.

Figure 2.3 Cybernetic feedback-loop between the digital and the physical world



2.6 Ultimately

The key question in this chapter was how to grasp the digitization of society. We charted the resources for digitizing such as computers, software and the internet, and illustrated the digitization of new objects in our environment. More and more sections of our material, biological and socio-cultural worlds are being represented virtually in the digital world. Ultimately, digitization does not appear to be a new development, but – now that so many things in our lives are digitized – a new phase in the digital society seems to have arrived: a continuous feedback loop and interaction between the physical and virtual world, which allows real time intervention.

We selected eight technology areas that are expected to shape the digital society in the coming years (see Table 2.5). In the next chapter, we use these technology areas to analyse the societal and ethical issues they raise.

Table 2.5 Technology areas in the four worlds

Material world	Biological world	Socio-cultural world	Digital world
Robotics	Persuasive technology	Platforms	Artificial intelligence
Internet of Things	Multimodal biometrics	VR/AR and social media	Big data and algorithms

Rathenau Instituut

3 Societal and ethical issues in digitization

3.1 Introduction

The digitization of society pushes the boundaries of our abilities and offers all sorts of opportunities, but also challenges our moral boundaries. In this chapter we describe what social and ethical issues arise when society becomes digitized.[18] To do so, we take examples from the technology areas discussed in the previous chapter: Internet of Things, robotics, biometrics, persuasive technology, virtual & augmented reality, digital platforms, big data, smart algorithms and artificial intelligence. Our description is not exhaustive but gives an idea of the various types of societal and ethical issues that arise as a result of digitization. We approach ethics as the systematic reflection on morality, the entire set of standards and values that actually exists in a society (see box 3.1). We thus look at ethics as something that plays a role not only on an individual level, but also from the viewpoint of ethical values in a society (both individual and social).

Box 3.1 Ethical and social issues

In this chapter we discuss the social and ethical issues that arise as a result of digitization. It is not easy to say what ethics is exactly. Here we define ethics as the systematic reflection on morality, the entirety of norms and values that actually exist in a society. Such a reflection can increase our ability to deal with the moral issues associated with digitization. The developments within the technology areas we have selected will digitize our society still further. This raises the question of how we can shape that digital society in a socially and ethically responsible way. Based on the selected technology areas, we will highlight the many developments in the digitizing society that appear to be at odds with ethical values, such as privacy and autonomy. This chapter charts these ethical values. The follow-up question is then how to safeguard these ethical values or at least how we can best protect specific values. That governance issue is the theme of the following chapter.

In a similar vein as the previous sections, this chapter looks at the issues which arise in the material (section 3.2), biological (3.3), socio-cultural (3.4) and digital worlds (3.5). This overview illustrates the most prominent issues and the developments taking place relating to these issues. Our analysis of the scientific literature on technologies revealed several recurring themes. We have

[18] We recognize the many positive effects of digitization development. Because this text aims to shed light on the areas in which ethical and social values are at stake, we focus on those situations where digitization has a potentially undesirable impact..

applied these themes – privacy, autonomy, security, controlling technology, human dignity, equity and inequality, and power relations – to structure our discussion in this chapter (see Table 3.1). The various ethical and social issues manifest themselves per technological area in different ways. Privacy, for example, takes on a whole different meaning in the context of robotics than in the context of virtual reality. Not every theme is explored in depth for every development; we focus on the distinctive issues that a particular technology demonstrates within the overarching trend of digitization. Finally, our summary in section 3.6 shows which ethical and social issues have explicitly put the new wave of digitization on the map. We briefly indicate how the issues in this chapter relate to important values as laid down in international treaties. Our insights on ethical and social issues are linked to the insights on the development of digitization that we mentioned in Chapter 2. Based on the various phases in the cybernetic loop – collection, analysis, and application (see Figure 2.3 in Chapter 2), we see various ethical and social issues emerging. They give us an idea of which aspects related to the development of technology require attention in the coming years.

Table 3.1 Social and ethical themes

Theme	Issues
Privacy	Data protection, privacy, spatial privacy, mental privacy, surveillance, function creep
Autonomy	Freedom of choice, freedom of expression, manipulation, paternalism
Security	Information security, identity fraud, physical safety
Controlling technology	Control and transparency of algorithms, responsibility, accountability, unpredictability
Human dignity	Dehumanization, instrumentalization, de-skilling, de-socialization, unemployment
Equity and equality	Discrimination, exclusion, equal treatment, unfair bias, stigmatization
Balance of power	Unfair competition, exploitation, shifting relations between consumers and businesses, and between government and businesses

Rathenau Instituut

Methodology

The research to describe the ethical and societal issues raised by digitization was done by carrying out a literature review.[19] The scientific literature from 2010 was investigated for each area of technology, using search engines such as Google Scholar and Scirus as well as the PiCarta database. Combined with the term for the technology (or related terms and synonyms of this technological field), we entered the following search terms for each area of technology: ethics, ethical, moral, morality, normative, or normativity. This resulted in approximately 100 publications per technology area. After an initial screening, they were reduced per technology area to between 20 and 40 scientific publications considered the most relevant for this research. Based on this selection, we describe the most important ethical and social issues per technology mentioned in the

[19] We are indebted to Luca van der Heide for collating the specific literature for this review.

literature. As stated earlier, although not exhaustive, the list of ethical issues does show which issues can arise relating to the digitization of society and which are considered the most urgent and problematic in the scientific literature. In addition to scientific publications, the desk review included consulting all kinds of newspapers and news sites to illustrate certain issues based on compelling reports in the news.

3.2 Material world

3.2.1 Internet of Things

The Internet of Things (IoT) is based on a worldwide network that integrates the physical world with the virtual world of the Internet. Through the emergence of IoT, we are on the brink of a new era in which objects and people in the material world can be monitored, and where objects and people can exchange information automatically. In this way, the alarm clock does not just wake up a person, but at the same time switches on the coffee machine for making fresh coffee with our breakfast; or the fridge tells us a product has passed its expiry date; or the lighting in the room adjusts itself to what is happening in a video game being played at that moment.[20]

Many technology companies predict that IoT will be omnipresent in our daily lives in the future. Many of the technologies we describe in this chapter are part of IoT: like the augmented-reality glasses which use the Internet to give users real-time additional information about their environment, or a biometric camera which can be linked to an online database to recognize faces.

Privacy: digital home

Through IoT, more and more information about ourselves is being exchanged, without us really knowing or having control over it (Barbry 2012; Peppet 2014; Romana et al. 2013). Samsung’s 46-page privacy policy that comes with its smart TV, tells you that Samsung registers where, when, how and what time you have your TV turned on. The TV also has a camera for face recognition and a microphone for speech recognition. Samsung’s manual warns you to watch out what you say in the vicinity of the TV: 'Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party.' This led to quite a fuss (Gibbs 2015). The example shows that permission is given unwittingly to use certain data, because people are not able to understand the entire manual or are suffering from so-called *consent fatigue* due to the large amount of permissions they have to grant about using data that devices capture (Pereira, Curvelo & Benessia 2013). This raises the question of where the responsibility lies in this process: should the user be expected to sift through the conditions for each and every device? Or do the manufacturers of all these devices also bear some responsibility? Should they not ensure a certain reasonable expectation of privacy?

Because of IoT, we can in fact be followed everywhere, which can lead to huge transparency at the expense of our privacy. In most cases, the data collated by smart toothbrushes, thermostats,

[20] youtube.com/watch?v=1Y3MQrcekrk

televisions, refrigerators and washing machines are the property of the manufacturer, not the user. The home, which we consider to be our private domain, is thus becoming transparent, because processes in the home can be monitored via the IoT devices inside our houses. The distinction between home and the outside world is blurring as the walls and curtains no longer protect the house against prying eyes. That is why Koops & Prinsen (2005) argue for protecting citizens against this digital spying and for providing citizens with digital privacy alongside physical privacy in the home. This should ensure protection against observation from outside with technical aids, so that citizens have a place where they can “pre-eminently be themselves” (Koops & Prinsen 2005, p. 630).

The question arises how citizens can control the data flows that contain all sorts of personal information that originates in the IoT. Not only is the amount of data growing, it is becoming increasingly difficult to make an informed choice because the many smart devices operating in the background do not have an easily accessible screen for settings or privacy notifications. One solution is a digital privacy assistant; this is a programme which enables the user to indicate their privacy preferences, thereby making the settings better and easier to manage. At the same time, some experts in industry and science think that consciously exercising control over the numerous data flows is almost no longer feasible in the IoT era (Eskens et al. 2016). Currently the responsibility for managing information flows falls mainly on the shoulders of the individual, but there is a noticeable shift towards the responsibility lying more with the manufacturers. Responsible information management is becoming part and parcel of delivering a reliable product.

The manufacturers’ responsibility can be about checking which devices are allowed to communicate with each other and which are not. A refrigerator, for example, does not need to communicate with the neighbour’s car. A solution for household appliances could be that these devices only communicate with each other via a closed network, ‘a personal cloud of things'. You don’t really need a world wide web for such appliances. This approach of opting for protected privacy is also called *privacy by design*. A perspective on privacy that goes further than controlling information allows us to consider other aspects of privacy, such as the freedom not to be monitored and the freedom to develop your own identity (Zureik et al. 2010). What is the impact of a smart TV that is continuously monitoring for instance the freedom of expression and identity of the occupants in a house? These are precisely the types of questions we see moving to the forefront as more smart and measuring devices nestle in our environment.

Autonomy: technological paternalism

The IoT combines the three steps in the cybernetic loop: collect, analyse and apply. Smart devices with sensors collect data on behaviour (how the thermostat is used), analyse data via network connections (when someone is at home and turns on the heating), and provide an adjustment (the heating will automatically fire up before anyone gets home). The brain behind IoT consists of smart algorithms that analyse the data in the cloud (big data) and make a decision. In a car for example, a sensor can indicate that the fuel is running low. Subsequently the route to the nearest petrol station appears on the windscreen. Clearly a convenient service for consumers, but also for companies – in this case fuel producers – because such highly targeted marketing is lucrative. The algorithm could, for example, be implemented in such a way that it shows the route to the nearest petrol station belonging to the company that pays the most to the designer of the algorithm.

IoT does not just offer us comfort, but can also lean towards technological paternalism (Hilty 2015). We speak of paternalism if someone professes to know better what is good for other people than these people themselves. With technological paternalism, the paternalism is 'delegated' to technology. A smart fridge is technologically capable of changing the order for your favourite cheese to a low-fat cheese because the biometric sensor has measured that the particular person's cholesterol levels are too high. The question is, however, whether the fridge and the biometric sensor should be allowed to make such a decision together. This kind of technological paternalism has serious ethical implications for IoT: the implicit enforcing or provoking of certain behaviour can endanger personal autonomy. What is more, IoT can thus be implemented as persuasive or even manipulative technology (see subsection 3.2.2 on persuasive technology).

Even where paternalism is not directly involved, the way IoT affects our environment can restrict our autonomy. When a smart IoT environment anticipates our needs and wants, a choice is made about our supposed preferences – for example, suggesting a selection of certain TV programmes – based on previously displayed behaviour. With that choice, the smart environment sorts our options and steers us in the direction of certain choices and behaviour. The way subtle changes in our behaviour can be accomplished through technology became apparent from the Facebook emotion experiment in 2014. By adapting the number of positive and negative messages in users' *newsfeeds*, they were able to influence users' state of mind without them being aware of this (Kramer et al. 2014).

Hildebrandt (2012; 2015) puts forward that a future generation of technology could be so sophisticated in reading our preferences, that it detects preferred choices before we ourselves are even aware of them. She outlines the scenario of a smoker: someone profiled as almost wanting to stop the habit, but has not yet consciously made that decision; they are subsequently targeted via ads and news reports criticizing the negative effects of smoking, to steer them in a different direction. According to Hildebrandt, providing transparency in the profiles on which automatic decisions are based, is an essential condition to protect the autonomy of the individual. The recently adopted European data protection regulation is a good starting point, even though implementing the included transparency obligations in a meaningful way for users still presents a major challenge.

Security: information security gets a physical dimension

Digitization also presents serious crime problems: the Internet or the devices connected to the Internet can themselves be the target of crime, as is the case with hacking or DDoS (*Distributed Denial of Service*) attacks which paralyse websites or systems. Experience shows that virtually any digital system can be hacked. This means that malicious parties can gain access to sensitive information, and that information could end up in the hands of the wrong people. A hacked smart meter could give burglars insight in the exact times of the day or week when we turn the heating down and are – evidently – absent. Besides extracting information that is valuable to them from smart devices, criminals can take over the control of smart devices. This adds a physical dimension to the issue of security. A security researcher demonstrated how simple it is to hack the toy doll

Cayla, and have it quote passages from the erotic novel *Fifty Shades of Grey* and from the fictional psychopath Hannibal Lecter in the book *The Silence of The Lambs*.[21] The hacking of the doll is a relatively harmless example, but New Zealand hacker Barnaby Jack showed at a conference in 2011 that he could hack his friend's insulin pump. He could take complete control and was able to administer a fatal amount of insulin. Other hackers have also already pointed out that they could take control of a wireless pacemaker and have the device deliver a fatal shock (Greenberg & Zetter 2015). This was what caused former US Vice President Dick Cheney to fear the reality of the situation; he had the wireless function on his pacemaker removed and the device controlled in an alternative way. In the Netherlands alone, there are thousands of people walking around with a similar wireless pacemaker, which highlights the extent of the consequences if criminals were to hack all these devices.

The issue of security is becoming even more complicated because of the fact that IoT devices are connected to each other. So, for example successfully hacking a coffee machine can give you access to a car or open the front door. In addition, this type of security issue is new for many manufacturers of consumer electronics, which means it has not always been given much thought. As hacker Runa Sandvik neatly surmised, "When you put technology on items that haven't had it before, you run into security challenges you haven't thought about before" (Greenberg & Zetter 2015).

Control: unpredictable network effects

Controlling data is one thing, but control in relation to the IoT involves different aspects. Not only has the number of IoT devices greatly increased in recent years, equally the number of potential interactions between these devices is increasing steadily. As described above, this can lead to security issues. A poorly secured device can allow access to another device, resulting in unexpected and unpredictable interaction effects between the devices. This is what happened when a Berlin computer scientist's smart home was paralysed – it did not react to any command; lights, kitchen appliances and heating could not be switched on or off – because one of the smart lamps had burned out, the constant flow of messages saying that the bulb wanted to be replaced, had shut down the entire home network (Hill 2015). It is still not clear who is responsible for the consequences of these kinds of unexpected effects at system level (Weber 2011).

Balance of power: 'Everything-as-a-service'

IoT devices are often offered as part of or in combination with a software service. Thus the sale of a smart TV or smart refrigerator can include software support. The product's capabilities are for the most part embedded in the accompanying software. Thus the ability to have the refrigerator in the morning display the schedule for the following day, is dependent on the manufacturer's software support. The manufacturer can decide to stop offering support for older appliances, rendering them partially or entirely useless. The Electronic Frontier Foundation raised the alarm because consumers, having forked out hundreds of dollars for a smart home console with lifetime software support, were suddenly left with a worthless product because the support was removed after a competitor took over the company (Walsh 2015).

[21] mirror.co.uk/news/technology-science/technology/friend-cayla-doll-can-hacked-5110112

When products become more dependent on software controlled by the manufacturer, this strengthens the manufacturers' control and how that can be utilized. In addition, there is a noticeable trend that the products themselves are being offered as services. This is called 'servitization'. One example is that consumers no longer buy light bulbs but purchase light as a service. They do not purchase a washing machine but make use of washing services. The manufacturer is responsible for the maintenance of the appliances, consumers only need to pay a periodic fee. Proponents advocate the convenience that such services provide, whereas opponents see consumers' control of their own environment dwindling; it is for instance no longer possible to unscrew or adjust something yourself. The manufacturer retains ownership and can decide to change the product in some way whenever they like. A case in point is when Amazon decided to remove from customers' eReaders certain eBooks by George Orwell, notably the author of the work *1984*, due to a conflict with the supplier about copyrights. Amazon was allowed to do this, because customers did not officially purchase the books, but had them on loan from Amazon (Stone 2009).

3.2.2 Robotics

The development of IoT and robotics is strongly linked. Just like IoT devices, robots are mostly equipped with sensors to read their environment; they are increasingly connected to the cloud to share and analyse data, and on the basis of those analyses, carry out independent actions. Although some issues consequently overlap, robotics triggers its own set of specific ethical dilemmas.

Privacy: *pervasive monitoring*

Just like the IoT, robots contribute to the increasing potential for collecting data in situations where formerly no (digital) data collection took place. Robot technologies can be deployed in a variety of ways to monitor certain situations, such as a patient's wellbeing, a car driver's state of mind or the safety situation on the street. As a direct result, robot technologies can invade our privacy in all sorts of ways. Robots and domotics for example, can monitor people, record and pass on details of their physical condition, and even enable a care recipient to be watched 24 hours a day with a care receiver. As this data provides a great deal of information on the care recipients' daily ups and downs, it thereby raises issues about their privacy. Care recipients will not appreciate for example that it is recorded when they are not yet dressed or about to have a bath. This issue is more complex when it comes to older people with dementia: to what extent can they show whether they are aware of the presence of a technology that captures their daily lives (Borenstein & Pearson 2010)?

Another important privacy issue that frequently reoccurs with digitization, concerns the possibility that technology is used for a different purpose than originally intended. This change in original scope is also referred to as *function creep*. A prime example is the digitization and robotization of the car. The European Commission has made the eCall system – that automatically alerts emergency services when there is an accident – compulsory in all passenger vehicles sold after 2018. The European Parliament has insisted that this eCall system will have a 'dormant existence' and will not take any action until an accident has happened. This system cannot therefore be used to track down criminals. Function creep, however, is always lurking. The question is whether such possibilities might nevertheless be used in the future to collect data for detecting or maintaining (traffic)security. For example, in 2011, we learned that the cameras supervising polluting lorries in Amsterdam would also be used to check if licence plate owners had chalked up any history of things like unpaid fines. According to Amsterdam newspaper 'Het Parool', this fulfilled a long cherished desire of former chief of police Bernard Welten: to create a 'digital moat' around the city.[22]

Autonomy: 'man out-of-the-loop'

In robotics we see a shift "from *in*-the-loop to *on*-the-loop to *out*-the-loop" (Sharkey 2010), which is also noticeable in IoT. In the loop means that the person is in control and human permission is required to have the system carry out an action. On the loop means that the person makes a decision based on information in the system. Out the loop refers to a situation of full automation, where the system makes a decision without human intervention. The shift from *in* to *on and out* the loop has occurred due to the increasing amount of information from various sources/devices that has to be integrated and subsequently interpreted to come to a decision. Robots can do this far more efficiently and effectively than humans, for whom it is almost impossible. As a result, people in fact no longer make the decisions themselves but leave it to technology. Examples include knowledge systems that make medical diagnoses based on a large amount of information, military robots that take life or death decisions using information from various sources, and the driver support systems that decide what speed we should drive on a particular stretch of road. It raises the question of how these systems come to their decisions and if the competitor's software would make the same decision.

Ethical questions regarding autonomy need answers: in what circumstances and to what extent may people's personal autonomy be affected? Where is the leeway for making your own decisions? And what consequences does the impairment of personal autonomy have on the role of people's own responsibility? Regarding the latter, people are inclined to trust and rely completely on technology. But what happens when the technology fails – for example, if no signal is given that the car might hit the wall, and it goes wrong – who is responsible for that?

Thanks to the huge advances in artificial intelligence, robots are becoming more and more autonomous. The crucial question is: to what extent is it ethically acceptable to delegate the responsibility for moral decisions to robots? This is an ongoing debate in the field of military robots and self-driven cars. According to Arkin (2010), the military robot will surpass humans when making moral decisions, because human soldiers undergo tremendous stress in the battlefield, and robots – free from stress – make fewer mistakes. The problem here is that robots cannot be called to account, and for many scientists, that is the reason why robots should never be allowed to make life and death decisions.[23]

[22] *Het Parool* (7 September 2011), Digitale ring scant alle auto's [*Digital moat scans every car*].

[23] When the International Committee for Robot Arms Control (ICRAC) organized an expert workshop 'Limiting Armed Tele-Operated and Autonomous Systems' in 2010, the majority of the attendees signed a statement emphasizing the necessity to limit armed military robots and ban autonomous armed military robots, the underlying thought being that a human being must always make life and death decisions (icrac.co.uk/Expert%20Workshop%20Statement.pdf). See also the open letter from more a thousand experts regarding AI and robotics in 2015 (futureoflife.org/open-letter-autonomous-weapons).

The same problem occurs with self-driven cars. Traffic accidents are inevitable, also with a self-driven car, and so this car will experience situations that require a moral decision (Goodall 2014). In such a situation, a human driver acts instinctively; It is impossible to expect him in half a second to make a well-considered choice between driving into a truck or mowing down a child on the pavement. For a self-driven car, however, half a second is more than long enough to asses various scenarios. Should the car choose the least injury to the occupants of that car or, for example, for the least total damage, thereby also taking other road users into account? The question we need to ask before this issue arises is: Do we leave this moral decision to the self-driven car, or do we determine beforehand what this car should decide in situations where it cannot avoid an accident? Here, too, many people will tend not to let a device make a decision, but leave this choice to a person because it involves life and death. This brings us to the next question: who should decide how the self-driven car must 'behave' in this kind of situation? Consumers, the government, the designer, or the manufacturer? This complexity of questions will surely have to be answered before self-driven cars become available to consumers.

Security: hacking robotics

Just as with the IoT, robotics clearly demonstrates that digital security is acquiring a physical dimension. The digitization of the car makes it vulnerable to hacks. Viruses can disrupt cars so severely that they become uncontrollable and perform unwanted actions. It is even possible to get full control of a car by 'hacking' it. The same applies, probably to a greater extent, with military and police drones. In 2012, researchers at the University of Texas demonstrated to the US Department of Homeland Security how relatively simple it was to hack into and take over control of a drone.[24] To do this, they used the technique known as *spoofing*: obtaining unauthorized access to a device by forging the identity of the person controlling the device. There is indeed a fear of cyber-terrorism in policy circles.

Human dignity: moral obligations for robotization, dehumanization and unemployment

A key question in the development of robotics is when to apply it. Robots can benefit people's well-being, but also lead to dehumanizing situations.

One of the positive contributions of robotics is that robots are able to carry out '*dirty, dull & dangerous'* work. Certain tasks can indeed be so dirty, mind-numbing or dangerous that it is undesirable to have people carry out such work if it is also possible to have a machine do it. Strawser (2013), for example, finds it morally repugnant to give a soldier a command that puts him in mortal danger if a military robot could otherwise have carried out that order. This 'principle of unnecessary risk' results in an ethical obligation to apply robotics in certain situations, for example when detecting and dismantling roadside bombs. Turning to a different profession, we see that prostitution has been legal in the Netherlands since 2000, but it is often dirty, dangerous and degrading (Werson 2012). According to the national police, between fifty and ninety percent of the 25,000 women working as prostitutes in the Netherlands are doing so involuntarily (KLPD 2008). A topical issue is how politicians can combat such serious and certainly traumatic human abuse for the women concerned. The emergence of the latest robotics adds a new perspective to this debate.

[24] bbc.com/news/technology-18643134

An important discussion point is whether in the long term, sex robots can provide a reasonable alternative to human prostitution. Facing such an alternative, or given the many degrading circumstances in prostitution, should the next step be to make the use of sex robots an ethical obligation.

The 'principle of unnecessary risk' applies to various areas (Rahul & Velez 2015). Robotics offers numerous possibilities for improving the safety of the current traffic system, including the existing intelligent speed assistant (ISA) system. This ISA system provides information about the speed limit and warns or intervenes if a driver exceeds that limit. According to experts, making compulsory the intervening aspect of the ISA system would decrease the number of traffic fatalities by 20 percent in Europe.[25] In 2014, nearly 26,000 people were killed on the roads.[26] New robotics clearly raise the question of whether or not we are morally obliged to make automatic speed limitation in cars legally compulsory. Although this would be a curtailment of individual autonomy, the trade-off can be made that this restriction is justifiable due to the reduction in the number of road accident victims. Another application is, for example, medical operations. With a surgery robot like the Da Vinci robot, doctors can perform much more accurate and less invasive procedures. [27]

The negative side of robotization becomes apparent especially where the use of robotics leads to dehumanization. Although robotics can provide great support in health care, entertainment, the police and the army, if the technology is not applied within certain framework conditions, it can undermine human dignity. We are talking about the risk of objectification or instrumentalization of people, in other words dehumanization. The health care sector seems to be anxious about the implementation of robotics. The way robots are deployed seems to be the crucial fear. Coeckelberg (2010) argues that care robots should only be used for 'routine care tasks'. That means tasks for which no emotional, intimate, personal involvement is required. The '*care giving'* is restricted to people. If robots are deployed to replace the caregiver, there is a risk that care is dehumanized (Sharkey 2014). When robots take over tasks such as feeding and lifting, the care seekers can feel like objects. What is more, it is likely that older people will feel they have less control over their lives than if they are looked after by carers. The ethical complaint about 'objectification' ties in with the idea that robots cannot provide care. The underlying argument is that robots are devices which are not able to replicate the empathic capacities and reciprocity of human care relationships. Human contact is usually found to be essential for providing good care. The patient's quality of life should therefore be the guiding principle for robotics in healthcare.

There is also a risk of dehumanization in other areas of care. Soldiers or police officers who control robots remotely, are not present in the danger zone. In this situation, the use of tele-guided robots thus maintains an emotional and therefore moral distance between the action and the ethical implications of that action. Proponents argue that this can reduce psychological suffering among soldiers and ensure decisions are more rational. Critics fear that the danger lurking in creating more distance between an action and its consequences, is that controllers make important, sometimes life or death decisions, as if they are playing a video game. Moreover, for making their decisions,

[25] http://www.rospa.com/roadsafety/adviceandinformation/driving/speed/

[26] ec.europa.eu/transport/road_safety/pdf/observatory/trends_figures.pdf

[27] erasmusmc.nl/davincirobot/DaVinciRobot

the controllers are dependent on the limited information provided by the robot. Tele-guided armed robots can heighten the risk of dehumanizing the enemy and desensitizing the controller (Royakkers & Van Est 2016).

Another aspect that has led to a great deal of discussion in recent years is the potential impact of robotization on employment. Robots are not only capable of supporting human tasks, they can gradually replace more and more human tasks and therefore also jobs. Two opposing views dominate this discussion on the effect of automation: on the one hand robotization leads to economic growth, employment growth (new jobs are created) and an acceptable distribution of wealth; on the other hand, robotization leads to fewer jobs and consequently declining prosperity.[28]

The preservation of human dignity is crucial for the social acceptance of new robotics. Although robotics can play an important role in enhancing people's wellbeing, this also means we need to think carefully about the ways to safeguard human dignity. The developments in robotics show that these issues will not only rear their head in the long term, but are forcing us now already to reflect on current practice.

3.3 Biological world

3.3.1 Biometrics

Biometric information enables the use of unique physical characteristics – such as a person's face, voice or fingerprint – for verification or identification purposes. An example of verification through biometrics is the electronic border control (e-gates) at airports. The traveller puts their passport on a reader, looks in the camera and the gate then opens or not. The identification system operates as follows: a digital image of the face stored in the passport is compared with the picture of the face taken when the traveller looked in the camera. If the biometric system – in this case a face recognition system – decides that the face stored in the passport is the same person as in the picture, the passport control system concludes they must be the rightful owner of the passport and opens the e-gate.

Privacy: *privacy enhancing* versus losing control of sensitive information

In relation to privacy, biometric technology is a double-edged sword. It can be used to protect privacy, whereby only the minimum amount of information is required to determine whether someone is entitled for example to enter a building or to buy alcohol. On the other hand, because biometrics can identify sensitive information, controlling what happens with that information may be tricky, especially now that the technology has reached the stage of being applied in many more devices and situations.

In the above example of the e-gates, biometrics is implemented in such a way that privacy is guaranteed. The identity of the user is not released, only authentication takes place: is the face in front of the camera the same face as in the passport? Verification can also be done by comparing

[28] For an extensive study on this topic, see Van Est & Kool (2015).

someone’s biometric characteristic with the information already stored about that person. For example, if wine shops make use of a biometric fingerprint system to verify that someone is older than eighteen, all they need to know is that the information in the fingerprint belongs to someone over the age of eighteen. The name of the customer is not important. Thus biometrics can be a good way to prove legitimacy while maintaining privacy.

Other applications of biometrics are particularly aimed at identification. For example, someone’s facial profile is compared with a database to see if the scanned person appears in that database. The technique is applied in police investigations or for security cameras in public spaces. This use is regulated by law; importantly, such highly sensitive information must be stored safely and securely. The biometric data can namely contain information about the user’s health and ethnicity (Juul 2013). It could be undesirable that for example an insurance company or employer gets a hold of the information. This problem is aggravated by the fact that modern biometric identification methods can also find indications of a person’s health risks. An iris scan can for example determine diabetes or high blood pressure. Irregularities in fingerprints may indicate leukaemia or breast cancer.

In order to prevent the privacy risks of biometrics, it is vitally important, according to Veldhuis (2015), to store biometric data in such a way that it can be used for recognition, but without disclosing information on the underlying biometric characteristic. The answer can be to apply technical solutions such as biometric template recognition[29] and smart cryptographic encryption. At the same time, when it comes to biometrics, function creep and the improper use of data are lurking around the corner. As regards purpose limitation in biometrics, it is a question of whether the biometric data is adequate, relevant and proportional in relation to the purpose for which it was collated. There are examples in the past where these criteria have not always been met (Renaud, Hoskins & Von Solms 2015). In a Glasgow nightclub, staff used a fingerprint reader to verify the age and identity of its customers. The club claimed this was to reduce the city’s alcohol problems. It turned out later, however, that the scanning was for the convenience of the bouncers and to make greater profit by profiling the clubbers’ identity more intelligently.

Recent years have seen huge advances in biometrics. The presence of large databases with photos, the accessibility of software, and the ubiquity of cameras in smartphones, ensure an uptake of facial recognition technology in an increasingly wider range of situations (Jansen et al. 2015). Scientists showed that by using facial recognition technology and public data in Facebook profiles, they could identify a third of the students on a university campus (Acquisti et al. 2014). The fear is that accessible facial recognition technology could ultimately lead to a situation where it is no longer possible to walk down the street anonymously. The app FindFace, which was launched in Russia in 2016, allows users to compare a picture they have taken of someone on the street, with profile photos on Vkontakte – the Russian counterpart of Facebook – in order to discover someone's identity. “If you see someone you like, you can photograph them, find out their identity, and then send them a friend request,” according to one of the app’s creators (Walker 2016).

[29] *Biometric template recognition* uses only a profile of the distances between different facial characteristics, without having to store the original image. The template can thus be separated from data identified on an individual (Veldhuis 2010).

The next generation of biometrics not only gives insight into “who you are” but also focuses on the question “how you feel” (Mordine, Tzovaras & Ashton 2012). Emotion recognition technology for example gives insight into people’s state of mind, and can even be used to expose emotions that people try to hide, by examining people’s unknowingly automatic non-verbal comments (Dwoskin & Charlotte 2015). This is an invasion of a new field of privacy, namely “mental privacy”. We are talking about people’s right and ability to keep private what they think and feel. In addition to facial expressions, other forms of behaviour can be analysed. Certain ways of walking, grimaces and other facial expressions can reveal something about a person and their behaviour. The extent to which a person has control over whether they submit the above data seems to be limited, as the collection of this information can be done remotely and covertly, for example by inserting facial recognition technology in mannequins,[30] without the knowledge of the person being observed (De Hert & Sprokkereef 2012).

Security: identity fraud

PwC research (2013) shows that identity fraud is a major social problem that will probably only increase in scope. Identity fraud is the intentional obtaining, appropriating, owning or creating of false identifiers, thereby committing or intending to commit unlawful conduct. Advanced biometrics has to reduce identity fraud. Passports nowadays have a chip with a facial scan and digital fingerprints. In the United Kingdom they use iris scanning. Besides the frequently mentioned convenience for users, biometric recognition also has the advantage from a security point of view that the user must be physically present. This reduces the risk of fraud by means of falsification of documents, theft of cards and revealing of passwords.

Although biometrics offers advantages with passwords, PIN codes, magnetic strips et cetera, there are also significant downsides. As already noted, this is very sensitive information that should not end up in the wrong hands. Moreover, biometric technology is not infallible (Heimo et al. 2012): biometric systems can be misled with falsified elements, for example by means of spoofing: falsifying characteristics in order to assume a false identity temporarily. In this way German hackers showed that by using a couple of photos – among other things of a press conference – they could forge the German Minister of Defence’s fingerprint (Hern 2014). Another disadvantage is that in cases of biometric identity theft, no other fingerprint or facial profile can be made, unlike being able to request a new password. Less sophisticated methods of detecting identity fraud also led to the first horrific scenarios with securing fingerprints. In a car equipped with a fingerprint reader, during a car theft, in order to disconnect the security, the owner’s finger was cut off, so the perpetrators were able to drive off in the car.[31]

Human dignity: instrumentalization and the standard user

Biometric systems are indeed fallible. They can give both ‘false negative’ as well as 'false positive’ results. You get a ‘false negative’ result when the identification device does not recognize an authorised person. This need not be a problem if they can immediately try again to identify

[30] wired.co.uk/news/archive/2012-11/23/mannequin-spies-on-customers

[31] news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

themselves. But something like this can also cause a great deal of inconvenience. For example, a motorist in the United States had his licence taken away because the facial recognition system mistook him for another person. It took ten days of bureaucratic wrangling before he could prove who he was and finally get back his licence.[32] This example shows that the use of biometric systems can lead to instrumentalization of the individual, thereby reducing the individual to a data point in a system. The user-friendliness of biometrics is great if the system works well for people. But for those who are incorrectly identified as suspicious by the system, it is often very difficult to rectify errors. In addition, it appears biometrics cannot be used for everyone. Two percent of people's fingerprints cannot be 'read' because they are senior citizens or because of certain chemotherapy treatments (Renaud, Hoskins & Von Solms 2015). This kind of problem occurs in many digital systems: they are designed on the basis of particular standard user characteristics, which means they are not always accessible to people who do not conform with these criteria, for example because their name does not match the system, or they have changed gender.

Justice: classification and the presumption of innocence

The application of biometrics can result in misclassification and stigmatization, by automatically putting someone in a certain category, such as a terrorist, criminal or unreliable individual. This can lead to a reversal of the presumption of innocence. Biometric systems can cause someone to be considered a criminal until evidence to the contrary is furnished. It is highly likely that this stigma will stick with such a person, for instance because the presumption is stored in a database (Sutrop & Laas-Mikko 2012; Sutrop 2010). This could be reinforced by facial recognition, which makes it easier to figure out a person's identity. Thus the stigmatization of a person can take place without that person knowing about it. In the name of national security, it is only a small step to function creep.

3.3.2 Persuasive technology

Persuasive technology is defined by Fogg (2002) as a technology that aims to encourage people to change their behaviour. To achieve this, there should be the right motivation, the possibility to undertake action and a stimulus that induces certain behaviour. Persuasive technology is for example used to persuade a driver to wear a seat belt. Security is the motivation here. By sounding a signal when drivers are not wearing a seat belt, they can be persuaded to actually fasten the belt.

Autonomy: control and manipulation through technology

The most prominent ethical issue that imposes itself on persuasive technology is that of human autonomy: to what extent may we influence people and when can we apply this technology? According to Sahin (2012), persuasive technology should comply with the requirement of voluntariness to guarantee autonomy. An action is only done voluntarily if the action is done intentionally (the one acting is 'in control') and is free from controlling influences. For example, if someone does not want to wear the seat belt and hears a constant beeping sound, they are being subjected to a controlling influence – in this case a kind of coercion. The driver can only stop the irritating sound by fastening the belt. Besides this coercion, there are examples of manipulation of

[32] schneier.com/crypto-gram/archives/2011/0815

controlling influences (such as withholding information or deception) and excessive stimuli (for example a massive reward).

Ideally, persuasive technology aims to halt temptation, and have the user independently display the ‘desired’ behaviour. In that case, persuasive technology is training the user. The purpose of training someone is that they can function independently and no longer need guidance. Unlike training, manipulation aims to keep someone dependent. According to Spahn (2012), persuasive technology should be training not manipulation, and eventually make itself superfluous. An important condition for this is that the user shares the same goal of the intended persuasion. If a user wants to drive more sustainably, he will warmly embrace any attempt to help him achieve his goal. If the user does not share this goal, then an additional motivation can provide a solution, in this example by pointing out that it is financially attractive to drive sustainably.

Technology that triggers behaviour in a more compelling way is, however, not necessarily undesirable. Firstly, people themselves can opt for compelling technologies. Some people are very pleased with the peeping sound that a car makes if it is too close to another vehicle or object, for example when parallel parking, or with rest break software to prevent RSI with programmes that compel you to take a break. People decide for themselves, by not switching off these systems, to depend on this technology. Secondly, compelling technologies could be used if the individual’s behaviour can lead to a collective risk. Some people advocate mandatory speed limiters in cars, which restrict individual freedom but reduce the collective risk of other road users. Thirdly, technology can be used to stop people displaying various types of behaviour which, by definition, could be a danger to others, such as wanting to drive a car under the influence of alcohol. From an ethical point of view, the alcohol interlock system could be a justifiable argument.

As we have seen, persuasive technology can also feature in smart IoT environments. This means that influencing becomes part of the environment and in some instances occurs less consciously. This is the case when subtle feedback is given on ambient lighting (Maan et al. 2011), whereby the ‘nudging’ takes place at a low cognitive level without the user being aware of it. Such forms of persuasion may constitute a threat to the individual’s autonomy if behaviour is controlled without the individual knowing or being aware of it. Transparency and insight in the way persuasive technology is applied are therefore important factors for protecting autonomy (Compen et al. 2014).

Human dignity: unlearn moral skills

One objection to persuasive technology is that users’ actions have nothing more to do with ethics: they make no moral decisions but simply display controlled behaviour (Spahn 2013). A driver support system that constantly warns us if we are driving too fast can be very effective in terms of safety, but the risk is a certain reduction in standard awareness. Persuasive technology is potentially a powerful regulatory tool, but the moral issues call for further consideration of applying it as technical regulatory instrument. Critics paint a doom and gloom picture of persuasive technology creating a society whose citizens are controlled to behave according to the norm, without sensing that norm themselves. Internet critic Morozov (2013) therefore makes the case for technology that stimulates people’s deliberative capacity (the ability to gather information and consult with other people and exchange arguments), encourages reflection and from there ultimately leading to behavioural change. A washing machine can stimulate a user by means of a feedback mechanism to wash at an energy-efficient, lower temperature, but the user does not therefore automatically consider whether or not he should wash his clothes every day. A smart car prompts the user to drive more economically, but not to think about leaving the car in the garage for a day. In Morozov's opinion, persuasive technology should therefore encourage us to do the right things.

Balance of power: who sets the standards?

In relation to persuasive technology, a user is not able to engage in a discussion with the technology like they can with a human interlocutor. That makes for an asymmetrical relationship in this communication: the standard is set in the technology, and the user is unilaterally exposed to it. Spahn (2012) therefore argues that it is important that the user has as much influence as possible on how this standard is determined, and consciously agrees to applying persuasive technology. If a user decides to purchase a digital fitness coach, we can assume this is of their own accord. However, when persuasive technology is used in the context of a working environment or in insurance, this issue becomes more problematic (Timmer et al. 2015). It raises the question of whether the employer or insurer should be allowed to determine the standards for an employee or client's behavioural change, or if this is an infringement of their personal autonomy. The data protection authorities recently ruled on the application of wearables by employers for gathering personal information,[33] but there is still no ruling on whether employers may implement wearables for steering behaviour.

3.4 Socio-cultural world

3.4.1 Augmented reality & Virtual reality

The fields of augmented reality (AR) and virtual reality (VR) are greatly expanding. In AR, the real world is mixed with virtual information, animation or objects. In fact an additional digital layer of information is added to our reality, for example via smart glasses such as Google Glass. With VR, the interaction takes place in a completely virtual, three-dimensional, interactive and computer-generated environment, in which users have an artificial experience. The launch in 2012 of the Oculus Rift VR glasses, which provide this possibility, focused a great deal of attention on virtual reality. In 2014 the company was bought for two million dollars by Facebook, which had great plans for virtual reality. CEO Mark Zuckerberg stated, "After games, we are going to make Oculus into a platform for all kinds of other experiences. Imagine that you are sitting on the touch line during a match, studying in a classroom with students and teachers from all over the world, or having a personal consultation with a doctor – just by putting on glasses at home."[34] In the future, virtual reality could play an important role in our social lives. It will vastly expand the social media opportunities: people will be able to spend not only time with friends online but also share all kinds of experiences and adventures.

Privacy: Little Brother (AR) and misuse of virtual avatars (VR)

A hotly debated development in augmented reality is Google Glass. Launched in 2013, this portable computer designed in the shape of a pair of glasses, projects information onto a small display in

[33] autoriteitpersoonsgegevens.nl/nl/nieuws/ap-verwerking-gezondheidsgegevens-wearables-door-werkgevers-mag-niet

[34] nu.nl/internet/3735946/waarom-heeft-facebook-interesse-in-virtual-reality.html

front of you. In early 2015, Google stopped manufacturing Google Glass as a consumer product for the time being in order to focus on business applications.[35] One of the reasons why the public launch of Google Glass floundered was because of so much public unrest concerning the possibility to film private conversations and social interactions (unsolicited) with the glasses. The development of AR is causing concerns about a so-called 'Little Brother' scenario: instead of a government spying on everyone, citizens and companies are the ones spying on each other continuously. Smart glasses or lenses are ideal for tracking people and spying on them without people being aware of it (Geser 2010). Especially if such AR glasses or lenses are equipped with a face recognition app, the user gets real-time information about the person in front of them. The glasses thus enable the wearer to register all sorts of things without others seeing that registration is taking place. The fact that this is against the law will probably not hinder attackers, because it is almost impossible to trace them.

In addition, the smart glasses or lenses raise yet another issue: who owns the images that the glasses record? In other words: does the wearer of the smart glasses or lenses have exclusive rights to his/her own observations (Brinkman 2014; Wolf, Grodzinsky & Miller 2015)? Google applied and obtained a patent for the technology that enables the company, by following eye movements, to see what the person wearing Google Glass is looking at.[36] In this way the company not only has at its disposal the image that the wearer of glasses sees, but also obtains information on precisely when and what the wearer is looking at. Other companies that record images can make very good use of this data for profiling and thus incorporating it in their business model.

The issue with privacy in virtual reality concerns the new ways of tracking people's behaviour in virtual spaces. Games manufacturers like Knack[37] demonstrate, that from the way someone plays a game in the virtual world, we can learn a great deal about their personality, how they interact with others and how they solve problems (Peck 2013). The more that social interaction shifts to social networks in VR – Facebook's aim – the greater the impact on privacy. Not only will the control over personal information come under pressure, also the ability to determine who is and who is not part of an interaction is more difficult in a virtual space. In addition, continuous monitoring can lead to social conformism, reduced authenticity and self-censorship (O'Brolchain 2016). Finally, another issue is how we should deal with people's images. As realistic avatars can be made in VR – for example of famous people – this raises the issue of how they maintain control of their own image. How can we prevent an avatar from being applied in VR for undesirable activities in a new virtual form of identity misuse?

Safety: psychological damage in virtual worlds (VR)

The aforementioned misuse of images in virtual worlds makes us question what these actions in the virtual world signify. German philosophers Madary and Metzinger (2016) made an initial attempt to draw up a code of conduct for investigating and using VR technologies. They focussed on the risks of VR technologies that give users the feeling they are in a different body to their own and

[35] theguardian.com/technology/2015/jul/31/google-glass-wearable-computer-businesses

[36] patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=36&p=1&f=G&l=50&d=PTXT&S1=%2820130813.PD.+AND+Google.ASNM.%29&OS=ISD/20130813+AND+AN/Google&RS=%28ISD/20130813+AND+AN/Google%29

[37] Knack produces so called *assessment games*, computer games designed to test people's performance in a work situation.

particularly in situations where users interact with other virtual or real people. In these situations, unethical behaviour occurs which has already led to controversy with computer games (Seddon 2012). A well-known example is that someone reported that her avatar was apparently indecently assaulted in the computer game Second Life. According to Madary and Metzinger (2016), the emotional involvement within a virtual environment in which we are *actually embodied* is much greater. That means that the psychological damage that someone incurs as a result of an indecent assault in virtual reality, will probably be much greater than previous cases in the game Second Life. It is expected that in the near future, people will visit each other more often in virtual environments and that social networks such as Facebook will also support these possibilities. Successful implementation depends to a great extent on how people will behave in virtual spaces. An ethical code of conduct or certain regulation of behaviour in these virtual spaces is therefore desirable.

Not much research has been carried out on the impact of the emotional involvement in VR and whether experiences in VR have a knock-on effect in the real world (Kizza 2013). The initial experiences with forms of therapy offered in VR – for example to overcome a phobia or to practice awkward social situations like a job interview – show that VR can make a positive contribution to treating fears and disorders.[38] Conversely, we would therefore also expect emotional damage in the virtual world to have an impact in the real world. Madary and Metzinger (2016) support the need to first investigate these issues, so that introducing such VR technologies in the market is done in an ethically responsible manner.

Human dignity: desocialization and alienation (VR)

VR technology defies the usual distinction between virtual and real worlds. This arouses the fear that at a certain moment, people can no longer distinguish 'real' from 'fake'. Melson et al. (2009) fear that the massive use of these technologies will replace our interaction with nature. As a result, we will also miss the healing and creative power of nature. Louv (2005) speaks of the *nature deficit disorder*. Madary and Metzinger (2016) even voice the danger that frequent VR users will regard the real world and their body as unreal, and that their sense of reality shifts exclusively to the virtual environment. They end up neglecting their actual physical and social environment.

As far as shifting social contacts to the virtual world is concerned, Turkle (2011) is afraid that people will lose their social competencies – like dealing with rejection and settling arguments – if we have predominantly virtual contacts in the future.[39] Turkle's fear for this loss is based on her lengthy research into the influence of social media and mobile phones on communication between young people. Turkle argues that the younger generation is much less empathetic than its predecessors were, because intimacy can be avoided and therefore relationships through social media or virtual reality are less binding. Dotson (2014) even envisages a future in which we have contact with virtual people. In his opinion, this will contribute to an undesirable shift in the collective view of 'authentic sociality'. A small group of Japanese men, nicknamed Otaku, already indicated that they prefer a virtual girlfriend to a real relationship: "With real girlfriends you have to consider marriage. So I think twice about going out with a 3D woman" (Rani 2013). Another risk, according to O'Brolcháin et al.

[38] mmi.tudelft.nl/vret/index.php/Virtual_Reality_and_Phobias

[39] See also Sullins (2012).

(2016), is that VR can be addictive, just as the virtual world has produced other addictions. Gambling and pornography are constantly available through the internet, thus allowing for new online forms of addiction. In short: a spotlight on the impact of social media and virtual reality on our social skills is not just a long term issue, but is needed now.

3.4.2 Digital platforms

Digital platforms enable smart and efficient transactions. Uber and Airbnb are the most visible examples of this. There are plenty of other initiatives particularly in relation to the sharing economy: “the phenomenon that consumers let each other have their unused consumer goods, perhaps for a fee” (Meelen & Frenken 2014). Examples are Marktplaats, Peerby ('Borrow stuff easily and quickly from your neighbours'),[40] ParkFlyRent (‘Free parking at the airport and hire your car fully insured’)[41] and Thuisafgehaald (‘Share meals with your neighbours’).[42] These digital platforms have many advantages, such as ease of use, efficiency and possible sustainability, considering that products acquired via the sharing economy are probably used more often and can therefore be used more efficiently. There are, however, a number of ethical-social concerns that require serious attention.

Privacy: insight in all platform interactions

The issue of privacy also applies to digital platforms. The platform administrator can track all the transactions and interactions that take place within the platform and many of these transactions contain sensitive information. Platforms can easily track their users with simple tools. In particular the way Uber (employees) dealt with the privacy not only of their drivers but also of their customers, caused quite a stir (Rogers 2015). It was reported that Uber used their so-called ‘God View’ real-time tracking system on customers as well as drivers. An Uber employee’s blog post, which incidentally has been removed, bragged that, based on the data they collect, Uber can assess which of their customers has had a one-night-stand. They can draw this conclusion when two different customers are dropped in the evening at an address where neither of them lives, and are picked up in the morning and then each taken to their own address.[43] In addition, it turned out that Uber had not reported a data leak, which meant fifty thousand Uber drivers’ personal information was online for months. After reaching a twenty thousand dollar settlement with the department of justice in New York, Uber tightened up their privacy policy. ‘God View' has since been anonymized and the number of employees that can access drivers’ personal information has been reduced. In addition, the location data for the Uber drivers and customers is encrypted.[44] This data can still, however, be viewed with a password known to Uber. Strict surveillance of privacy guidelines for platforms that have a tendency to evade regulations, seems badly needed. In this way, it can be clarified what data is collected, how it is collected and used, and whether it is resold (Scholz 2016b).

[40] peerby.com/nl

[41] parkflyrent.nl

[42] thuisafgehaald.nl

[43] whosdrivingyou.org/blog/ubers-deleted-rides-of-glory-blog-post

[44] buzzfeed.com/johanabhuiyan/uber-settles-godview#.yvb4dKlNR

Control: transparency of steering algorithms

Platforms use algorithms to make certain choices and decisions. Algorithms used to be deterministic – the programmer determined beforehand an action for every situation – and it was possible for someone to figure out how the algorithm came to a decision. Through systems like artificial intelligence, algorithms do not follow a predetermined set of rules but make use of self-learning statistical techniques. As a result, the decisions that an algorithm makes are almost unfathomable for humans (Scholz 2016a). To prevent manipulation, it is therefore crucial that we understand why such algorithms make certain choices. Research by psychologist Robert Epstein showed that search results can greatly influence voters' preferences by changing the order of the results in a search engine, such as Google. According to Epstein, this represents a serious threat to democracy.[45] But algorithms are used in many more areas. For example, the way Uber deals with transport supply and demand is also determined by algorithms. The emergence of the block chain outlines a future of fully automated and decentralized organizations that can be captured in code (Wright & De Filippi 2015). An organization such as an insurer, on the basis of certain rules laid down in software, would be able to collect automated money and pay it out when a customer fulfils certain conditions, without another human being involved in that decision process. Expanding automation raises the question of how to control and monitor such systems.

On several occasions, transactions between Uber and their customers have already led to misunderstandings because customers were not aware of the algorithm Uber used. Once the hostage drama in Sydney in December 2014 concluded, many people tried in an Uber-taxi way to get away from the crime scene. The Uber algorithm detected the surge in demand and consequently calculated four times the normal fare.[46] On social media, Uber was accused of taking advantage of the hostage situation. Uber apologized in a blog post: “Surge pricing is algorithmic and kicks in automatically when demand outstrips the supply of cars for rides that are on the road.” When algorithms do not take account of unforeseen situations, this can have undesirable consequences.

Justice: exploitation and exclusion

Platforms ensure that users have a dual role: as producers and as consumers. In this context, they are called *prosumers*. The power of platforms is that they bring supply and demand together in an efficient way, and via smart assessment mechanisms, they create the confidence that enables transactions such as renting out an apartment to an unknown person. To be able to respond efficiently to the changing demand, platforms often have a flexible team of providers who are available on demand. For this reason we refer to an *on-demand economy*. The fact that providers offer their services on call and are not employed on a permanent basis can put pressure on traditional mechanisms of employee protection, with the lurking risk of exploitation. We see that Uber drivers' working days are too long and they have little input if the company decides to adjust the fare rates (Rogers 2015).

At the same time, platforms can decide unilaterally to deny a user access to the platform. For users who depend on access to the platform for their income, this can have far-reaching consequences.

[45] politico.com/magazine/story/2015/08/how-google-could-rig-the-2016-election-121548

[46] thestar.com/news/world/2014/12/15/uber_backtracks_on_price_hikes_during_sydney_drama

Current case histories moreover show that platforms have no qualms about excluding certain users. Uber drivers may not have a rating lower than 4.6 stars (4.8 stars is average). Otherwise they can be removed from the service. Rogers (2015) describes how the continuous review system means that providers must always be friendly and cheerful. In addition to their physical work, they are expected to perform certain ‘emotional labour’. Regular taxi drivers are free to sit behind the wheel with a grumpy face, whereas for Uber drivers, that could mean losing their source of income.

Balance of power: unfair competition and monopolization

According to Scholz (2016b), certain platforms’ success is not only due to the technological possibilities, but is to do with the companies concerned applying ‘illegality as a method’. This leads to unfair competition between platforms and regular companies, because platforms do not (have to) stick to the rules or permits that apply to regular companies. Airbnb enables individuals to let rooms without a licence, and do not have to fulfil the same safety and tax liability requirements as regular hotels. UberPop drivers do not have to keep to the driving and rest periods, nor comply with the same safety regulations as taxis, and they do not need to charge VAT. On the other hand, the average UberPop driver earns less than the minimum wage and most drivers see this as a part-time job.[47] Although UberPoP was forbidden to operate in the Netherlands in December 2014, Uber continued offering the service for nearly a year, and even paid the fines for the illegally operating UberPop drivers.[48] In November 2015, Uber finally stopped offering the UberPoP taxi service, because, as the company put it: “the service is hindering constructive dialogue on the modernization of existing rules and regulations.”[49]

Frenken et al. (2015) think that a tolerance policy is initially logical in order to give experiments space and to assess the effects. However, the authors advocate clear legislation as platforms like Airbnb and Uber are growing so quickly that they have a disruptive and unexpected impact on existing sectors and on society as a whole. Such platforms can be concentrations of power, with monopolies consequently yielding high profit margins. These monopolies can exist because the platforms typically benefit from network effects as we have seen with internet companies like Google (internet searching), Facebook (social networking) and WhatsApp (mobile messaging). Whatsapp for example only works if there is a large network of users. Once an app like this becomes the largest, competing with it is almost impossible because of what we call *the winner takes all* (Kreijveld 2014). Kreijveld states that it is relatively easy for platforms to expand their scope by integrating and adding new services (like Uber, that is now working on package delivery[50]), which begs the question whether such platforms are not getting too big. One consequence is that users become dependent on such a platform, because it is a hassle to use a different platform where the network is too small and therefore not interesting. Accumulated data and connections within a platform as well as other services associated with the accumulated profile also make it difficult for a user to move to another service – the so-called *lock-in* effect.

[47] volkskrant.nl/economie/uberpop-chauffeur-haalt-vaak-minimumloon-niet~a3823583

[48] nos.nl/artikel/709243-uber-betaalt-desnoods-boetes

[49] nrc.nl/nieuws/2015/11/18/uber-stopt-met-uberpop-in-nederland

[50] rush.uber.com/how-it-works

3.5 Digital world

As discussed in Chapter 2, the digitization of our material, biological and socio-cultural world leads to an ever-expanding digital world of data. In that digital world, the data which is processed and analysed forms the basis for people as well as automated systems to make decisions that subsequently have an impact on the physical world. Developments in the field of big data, smart algorithms and artificial intelligence (AI) are indispensable elements of the technologies discussed above. These developments then play a role with IoT devices that send information to the cloud (big data) and are at the same time steered by data and algorithms from the cloud to perform a specific action in the physical world. Because the issues concerning big data, algorithms and AI overlap, we will discuss these developments here altogether as part of the digital world.

Privacy: regulating big data

Thanks to digitization, there is now a lively trade in information. 'Big data' is sometimes referred to as 'new gold'. Data is valuable because it enables better decisions, for example about which consumers should be shown which ad or which people should be investigated as potential fraudsters. We have already discussed various issues regarding privacy, and big data presents a specific challenge in this respect due to the re-use and potential combinations of different data sources. In addition, a significant characteristic of big data is that it is not clear beforehand which insights can be captured from the data. Researchers showed that on the basis of Facebook ‘likes’, it was possible to identify someone's sexual preference, religious and political orientation, personal characteristics and use of addictive substances (Kosinsky et al. 2012). Authorities are also looking into big data’s potential. One example is the Dutch anti-fraud system called System Risk Indication (SyRI) which encrypts, combines and analyses data about fines, debts, benefits, education and integration in a secure digital environment in order to search more effectively for people abusing benefits or surcharges. SyRI has been criticised by both the Data Protection Authority and the Senate because of the impact on privacy (WRR 2016). In response to this criticism, some points in the system have been adapted but not all recommendations have been implemented.

Combining and reusing big data seems to be at odds with the principle of purpose limitation, which is one of the pillars of data protection legislation (Kool et al. 2015). Various authors argue that legislation and supervision in the big data era should focus more on companies’ responsibilities (accountability) and how data is used (Podesta et al. 2014; Cate et al. 2014). But opponents say that the principle of purpose limitation is an important mechanism to counteract unbridled collection and *data obesitas* (Hildebrandt 2015). At European level, there has been an attempt to deal with big data issues by modifying the legislation. The new European Data Protection Regulation (EU 2016/679), building on the principles of the data protection directive (95/46/EC), adds a number of new obligations and responsibilities for data processors, and strengthens individual rights. This regulation shows that the topic of data is high on the agenda. However, there is also an ongoing debate about whether these legislative adjustments are adequate to deal with the inherent challenges of digitization. Particularly with regard to profiling, the legal framework only offers partial protection (Kool et al. 2015).

Autonomy: filtering and freedom of expression

When data collection moves to the next phase of the cybernetic loop, analysis and application, new issues emerge. Online platforms play an increasingly greater role in determining what information and what news people see. A well-known example is how different persons' Google search results vary because of a personalization algorithm that looks at things such as previous searches (Pariser 2011). This raises questions about the steering role of major platforms and also about freedom of expression. A recent example is when Facebook removed the iconic and harrowing 1972 World Press Photo of a girl fleeing from a napalm attack (the 'napalm girl' as the picture would later be called). Following widespread criticism, Facebook later reversed its censorship decision and reinstated the photo.[51] Other platforms like Google and Twitter (not forgetting Facebook), have been criticised for facilitating the spreading of 'fake news'.[52] This has led to a debate on the role and responsibilities of platforms in relation to freedom of speech and filtering information. In the aftermath of the 2016 US presidential elections, this debate triggered a great deal of controversy. The platforms are examining what action they can take against fake news.[53]

Control: insight in algorithms and AI

Software and automated systems are playing an increasingly important role in analysing and making decisions based on data. This trend is expected to continue. Algorithms are already playing their part in controlling personal online information provision on social networks, determining credit worthiness, tracking down fraudsters and terrorist suspects, and trading on the stock market (Pasquale 2015). IBM is experimenting with its supercomputer Watson to support doctors with medical diagnostics. And case-law is looking into how automated systems can help with the analysis of mountains of legal case histories and providing advice.[54]

In recent years, the discussions on monitoring the underlying algorithms in automated systems have come from different angles (Zarsky 2013, Pasquale 2015, Kool et al. 2016, WRR 2016). The German Government recently released a position paper stating that online platforms – such as Google and Facebook – should provide more information about how their algorithms work, for example when filtering news or search results.[55] As the complexity of the algorithms and the speed at which computers make decisions are very high, it is difficult to understand how a particular decision has been reached, and how to check errors and correct them if necessary. For the purposes of applying automated analysis systems in case law or in the medical world, such control is indispensable. How do you allocate accountability for a decision made by a computer? Can the advice that a judge or prosecutor receives depend on the supplier from whom the software has been purchased? To enable insight and control, IBM is working on a system for Watson called Watson Paths. This should make it possible for the computer to explain how a certain decision has been reached for instance in the field of medical diagnostic.[56]

[51] http://www.volkskrant.nl/buitenland/facebook-maakt-verwijdering-napalmmeisje-na-kritiek-ongedaan~a4373624/

[52] http://www.rtlnieuws.nl/technieuws/nepnieuws-verspreid-door-aanpassing-zoekalgoritme-google, http://www.reuters.com/article/us-twitter-facebook-commentary-idUSKBN13W1WO

[53] http://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html?_r=1

[54] theatlantic.com/sponsored/ibm-transformation-of-business/watson-takes-the-stand/283

[55] bmwi.de/DE/Presse/pressemitteilungen,did=764540

[56] research.ibm.com/cognitive-computing/watson/watsonpaths.shtml#fbid=T7yOxG_VXYP

Diakopoulos (2016) has made an initial attempt to develop a transparency standard for using algorithms, in order to enable their control and supervision. He describes five categories that should be taken into account to ensure transparency:

1. Human involvement. It must be clear who (in the company) controls the algorithm; who has responsibility; and who develops the algorithm.
2. Data. Clarity in the quality, accuracy, uncertainty and completeness of the data, as well as which data is used and which data is combined.
3. The model. It must be clear how data is combined, how certain data is weighed and which assumptions are made.
4. Inferencing. What is the margin of error? For example: how many 'false positives' and 'false negatives' are there, and are these errors due to data input, human involvement or the algorithm?
5. Algorithmic presence. It must be clear at what moment and in which instances an algorithm is applied.

The problem, however, is that companies will claim that they cannot indicate precisely how their algorithm works, because this is part of their strategy. If this information is divulged, competitors can easily adopt the algorithm and offer the associated services (Gillespie 2014).

Developments in the field of artificial intelligence (AI) make the issue of control and supervision even more complex. With self-learning forms of AI systems, it cannot be determined beforehand how they will react to certain situations. Techniques such as Deep Learning (see box 2.5 in Chapter 2), using various layers of neural networks, make it difficult to provide transparency and explain why a system makes a certain decision. That leads to concerns about how to facilitate control and accountability when implementing AI systems (Royakkers & Van Est 2016; Helbing et al. 2015). For the longer term, there are also concerns about how a continually developing AI can still be controlled by humans. People like internet entrepreneur Musk and scientist Hawking have warned about the existential threat of super intelligent AI (Gibbs 2014; Hawking et al. 2014). But also less sophisticated forms of automatic systems can cause problems that are unforeseen and difficult to monitor, particularly when various systems interact in a complex way. A well-known example is the so-called Flash Crash that occurred on 6 May 2010. Due to an unforeseen combination of factors, various automated trading systems (used in *high-frequency trading*) began to sell large amounts of shares in just a few seconds, losing the stock exchange billions, most of which it subsequently managed to recover within a couple of minutes.

Justice: discrimination and unjust exclusion

The automated decisions and assessments that computers make are not flawless. Errors in data or incorrect assumptions in an analysis model can lead to a wrong judgment, resulting in undesirable forms of discrimination and exclusion by the computer system. The previously described lack of insight and transparency of decision systems makes it difficult to estimate when a system has got it wrong. For the individual, it is therefore often difficult to raise objections to the system. An example of this practice is the automated credit rating in the United States (Citron & Pasquale 2014). To determine whether someone is suitable to receive a loan, many lenders use automated systems that calculate a credit score based on data from various sources. The data that is used and the way it is analysed, are not transparent to the public; because transparency could in fact damage the assessor's trade secret. Although the scores have a significant margin of error, the computer analysis is often trusted blindly. As the logic behind a certain decision is not transparent for clients, it is hard to object and to prove where the system is wrong (Citron & Pasquale 2014).

Automated systems harbour a risk of wrong judgements. Several studies warn against wrongful exclusion and discrimination by automated systems (Zarsky 2013, Podesta et al. 2014, Citron & Pasquale 2014). Profiling puts people in certain categories, each of which is handled differently. From a service point of view, this can offer convenience and customization. But if it causes certain (groups of) people to be structurally disadvantaged, that is problematic. It appeared that women jobseekers were shown advertisements for senior posts less frequently than men with a similar profile (Datta 2015). Even if no data about race or religion is used, other strongly correlating variables can still cause discrimination to occur (Hildebrand 2016:202).

A profile that sticks to someone on account of their behavioural history, can affect their options for the future. That can lead to a self-fulfilling prophecy: someone with a good credit score finds it easier to secure a loan and to work on their financial future, whereas someone who poses a higher risk and has to comply with stricter conditions is therefore more likely to land in trouble with repayments (Citron & Pasquale 2014). The Data Protection Authority warns of ‘digital predestination’,[57] the danger that people can no longer ‘escape’ from the digital profile established about them. When profiling and risk assessment methods are also deployed in the security domain, for example to track down potential fraudsters or criminals, the presumption of innocence is put under pressure (WRR 2016). Whereas data is normally only collected *after* people are suspected, big data enables data and risk profiles to be prepared before there is an actual suspicion. According to the WRR (Scientific Council for Government policy), the far-reaching possibilities created by big data and predictive algorithms in the domain of security, must go hand in hand with additional monitoring and protection of fundamental rights.

Balance of power: relations between private and public parties

Big data, smart algorithms and AI ensure a shifting balance of power in the relationships between businesses, governments and citizens. The ‘public space’ on the Internet – consisting of things like social networks – is mostly in private hands. All the interactions that take place in that pseudo-public space are therefore the property of the platforms, and the information generated in this way can be used or resold as required. Also the conditions for interactions taking place, and what statement may or may not be desirable, can be changed by the platform administrator at will. There has been a lot of controversy about Facebook’s decisions to remove certain statements from the platform. Critics argue that the current situation is leading to a form of digital feudalism (Meinrath et al. 2011, Balkan 2013, 2015 Zuboff, Helbing et al. 2015); a situation in which people’s ownership of themselves – their digital representation – is lost.

Governments are also gathering more and more data about citizens. Helbing et al. (2015) describe a future scenario of *big nudging*, with authorities using data to steer citizens’ behaviour. The most striking example is the Chinese Government: for each of its citizens it keeps a *citizen score*, which plays a role in determining whether someone is eligible for a loan, a visa or a job. Government data

[57] autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-meer-privacywaarborgen-noodzakelijk-bij-toepassingen-big-data

collection is causing increasing information asymmetry between citizens and governments, with citizens becoming more transparent and governments becoming less transparent for their citizens.

In the relations between government and industry, companies are increasingly rubbing up against the public sector. One such interesting case occurred when the FBI asked Apple to help hack an iPhone belonging to Syed Rizwan Farook, one of the gunmen involved in the shooting at San Bernardino in December 2015, when 14 people were killed and 22 people seriously injured. The FBI wanted to use brute force to read the phone by entering all the possible combinations of numbers and letters in very quick succession. However, an iPhone erases data after a wrong code is entered ten times. Apple was commissioned to develop software that could bypass this. According to Apple, this will create a dangerous precedent, because if the wrong persons managed to get their hands on the software, they would be able to read every iPhone. Apple feared that, in the long term, the FBI's demand "would undermine the very freedoms and liberty our government is meant to protect".[58]

Ultimately, together with a hacker, the FBI managed to intercept the San Bernardino shooter's iPhone without help from Apple. Nevertheless, this example demonstrates that large corporations like Apple wield positions of power, holding considerable sway in how they allow their infrastructure to be used.

3.6 Conclusion

We described above the societal and ethical issues emerging with the digitization of society. In this overview, we limited ourselves to issues associated with developments in the technology areas mentioned in the previous chapter: robotics, Internet of Things, biometrics, persuasive technology, platforms, augmented and virtual reality, big data, algorithms and Artificial Intelligence. In this concluding section, we will summarize the social and ethical issues that have arisen and discuss the visible trends and developments. We will do this on the basis of the seven overarching themes we defined at the beginning of this chapter. To underline the importance of these issues, we will briefly discuss the connection with important values set out in international treaties and fundamental rights. In addition, we will show how the societal and ethical themes are related to a strong upswing in the collection, analysis and application of data, or in other words, to increasing activity in each of the three phases of the cybernetic loop we introduced in Chapter 2.

3.6.1 Overview of societal and ethical aspects

Table 3.2 below provides for each overarching theme an overview of the societal and ethical issues evoked by various technological developments in digitization. This subsection briefly explains our overview.

Privacy

Privacy is certainly the most prominent issue. And it is clear from our discussion that privacy is about more than just data protection. With the advent of *pervasive* and ubiquitous monitoring – through smart devices, robotics and biometric identification – and techniques such as profiling, we

[58] apple.com/customer-letter

see new issues emerging around privacy. The current regime where users are responsible for checking their data streams via consents, does not seem adequate for a future in which the individual will be surrounded by dozens of smart Internet-of-Things devices, each with their own data streams. Furthermore, digitization is expanding like lightning. Biometric technology enables all kinds of information to be detected from our face and body, sometimes even from a distance, with or without the individual's consent. Reading a mental state of mind from micro-expressions on our face can pose a threat to mental privacy – the ability to keep our thoughts and feelings private.

Table 3.2 Social and ethical issues evoked by digitization

Theme	Issues
Privacy	Data protection, privacy, spatial privacy, mental privacy, surveillance, function creep
Autonomy	Freedom of choice, freedom of expression, manipulation, paternalism
Safety and security	Information security, identity fraud, physical safety
Control technology	Control and transparency of algorithms, responsibility, accountability, unpredictability
Human dignity	Dehumanization, instrumentalization, deskilling, desocialization, unemployment
Equity and equality	Discrimination, exclusion, equal treatment, unfair bias, stigmatization
Balance of power	Unfair competition, exploitation, shifting relations between consumers and businesses, and between government and businesses

Rathenau Instituut

Autonomy

Autonomy is strongly linked to privacy as a condition for the unimpeded development of one's own identity. The emerging challenges in the area of privacy, such as continuous monitoring by IoT devices, are conflicting with the idea of autonomy. To what extent can children's development still be unhindered, if they know that smart Barbie is monitoring their playing behaviour? The issue of autonomy is playing a more significant role as technology filters, fills in or takes over more decisions for people. This development is clearly manifest in all sorts of domains: online platforms that filter information, smart environments that anticipate behaviour, persuasive technology that can exercise influence consciously and at a deliberately low level, and robotics that take over tasks partially or entirely. The issue of autonomy whereby people still have the space and the freedom to choose, is therefore becoming an increasingly important theme.

Security

Digitization gives us the opportunity to set up more secure systems, for example by saving data locally or through encryption, which only keeps information that is strictly necessary. Yet at the same time, digitization is also introducing new vulnerabilities. Cyber security, for years a major theme in digitization, has recently taken on a much greater dimension because of the increasing number of devices and services being connected to the Internet. The impact surpasses the level of data leaks and misuse of data, and is shifting to a new level of hacked cars that can be steered remotely and pacemakers that can be set to deliver fatal shocks. For our physical security, it is therefore increasingly important that the security and operation of digital systems are well safeguarded.

Controlling technology

As more processes in computer systems are being outsourced, the question of how to equip such systems with human controls is becoming all the more acute. We are talking about systems that make a medical diagnosis, advise and support case law, or with autonomous weapon technology that can even make life or death decisions. Insight into how these systems come to a certain decision is crucial in order to be able to justify these decisions, and to signal and prevent errors, for example when a system makes an incorrect diagnosis due to an error in the software or in the data. The combination of the spiralling number of trading systems creates a new layer of complexity, with potential unforeseen effects: the same is true for the individual citizen when the smart house is paralysed by the interactions between various ‘smart’ devices, but also at a social level when the stock market crashes due to autonomously operating algorithms.

Human dignity

Concerning human dignity we see that digitization and automation – in the form of robotics – can play a role in relieving people of ‘inhuman’ work. At the same time, there are also concerns that AI and robotics can and will take over more and more work from people, and lead to unemployment. But there are also more subtle effects when technology takes over tasks: the decline in moral skills (deskilling) as persuasive systems steer us in the direction of morally correct behaviour, or desocialization because people find virtual interactions more pleasant and stimulating than awkward social interactions in the physical world.

Equity and inequality

Digitization means that people and their behaviour can be analysed in all sort of ways. In doing so, the computer is not an unbiased evaluator, since it is always programmed by people with certain goals, assumptions and ideas. With the increasing number of analyses, concerns are also mounting about discrimination, equal treatment and wrongful exclusion of people. Based on their profile, people can be denied access to a loan, have to pay a higher price for the same product, or be branded as a suspect. Errors in analyses and profiling can have serious consequences for individuals and that is not desirable. It is also very undesirable that profiling systematically jeopardises certain groups of people. An additional problem is that with automated analyses, there is very little transparency on how these analyses came about. In instances of an incorrect judgement, it is also difficult for an individual to rectify such a system error. Kafkaesque scenarios are lurking.

Balance of power

The balance of power is a significant societal issue. The relationship between consumers and businesses is changing because products are offered more as a service in the Internet of Things. We see that software is playing an increasingly important role in everyday products and services. Whoever controls that software determines in the programming how it can and cannot be used, what American law professor Lessig calls ‘Code is Law' (2006). Several major internet companies’ position of power raises discussions about the dependence and position of administrator – of information or services – that these companies acquire. But digitization also changes the relationship between citizens and authorities, as we see in public systems where governments are doing more to anticipate citizens' reactions, for example by means of preventive policing (*predictive policing*) or the above mentioned SyRI system. The pendulum of power is swinging as citizens become more transparent while governments become increasingly vague.

3.6.2 Collect and analyse and apply

Since the 1970s, the debate on digitization has centred round the societal and ethical issues associated with the large-scale collection of data (Van Est et al. 2016). Privacy has always been a concern, the traditional focus being regulation and monitoring. Think for example of the Personal Data Protection Act, the Mandatory notification for data breaches and the European Data Protection Regulation. Data collection will remain an important topic as the emergence of IoT, robotics and biometrics has taken monitoring to a whole new level.

Not only the collection, but also the analysis and application of data are already evoking many issues. Talking about profiling brings us to the domain of analysis. Many of the issues here are associated with justice and discrimination as well as the lack of transparency in the analyses. The need to control and supervise algorithms is becoming increasingly important as they are applied in more and more domains (on the roads, health care, justice, e-commerce) to support or even take over the decision-making.

This step takes us to the third stage of the cybernetic loop, the application. Here we are at the level of interventions, confronting us with issues like individual autonomy and the controllability of technology. To what extent are choices filtered for us and nudged by software, what tasks do we want to outsource to robotics, what human work is still remaining and what is the effect on our human dignity? Besides collecting data, the new challenges of digitization over the coming years lie precisely in the analysis and application of digital data.

Looking at all the issues described here, we can clearly see that it would not be wise to underestimate the impact of digitization. The need to focus on the effects of digitization is underlined by the fact that the central ethical themes relate to important values set down in international treaties and the Dutch Constitution. We can see issues such as privacy and justice reflected in the right to respect for private life, the right to equal treatment and the right to a fair trial. Human dignity and safety are not part of the Dutch Constitution but are mentioned in international treaties such as the Charter of Fundamental Rights of the European Union (EU Charter) and the Universal Declaration of Human Rights (UDHR). Values such as autonomy, equal power relationships and control over technology are not explicitly named in the treaties but can be seen as part of or following from these fundamental and human rights. Digitization touches so important public values. This is what makes the governance of these ethical and societal issues such an important challenge.

4 Governance from a historical perspective

4.1 Introduction

In Western societies, science and technology are seen as important sources of economic and societal progress, but often lead to public and political debates on for example physical risks or ethical boundaries. Typical discussions are research with human embryos or genetic modification of food and animals. These topics have often caused governments to consider whether ethical and societal issues associated with the new technological possibilities can be dealt with in a systematic way. The question that always arises is to what extent the existing institutional embedding is adequate or needs strengthening.

In this chapter we aim to gain general insight in the *governance ecosystem* of social and ethical issues that arise through technology. Box 4.1 explains the term public governance. We focus specifically on the *structure and functioning* of the governance ecosystem, and the role committees play in these. We do this by presenting a historical overview over the past half century and from a political-administrative and societal perspective, of how we have dealt with the social and ethical issues relating to four technological developments: ICT, biotechnology, research on human subjects and animal experiments.[59] These four themes do not cover all the scientific and technological developments that evoke societal and ethical issues. However the description is broad enough to establish a general conceptual framework of a governance ecosystem of ethical and societal issues connected with technological developments. The historical overview also shows what kind of committees have been set up earlier in the four areas, what type of committees they were and what part they played in this ecosystem. In the following chapter we apply this conceptual framework to see how the current governance ecosystem for dealing with ethical and societal issues related to digitization is currently taking shape.

We describe the technological areas chronologically, from decade to decade. To make sure the reader is aware of the coherence between the many events over the years, we will regularly refer to things that happened a decade earlier or later.

[59] Since 1986, Rathenau Instituut has been part of the governance ecoysteem dealing with societal and ethical issues in technology. The Institute's role is to stimulate the forming of public and political opinion on science and technology. That is why we mention the Rathenau Instituut's activities in our analysis of the four technology areas in the ecosystem.

Box 4.1 What does public governance mean

The ambiguous concept of governance is described in extensive literature. In Appendix B, we present various insights and concepts from that literature that are relevant to our approach to this study. We briefly summarize some of these concepts here.

Various governance concepts refer to certain types of interaction between government and civil society actors. Forms of governance include *multi-stakeholder governance* or *network governance, multi-level governance* and *deliberative governance* (Hajer et al. 2004). With *network governance,* stakeholders in business, society and the government develop a joint approach to an issue that concerns them all but is too complex to tackle effectively without collaboration. In *network governance* we find more horizontal agreement between stakeholders, and joint decisions are laid down in ‘agreements' (NSOB & PBL 2014, p. 21). Alongside interaction between public and private actors, many issues require consultation with various levels of administration such as at European, national, regional and local level. This is called *multi-level governance*. When it specifically concerns the interaction between government parties, citizens and social groups, the term *deliberative governance* is often used.

The Dutch government has a long experience of working with various stakeholders in society. The need for governance has grown in recent decades because of digitization, privatization and internationalization (Hajer et al. 2004). Governance can also be a response to public resistance, lack of support, institutional distrust or the complexity of issues.

Governance thus not only revolves around the government’s actions. The entire system of governance arrangements in society must be considered in order to bring public issues to the table and find solutions. This requires a diverse set of institutions as well as administrative and social processes. Together this set forms a so-called governance ecosystem: the entire set of governance arrangements surrounding a particular public problem. Hoppe (2004) refers to it as *meta-governance* because it is about the governance of problems, or rather the establishment of a governance ecosystem that can identify and address collective problems.

For our approach, it is important to distinguish between governance and meta-governance. Governance addresses questions such as: What public problems have been identified? Which interests or values are articulated better than others? How do citizens and politicians discuss these problems? How do problems, political or otherwise, get onto the agenda? Which parties have been involved in the debate and the formation of policy? What solutions have been proposed and institutionalized?

Meta-governance looks at questions such as: what institutions exist to discuss public problems and raise these as political issues? In what ways is a collective standpoint agreed between public and private actors and between governments, citizens and civil society organizations? How are public values institutionally safeguarded? Which institutions have been created over the years to do that? What constitutes the governance ecosystem for a particular issue?

4.2 The 1970s: social and ethical concerns about science and technology

Biotechnology: recombinant DNA and the DNA Commission

The 1970s saw mounting criticism of science and technology on various fronts. The 1975 Asilomar Conference on the discovery of recombinant DNA technology led to ethical discussions in small circles. In response, the Dutch Government set up a commission ('Brede DNA Commissie' 1981-1983) to consider the possible applications as well as the social and ethical aspects of recombinant DNA research. We will see that bio or genetic engineering continues to concern us to this day.

Animal tests: Experiments on Animals Act

In the course of the twentieth century, the use of animals in the biomedical sciences increased enormously (Swart et al. 2004). The number of animals involved in experiments grew from fewer than five thousand in 1908 to approximately one and a half million in 1978. To reverse this trend, legislation on animal trials had been introduced the year before (WoD, *Wet op de dierenproeven*). The principle of this Act was the protection of animals. It stipulated that establishments conducting experiments with animals had to have a licence. To be eligible for a licence, the establishment had to comply with various obligations: register animal tests and laboratory animals, formulate expertise requirements for researchers, bio-technicians and animal carers, and appoint an expert to supervise the welfare of laboratory animals (Swart et al. 2004). It took two decades to develop this system. As part of that process, a number of licensees voluntarily established an internal Committee for Animal Experiments (DEC) in the early 1980s.[60]

ICT: privacy as new fundamental right, the Act on Registration of Personal Data and the Rathenau Committee

The 1971 census in the Netherlands evoked a heated public debate on privacy. That led to a State Commission (Cals/Donner 1967-1971) and finally a constitutional amendment in 1983, which added privacy as a fundamental right (article 10). This amendment paved the way for the 1988 Act on Registering Personal Data.[61] The Registration Board was set up to supervise the implementation of this Act.[62]

In the late 1970s, the rise in micro-electronics (including personal computers) caused wide social concerns regarding employment. In 1978 and 1979, a committee headed by Professor G.W.

[60] With the animal testing resolutions, the Experiments on Animals Act (WoD) became fully effective in the 1980s. This Act also made provisions for a permanent advisory committee on animal experiments, which was tasked with advising the government in this area and promoting public awareness.

[61] Its successor, the personal data protection Act (Wbp), has been in force since 2001. The Wbp is the Dutch elaboration of the European data protection directive (95/46/EC).

[62] The Dutch data protection authority (CBP, since 2001) and Personal Data Authority (AP, since 2016). AP represents the fundamental right to protection of personal data, it monitors compliance with regulations for protecting personal data and advises on new regulations.

Rathenau investigated the social impact of micro-electronics. One of the committee's recommendations was the need to study the social significance of new technologies systematically, using what they called technology assessment. Thus the Rathenau Committee laid the basis for founding the Netherlands Organisation for Technology Assessment (NOTA, now the Rathenau Instituut), which we will discuss in the next section.

4.3 The 1980s: anchor issues in science and technology

The above discussions on specific technologies in the 1980s also directed the political-administrative focus to the question of how societal and ethical issues in general could be systematically anchored in science and technology policy. The government under prime minister Lubbers (1982-1986) set out in its agreement that the social and ethical consequences of technological innovations had to be made more visible (Parliamentary Papers II 1982-1983, 17555, no. 7, p. 87). This led in 1984 to the Bill 'Integration of Science and Technology in Society' (IWTS Bill; Parliamentary Papers II 1983-1984, 18424, no. 2) the main objectives being structurally embedding Technology Assessment (TA) in the policy and more focus on providing information and raising awareness of science and technology. As a result, the organization NOTA was founded in 1986 (renamed Rathenau Instituut in 1994). NOTA was given the task of investigating the social and ethical aspects of science and technology, in order to inform politics, but also to stimulate the public debate on new developments. The PWT (Dutch Foundation for Public Information on Science and Technology) was set up in 1986.[63]

Animal Experiments Committees

Following the 1977 Experiments on Animals Act (Wod), animal experiment committees (DECs) were established in the early 1980s as a form of self-regulation. During that decade, there was a growing need for uniform conditions in an independent ethical decision-making process (Van Boxsel 1991). In 1985, the Advisory Committee on Animal Experiments advised on the legal embedding of DECs (Swart et al. 2004). The Experiments on Animals Act was adapted in 1996 in accordance with EU regulations, and thus the DEC committees were formalized. These committees assess among other things whether the suffering of the test animals outweighs the purpose of the test. While the 1977 Act centred on the protection of the animals, in 1996 the general premise of the Act became the animals' intrinsic value (Swart et al. 2004). A DEC committee's advice is binding. In the case of a negative judgement, the licence holder can submit the research proposal to the Central Committee for Animal Testing (CCD) for a second opinion. If it also delivers a negative judgement, the animal experiment may not be conducted.[64]

[63] In January 1997, the PWT Foundation merged with the Foundation 'Wetenschapsweek en Techniek' [*Science Week and Technique*] to form the 'Weten' Foundation, which was discontinued in January 2005.

[64] At the end of 2014, the European directive (2010/63/EU), which deals with animal testing in scientific research, became part of Dutch law. Consequently, the organizational model for assessing animal testing has changed. Two organizations play a role in this: the CCD Committee and the National Advisory Committee on animal testing policy (NCad). CCD is the central organ that is exclusively authorized to grant project licences for animal experiments. NCad has been set up to protect animals used for scientific purposes and for education. NCad wants to minimize the use of test animals both nationally and internationally by replacing animal experiments with animal-free methods of research, and to reduce the number of test animals in research as well as their discomfort.

Medical-ethical assessment committees

Following the American example, in the early 1970s several university hospital in the Netherlands set up medical-ethical committees (METCs) on their own initiative. In the second half of the 1980s, the number of institutions with a METC committee increased dramatically, but there was a lack of uniform criteria for ethical assessment (Van Boxsel 1991). Reactions from the field showed the need for an independent body 'at a distance' that could give a second opinion on assessing medical-scientific research proposals relating to specific ethical, legal and social issues (KEMO 2004). In the late 1980s, the draft of the medical scientific research on humans Act (Wmo) already included such a committee. By 1989, the Key Research Ethics Committee (KEMO) was established. Ten years and 27 opinions later, KEMO was actually succeeded by the Central Committee on research involving human subjects (CCMO). The CCMO carries out various assessment tasks under the Wmo Act (1998) and the Embryo Act (2002). The CCMO also oversees the activities of decentralized, recognized METCs.

4.4 The 1990s: socialization and regulation of bio-ethics

Socialization of genetic engineering

In the 1990s, numerous debates flared up in the Netherlands and internationally around the application of biotechnology. Recombinant DNA technology had been discussed two decades earlier in smaller circles; however, by the 1990s, concrete applications of genetic engineering brought biotechnology to the attention of a wider public.[65] Along with the genetic modification of micro-organisms, genetic engineering for plants, animals and people became a widely discussed topic. A well-known milestone that attracted a great deal of publicity in 1990 was the birth of the Dutch bull Herman, the first transgenic bull in the world. In this decade, biotechnology shifted from being something that happened in the lab to something that touches society in all sorts of ways.[66]

At the same time, scientific developments in this area had also moved on. Society was becoming more aware of the use of genetically modified test animals, research with human embryos, mapping of the human genome and cloning animals and humans. In the first half of the 1990s, from a human rights and international organizations' perspective, the topic of human genetics (see box 4.2) was coming more under the spotlight. In order to guide these developments in the Netherlands, the (Provisional) Committee for Genetic Modification was established in 1990 and the Provisional Committee on the Ethical Evaluation of Genetic Modification of Animals in 1992 (later called the Committee for Animal Biotechnology).

Genetic Modification and Animal Biotechnology Committees

The Provisional Committee for Genetic Modification (VCOGEM) was established in 1990, followed by the current Committee (COGEM) in 1998. COGEM's tasks are set out in the Environmental Management Act [*Wet Milieubeheer*]. COGEM advises the government on the potential risks of producing and handling genetically modified organisms (GMOs) for people and the environment. At the request of the Minister for Infrastructure & Environment or on its own initiative, COGEM advises

[65] In 1982 the first synthetic human insulin was brought on the market. It was produced with the help of genetically modified E. Coli bacteria, into which recombinant-DNA-technology human DNA was inserted.

[66] Other examples are the first use of genetic engineering for humans in Italy in 1991 and the introduction of the first genetically modified food on the US market in 1994 and two years later in the UK.

the government about ethical-social aspects connected with genetic modification. This is done via alerts.

In 1992, the Minister of Agriculture, Nature Management and Fisheries set up the Provisional Committee for Ethical Evaluation of Genetic Modification of Animals, in the context of the new health and welfare Act for animals (GWWD). This provisional committee was to advise on the admissibility, from an ethical point of view, of research projects in the field of genetic modification of animals.[67] In 1997, by means of the Biotechnology Decree, this provisional committee was formalised in the Committee on Animal Biotechnology (CBD). The CBD advised whether permits could be granted for genetic modification in animals. Each individual permit application underwent an ethical evaluation to determine whether the legal conditions were met. The CBD's secondary goal was to gain insight into which biotechnological treatments of animals used in biomedical research are ethically acceptable.[68]

Box 4.2 International bio-ethical treaties from a human rights perspective

The Council of Europe and Orviedo Treaty

From a human rights points of view, a dominant topic in the first half of the 1990s was the progress in human genetics. By 1991, the Parliamentary Assembly of the Council of Europe (PACE) ordered the preparation of a convention on bioethics. This came to fruition in the 1997 Convention on Human Rights and Biomedicine (Oviedo Convention).[69] Despite the broad scope of the European Convention on Human Rights (ECHR), the Council of Europe considered it necessary to focus on scientific and technological developments; a balance had to be found between progress and human dignity. Article 1 describes the aim of the Treaty: "the parties to this Convention shall protect the dignity and identity of human beings and guarantee everyone, without discrimination, respect for their integrity and other rights and fundamental freedoms with regard to the application of biology and medicine." The Treaty upheld general principles. Additional standards and specific issues had to be settled in additional protocols. The first additional protocol to be drawn up, soon after the news broke about Dolly the sheep in 1998, prohibited the cloning of humans.

UNESCO Universal Declaration on Bioethics and Human Rights

Besides the Council of Europe, also the United Nations Educational, Scientific and Cultural Organization (UNESCO) examined the developments in genetics. In 1993, UNESCO was mandated by its member states to formulate standards and boundaries in the field of bio-ethics (Andorno 2006). After several breakthroughs in the unravelling of the human genome,

[67] This was as a result of the public and ethical debates on the use of biotechnology in animals (stimulated by the birth of the genetically modified bull Herman in 1990).

[68] In 2008 the Senate decided that the evaluation would not lead to new insights and simplified the regulations. Since 2010 an evaluation that complies with the Animal Experiments Act is sufficient. A permit was, however, still required for biotechnological treatments with animals not used for biomedical purposes, such as for food production. Although the CBD remained involved, this committee was dissolved in 2014. (wetten.overheid.nl/BWBR0008392/2005-07-01)

[69] Currently 29 member states of the Council of Europe have ratified the Oviedo Treaty. Six states, including the Netherlands, have signed but not yet ratified the treaty. You can find the Dutch text at: coe.int/t/dg3/healthbioethic/texts_and_documents/ETS164Dutch.pdf

the Universal Declaration on the Human Genome and Human Rights was adopted by the General Assembly of UNESCO in 1997. The International Declaration on Human Genetic Data followed in 2003. In addition, there was a need for a legal instrument with a more general bio-ethical connation and thus a greater scope than human genetics. That need led in 2005 to the UNESCO Universal Declaration on Bioethics and Human Rights. According to UNESCO (2005) it was appropriate and desirable “to set universal standards in the field of bioethics with due regard for human dignity and human rights and freedoms, in the spirit of cultural pluralism inherent in bioethics”. Two years later, this statement was unanimously adopted by the UNESCO member states.

Need to legally anchor ethics committees

As described above, in the 1980s the number of local medical-ethics committees (METCs) and ethics committees for animal experiments (DECs) had increased considerably. By 1990, the Dutch Senate wanted more clarity about ethics committees: how many were there, how did they operate and did they collaborate with each other? The politicians wondered if ethical and societal aspects were being adequately taken into account through all these committees. Via the Lada-Baird motion, the Senate asked the former Ministry of Education and Science (nowadays the Ministry of Education, Culture and Science) to develop a framework for ethical discussions and their evaluation (Papers II 1989-1990, 21319, no. 6). This led in 1991 to the bill ‘Framework for discussions on ethical aspects of scientific research' (Papers II 1990-1991, 21319, no. 12) (see box 4.3).

Box 4.3 Bill ‘Framework for discussions on ethical aspects of scientific research’

Four ways to create a framework for ethical aspects

Minister Ritzen of Education and Science distinguished four ways to create a framework for the ethical and social aspects of research: identification, articulation, authorized assignation of values, and analysis and underpinning of values (Parliamentary Papers II 1990-1991, 21319, no. 12). The Minister also indicated that the fora where decisions can be made on ethical issues in an authoritative (binding) way, vary from the very formalized (legislator and legislation) to the context-specific (for example, medical-ethical committees that make case-by-case judgments) or the more general (temporary committees, like the aforementioned ‘Brede DNA Committee’).

Identification

Groups in society make it known that they consider certain norms and values are coming under pressure from scientific and technological developments. They articulate their concern and attempt to bring this to the attention of the authorities whom they consider are capable of dealing with such an issue. This is how they indicate that there is a problem.

Articulation
In the second phase of this process, organizations that assess technology like NOTA (later Rathenau Instituut) play a role by mapping these developments and indicating under which discussion points the issues are presented. In this way the problem is articulated.

Value assignation by government and third parties
In the societal and political debates, the groups involved come to an agreement on which forum will have the authority to issue a binding decision on ethical problem areas. Subsequently these decisions are made. The forum and the way it reaches a decision can be very formalized (legislator and legislation), context-specific (medical-ethical committees that make case-by-case decisions) or more general (temporary committees for example on DNA topics). The outcomes of ethical scientific research are fed into these processes.

Analysis and underpinning of values
This is about ethical/philosophical research, in which the underpinning and content of values undergo critical consideration. Especially philosophists, ethicists and theologists work in this area.

Societal debate required on bio-ethical issues
In the 1990s, the government valued the public debate on the ethical issues concerning new technological developments. In 1994, Minister Ritzen established the Science and Ethics Platform at Rathenau Instituut for a trial period of three years. The aim of this platform was to stimulate public debates on the ethical aspects of scientific research. The trial period was extended for a further year and evaluated in 1997. The platform function was thereafter structurally embedded in the Rathenau Instituut.

Starting in 1998, three public debates were held on biotechnology within a timeframe of five years. Borst, the Minister for Public Health at that time asked Rathenau Instituut to organize a public debate on cloning. This was following the commotion that arose when scientists in Scotland successfully cloned Dolly the sheep. A public awareness campaign and debate on xenotransplantation[70] began in 1999, following advice from the Health Council regarding the social and ethical aspects of xenotransplantation, and the government's response (Parliamentary Papers II 1998-1999a, 26335 no.1).[71] The Dutch Institute for Consumers and Biotechnology organized this campaign and the debate (Parliamentary Papers II 1998-1999b, 26335, no. 3). Finally in 2001, the public debate 'Eten en Genen' [Food and Genes] began on the social and ethical issues surrounding biotechnology and food (Terlouw Committee, TK papers 2000-2001b, 27248, no. 3). The purpose of this temporary committee was to expand and exchange information on biotechnology and food with the broadest possible audience, provide opportunities for discussion and opinion-forming and record the outcomes of the public debate.

[70] Xenotransplantation is the process of grafting or transplanting organs between members of different species (usually humans and animals).

[71] The former Minister of Health, Wellbeing and Sport asked the Health Council for this advice in December 1996.

Ascertain the impact of ICT on society

In the second half of the 1990s, the emergence of the Internet coincided with the growing impact of ICT on society. During this period, the second cabinet under Prime Minister Kok (1998-2002) wanted to define its position on the government's role in the information society. For this purpose, the Programme Office Infodrome was set up in 1990. Infodrome was to make an inventory and analysis of the societal impact of the large-scale application of ICT, and subsequently specify the implications of these changes for the government's role. Infodrome's steering group was chaired by Rick van der Ploeg, State Secretary for Education, Culture and Science. In December 2001, Infodrome presented parliament with its final report *Give or take control: a political agenda for the information society*.

In July 1999, the state formed a committee led by Professor Franken 'Fundamental rights in the digital age', following discussions on amendments to the fundamental right to confidential communication. Following a study by Hofman, advocating a perspective independent of technique on 'confidential communication', the government presented a legislative proposal in 1997 to amend the fundamental right to privacy of correspondence (Parliamentary Papers II 1996-1997, 25 443, no. 1/2). The proposal was criticized by various parties and eventually withdrawn (Parliamentary Papers II 1998-1999, 25 443, no. 40). The subsequently formed committee (*Commission Franken*) was tasked with providing recommendations on amending fundamental rights in relation to developments in information technology (Nouwt et al. 2000). The Franken Committee came up with its report in 2000, focusing on the amendment of Article 7 (freedom of expression), Article 10 (respect for privacy) and Article 13 (confidential communication). The idea was to formulate these articles in a technology-neutral and future-proof way. The committee's advice was for the most part adopted by the government (House of Representatives 2000-2001, 27460, no. 1), but encountered sharp criticism from the Council of State in 2004, the year the decision was made to withdraw the proposals (Verhey 2011; Koops 2011).[72]

4.5 The 2000s: research, identify and debate ethics, bio and nano-technology

Need for integral bio-ethical evaluation framework

Once the public debate 'Food and Genes' was completed, next on the agenda was an Integral Policy Paper on Biotechnology in 2002 (Parliamentary papers II, 2000-2001a, 27428, no. 2). This paper was an attempt to find a balance between innovation and its potential negative consequences. Security and social-ethical admissibility were the conditions for applications in biotechnology.

Many political parties felt the need for an integral and ethical evaluation framework for applications in biotechnology, based on the intrinsic values of life, ecological sustainability and biodiversity. Such a framework 'Responsible and careful review' was drawn up in 2003 (Parliamentary Papers II, 2002-2003, 27428, no. 39). In the same year, the Center for Ethics and Health (CEG) was

[72] Partly because of digitization, a state commission (Commissie Thomassen) was appointed once again in 2009 to advise on a possible revision of fundamental rights.

established. The CEG was a partnership between the Health Council and the former Council for Public Health and Care (RVZ), (see box 4.4). The CEG identifies and informs about new developments in the field of ethics, health and policy. The CEG sends annual indicator reports on medical-ethical developments to the Ministry of Health. These reports are the input for the Ethics and Health agenda presented with the State budget every year and discussed in parliament. The CEG is also an information point for ethical issues in the field of public health.

Box 4.4 Health Council and Council for Health and Society

Health Council
The Health Council (founded in 1902) informs the government among other things on ethical topics related to biotechnology. The Health Council is one of the Dutch Government's advisory bodies and its mandate is to advise ministers and parliament on the current state of affairs in the field of public health and health(care) research. In addition, the Health Council has the task to signal key developments, and can therefore give the government unsolicited advice. The Health Council's opinions serve as underpinning for government policy and are compiled on the basis of both technical-scientific as well as ethical-social considerations (Zoeteman & Widdershoven-Heerdink 2007).

Council for Public Health and Society (RVS)
Similar to the Health Council, the Council for Public Health and Society (RVS) is another of the Dutch government's official advisory bodies. Formed in 2015, RVS is the result of a merger between the Social Development Council (RMO) and the Council for Public Health and Care (RVZ). RVS provides strategic advice for implementing policies on 'all aspects that can affect the health and functioning of citizens in society' (RVS 2016). Its task is also to identify developments that are significant for public health policy from an ethical perspective.

Some members of parliament, however, still had their doubts about whether the existing network of ethics committees sufficiently addressed new and wider ethical issues than the review committees via the legal and established procedures. Politicians were also worried that the ethical review had become detached from concerns discussed in the public domain, and that there was not enough room to manoeuver in politics for commenting and deciding on new ethical issues. Thus in 2004, the government agreed to conduct a biennial trend analysis that could indicate broader issues and where possible lead to amending or updating existing review frameworks (Parliamentary Papers II 2003-2004, 27428, no. 45). This was meant to create a certain dynamic between institutes that contributed to the trend analysis and society and to enable the parliament to translate this into political action" (Parliamentary Papers II 2003-2004, 27428, no. 45). In recent years, the existing advisory bodies ranging from the Committees for Genetic Modification and Biotechnology in Animals, the Central Committee for research involving human subjects, the Health Council and the Centre for Society and Genomics, have in various combinations made the analysis.

Plea for a National Council on Ethics and Biotechnology

In the first half of the decade the Christian Democrats (CDA) repeated their plea to instigate a National Council for Ethics and Biotechnology. Just as in Switzerland and Norway, the Netherlands did and does not have a national ethics council set up by the government, unlike Germany, France, Belgium, Italy and Denmark. According to CDA member of parliament Ormel, the above mentioned trend analysis can pick up indicators from society, but falls short when it comes to getting these indicators on the political agenda (De Vriend 2006). A National Council for Ethics and Biotechnology could certainly help to achieve this.

At the end of 2006, Van Geel, State Secretary of Housing, Spatial Planning and Environment (VROM) organized a conference to discuss the added benefit of such a council (De Vriend 2006). In preparation for the conference, COGEM outlined a number of pros and cons of a national council compared to more specialized committees, based on European research (Zoeteman & Widdershoven 2007). A national council is authoritative, easily identified by the public and offers a clear port of call. The disadvantages are that it is far removed from practice, and ethical issues can be narrowed down into medical issues. Also, there are questions about how to translate a national council's opinions into legislation and responsibility (for example, who is responsible in the cabinet). Virtually all the conference participants felt that ethical issues concerning biotechnology required more structural consideration, but the majority did not see any beneficial value in a national council (Conference Report). Consequently, no such National Council for Ethics and Biotechnology was formed (Parliamentary Papers II 2006-2007, 27428, no. 85).

Focus on risk and societal aspects of nanotechnology

In the second half of the decade, policies were considered for nanotechnology. Having proposed its vision for nanotechnologies in 2005, the government presented its vision 'From small to large' a year later. One reason for a cabinet-wide approach was because so much was happening in this technology area "that with a view to policy coherence, a coordinated approach is required" (Parliamentary Papers II, 2006-2007, 29338 no. 54). Dealing with ethical and social issues was just one action line. There had to be a wide-ranging commission to identify at an early stage any undesirable or harmful effects of nanotechnologies in the areas of health, working conditions, environment, ethics and social relations.[73] This would become the Commission for Civil Dialogue on Nanotechnology (CieMDN) in 2009.[74] The commission presented its final report 'Responsibly further with nanotechnology' in 2011. The public felt it was necessary to have an adequate system for research, granting permits and supervision, in order to apply nanotechnologies responsibly (Nanopodium 2011).

The need to integrate ethical, legal and social research

During this decade, people also began to focus more on the ethical, legal and social aspects associated with technological and scientific research. Consequently the Centre for Society and Genomics (CSG) was founded in 2004.[75] CSG's mission was to understand and improve the

[73] This was following the Health Council's advice in 2006, 'Significance of nanotechnologies for health'.

[74] The commission's remit is to compile a public agenda (a list of priorities of topics to be discussed) and a social dialogue to faciltate these topics, focussing on the social and ethical aspects of nanotechnology. See: wetten.overheid.nl/BWBR0025574/2009-04-01

[75] The Centre for Genomics and Society is part of the Netherlands Genomics Initiative. This initiative began in 2002 and its first phase was aimed at the Dutch knowledge infrastructure (clustering research groups, businesses and hospitals in centres). The second phase in 2008 focussed more on translating scientific outcomes into concrete contributions to social wellbeing and economic growth.

interaction between society and genomics. The Centre combines socio-scientific, philosophical and ethical research with social interaction, dialogue and education. Within NanoNed, the first national research programme in the field of nanotechnology, there was a specific technology assessment research programme (TA NanoNed). In addition, parliament insisted that NanoNed's successor, the extensive NanoNextNL programme (2010-2016), allocated fifteen percent of its research funds on risk assessment & technology assessment (RATA).

At both national and European levels, concurrent investigations into the social and ethical issues surrounding technology were featuring more and more on the research agenda. For example the Dutch Organisation for Scientific Research (NWO) began its 'Socially Responsible Innovation' programme in 2008. Important requirements for awarding projects are that they contribute to policy objectives (societal challenges) and incorporate user involvement. European research programmes began putting more emphasis on the concept 'Responsible Research Innovation' (see the Horizon 2020 and Europe 2020 research programmes) (Von Schomberg 2011; Owen et al. 2012). The key aspect is an open approach involving various stakeholders at an early stage of the research to learn about the consequences of potential innovations, evaluate them in terms of societal needs, standards and values, and subsequently use them as guide in every stage of the research process (EC 2013).

4.6 The 2010s: consider the social and ethical aspects of innovation

Two motions were tabled and widely supported in the Dutch parliament in 2014, showing that from a political-administrative point of view, there was a need for a more (systematic) consideration of the social and ethical meaning of innovation.

In March 2014, senator Ester of the ChristenUnie [Christian Union] party asked the government to structurally integrate the consideration of ethical issues in its technology and innovation policy and periodically report on them (Parliamentary Papers I, 2013-2014, 33750, XIII). The motion refers to converging technologies such as nanotechnology, information technology, biotechnology and cognitive technology (so-called NBIC convergence). In response, in May 2016 the Minister for Economic Affairs sent the Senate an overview of activities within the current innovation policy, underlining the government's focus on social issues. The cabinet intends to include such a review in its annual progress report on enterprise policy. The Senate asked the minister not only to list the activities but also to indicate the associated consequences for policies.

In September 2014, Senator Gerkens of the Socialist party (SP) asked the government to have Rathenau Instituut investigate the desirability of a committee that can advise on the ethical aspects of the digitization of society (Senate 2014-2015, CVIII, E). This motion referred to the emergence of the Internet of Things.

4.7 The governance ecosystem needs a broad perspective

The Gerkens motion in historical perspective

The historical overview clearly shows the political and public focus on the various ethical and social aspects of ICT over the entire period. Since the 1971 census, people had been aware of privacy issues related to ICT developments. This led to the inclusion of privacy as fundamental right in the revised 1983 Constitution and to legislation in the area of personal data. In the late 1970s, there was a fear that micro-electronics would cause many job losses. To allay these concerns, the Rathenau Commission was given the task of investigating the social impact of the advances in micro-electronics. In the second half of the 1990s, following the emergence of the Internet, the Franken Committee was set up to examine the Constitution from a digitization perspective. Infodrome was created to look at the government's role in the information society. The 2014 motions by Ester (referring to NBIC convergence) and Gerkens (on the emergence of the Internet of Things) put digitization and the ensuing social and ethical issues back on the political agenda. The spotlight was now not just on scientific research, but on the entire process of innovation.

Broad perspective on the governance ecosystem

In conclusion, the historical overview and the previous chapters give us three reasons to conduct a broad investigation of the governance ecosystem regarding the ethical and social aspects of digitization, in line with the underlying concerns voiced in the Gerkens motion (see chapter 1).

Firstly, digitization has indeed had an impact on all kinds of scientific, technological and societal developments, because ICT is an *enabling technology* as shown in chapter 2.

Secondly, history shows that a variety of committees is enlisted to look at the governance of ethical and social issues concerning technology. We mention four types:

- State commissions play a role in preparing changes to the Constitution or investigating whether digitization demands such changes. Examples of these are: State Commission Cals/Donner (1967-1971), State Commission Franken 'Fundamental rights in the digital era' (1999-2000) and State Commission Thomassen (2009-2010).
- Advisory committees are asked to chart and advise the government on the historical and social aspects of new developments in science and technology. One example is the Rathenau Commission which looked at the social impact of micro-electronics in the late 1970s, and the DNA Commission ('Brede DNA Commissie') which between 1981 and 1983 mapped the potential applications, social and ethical aspects of recombinant DNA research.
- Commissions tasked with organising public debates, such as the Terlouw Commission which led 'Food and genes' (2001) or the Commission for Civil Dialogue on Nanotechnology (CieMDN), which organised a social dialogue on nanotechnology in 2009.
- Alongside these temporary committees, there are permanent ones in specific areas such as the Central Committee on research involving human subjects (CCMO) and medical ethics committees (METCs). COGEM, the Commission on Genetic Modification, has an indicator role for the ethical aspects associated with the genetic modification of organisms.[76]

[76] We saw that the DECs and METCs started off as forms of self-regulation at a decentralised level and over a long period of time via professionalization, like the founding of NVDEC [Dutch Association of Animal Experiment Commissions] in 1995, and via embedding in legislation. On a European level and scale, legislation is playing an increasingly greater and standardizing role in this embedding and institutionalization.

This means we should not only view one facet of handling ethical matters in our digitizing society but the wide palette of relevant governance activities in the field of digitization, ethics and society.

Thirdly, the Gerkens motion is linked to a parliamentary tradition of questioning the future viability of the existing governance ecosystem regarding the social and ethical aspects of technological developments. In recent decades, parliament has discussed several times the adequacy of the political-administrative handling of social and ethical issues in science and technology. This often happened in response to new breakthroughs in science or technology.

It often takes quite a few decades to build up a governance ecosystem. In the 1970s and 1980s, the question was how to make the social and ethical implications of technological developments more visible. That led to the institutionalization of technology assessment and the creation of NOTA (later the Rathenau Instituut. In the early 1990s, parliament questioned whether the ethical review committees on research involving human subjects (METCs) and animal experiments (DECs) still adequately covered ethical and social aspects in their decision-making. That led to standardization, professionalization and legal embedding of METCs and DECs and lasted for decades. And despite the legal embedding and setting up of new committees such as COGEM, the turn of this century saw renewed doubts about the adequacy of the system. Parliament wondered if the existing network of review committees had due regard for the new and broader ethical issues than they were legally and officially expected to assess. It therefore asked to consider at system level the entire gamut of organizations and committees dealing with the relationship between society, ethics and science and technology. The need for coherence resulted in the 2000s for example in the request to develop an integral ethical review framework and in the plea to form a National Council for Ethics and Biotechnology.

We see three concerns re-emerging in the historical political discussions:

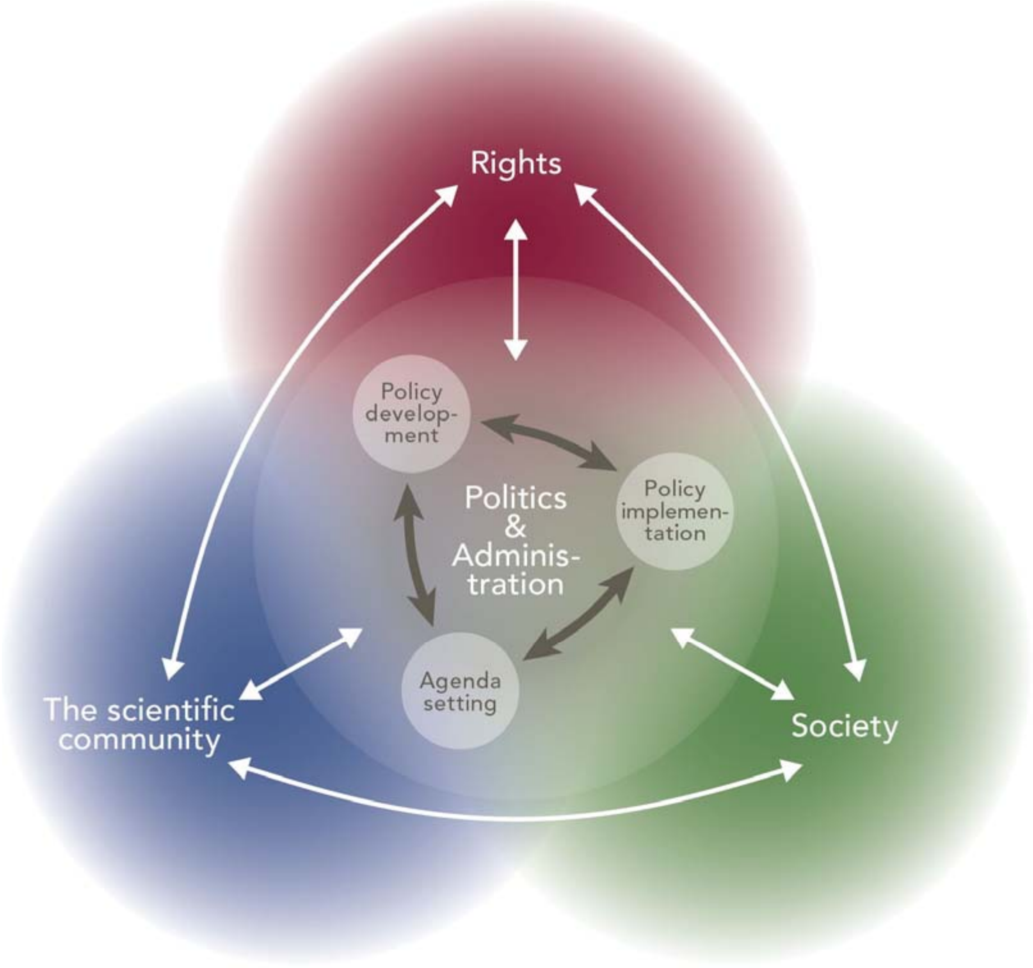
- The importance of systematically recognising new ethical and social issues around novel technology, as well as the public and political debate on those issues – what are the concerns precisely and which values are at stake?
- Does policy address the concerns highlighted – in other words, do these concerns get translated into legislation, are the existing regulations attuned to new developments or is new legislation required? And:
- Are the existing regulations, especially their implementation, sufficiently attuned to new developments and achieve outcomes that are desirable for society?

As stated above, it is obviously customary in parliament, where new scientific and technological developments are concerned, to question the future viability of the current governance ecosystem. This is echoed by the Esther motion regarding NBIC convergence and Gerkens motion regarding the Internet of Things, which raise meta-governance questions on whether the current system is adequate and will remain so in the future. To enable us to analyse how the governance ecosystem handles the social and ethical aspects of digitization, in the next section we present a conceptual framework for that ecosystem based on the historical review.

4.8 Framework for the governance ecosystem

Based on the historical overview, we distinguish governance activities in four domains, which each interact in a complex way (see Figure 4.1): fundamental and human rights, society, science, politics and government. Within the political-administrative sphere we see: a) agenda setting, b) policy-making and political decision making, and c) policy implementation. Regarding political decision making, there is a special role for parliament. Below we explain what part these four domains play within the governance ecosystem for handling the social and ethical aspects of science and technology. At the end of this section we will briefly reflect on the dynamics of the governance ecosystem and the fact that it takes decades to build.

Figure 4.1 Framework for the governance ecosystem



4.8.1 Human rights, fundamental rights and regulations

The first domain of governance activities we describe focusses on the role of fundamental and human rights. In the historical sketch, we saw that ethical and social discussions about new technology often centre round the values that are at stake, which often boil down to fundamental and human rights. Human rights are the rights to which every human being is entitled. They serve to protect people from the power of the state and ensure that everyone has a right to live with human dignity.[77] Human rights often form the basis for legislation and government policy. They are notably embedded in the United Nations Universal Declaration of Human Rights (1948), the Council of Europe's European Convention for the protection of human rights and fundamental freedoms (ECHR, 1950, and since 1998, binding for all Council of Europe member states), and the EU Charter of Fundamental Rights (2000). Human rights are also laid down in national constitutions such as the Dutch Constitution, and are often called 'fundamental rights'. For the Netherlands, these treaties embody important values such as human dignity, freedom, security, equality and justice. Technological developments can strengthen people's rights, but also put them under pressure, or even force them to formulate new human or fundamental rights. The historical sketch provided several examples. Think of privacy as being a new fundamental right (article 10) that was added to the Constitution in 1983 (see box 4.5). The emergence of the Internet in 1999 led to the establishment of the Franken Commission's 'Fundamental rights in the digital age'. For biotechnology, the Council of Europe and UNESCO drew up specific treaties, such as the 1997 Oviedo Convention and the Universal Declaration on the Human Genome and Human Rights, and later the International Declaration on Human Genetic Data (2003) and the Universal Declaration on Bioethics and Human Rights (2005) (see box 4.2).

Box: 4.5 Dutch fundamental rights to privacy and inviolability of the body

Article 10: Privacy
Everyone has, subject to restrictions under or pursuant to the law, the right to respect for their personal privacy.
The law establishes rules for the protection of privacy in connection with the capture and transmission of personal data.
The law sets rules for the entitlement of people to disclose information about them and of the use made as well as the improvement of such data.

Article 11: Inviolability of the body
Everyone has, subject to restrictions under or pursuant to the law, the right to inviolability of their body.

In practice, these general frameworks are often insufficient to address specific issues around a particular technology or practical application. These aspects are therefore often regulated in specific laws and regulatory frameworks. Regarding the fundamental right to privacy, the personal data

[77] See the website on human rights: mensenrechten.nl/wat-zijn-mensenrechten

protection Act (Wbp) lays down in more detail the way personal data may be processed. Another example is the medical-scientific research with human subjects Act (Wmo, 1998). This Act gives a more detailed interpretation of the fundamental right to inviolability of the body (see box 4.5).

4.8.2 Societal actors and debate

The following governance activity within the framework focuses on the role of various social actors and social debate. For a variety of reasons, in practice it can be difficult to establish official ways to handle social-ethical issues, whereas some companies or sectors may have a need to stipulate certain matters. Codes of conduct, such as corporate social responsibility with regard to human rights (see Box 4.6) and self-regulation are ways to fulfil that need. It is also clear that differences in opinions and convictions will always exist in Dutch society and that each individual, organization or company makes its own choices about what applications of new technology it finds appropriate or not.

Box 4.6 United Nations Guiding Principles on Business and Human Rights

In June 2011, the *United Nations Guiding Principles on Business and Human Rights* (UNGPs) were adopted. The UNGPs were developed under the leadership of UN Special Representative Ruggie (which is why they are nicknamed Ruggie principles). The principles consist of three pillars. The first pillar reaffirms the duty of states to protect human rights. The second pillar focuses on the responsibility of companies to respect human rights. The third pillar is the need to give victims of human rights violations the possibility of recovery and/or compensation through the activities of companies (Parliamentary Papers II 2015-2016, 26485, no. 219). The UNGPs do not impose any legal constraints but form an authoritative international standard. The responsibility of companies to respect human rights is included in the Organization for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises.[78] Companies should actively make efforts to acknowledge the risks of human rights violations by themselves or parties in their chain, and where possible prevent violations.

Political discussions on ethical and social issues around new technology often occur at the interface of general values and responsibilities established on the one hand by governments (such as the protection of public health, or the privacy of citizens), and on the other hand give individuals, organizations and companies the space to make their own considerations and choices. In general, the Dutch government would like to put these decisions at the lowest possible level (the principle of subsidiarity). At the same time, the freedom *to be able* to make individual ethical choices in practice also requires social choices. Think of euthanasia or being able to have an abortion. Individuals in the Netherlands, can, under certain conditions, make this decision, but that choice is enabled by organizing a social and legal practice around it.

[78] The OECD Principles for Multinationals (OECD 1976; 2011) are about enterprise-ethical issues and responsible company codes. The Dutch government has underpinned these guidelines; it expects companies to take corporate social responsibility (TK 2012-2013).

The political and social debate can feed into each other. The historical sketch showed that the authorities regularly wanted to encourage public debate on the ethical and social aspects of new technology, such as through the government-initiated discussions on genetically modified food or nanotechnology. The Rathenau Instituut's remit, among other things, is to stimulate the public and political debate on the ethical and social sides of technology.

4.8.3 Scientific knowledge

The third domain of governance activities we discuss is the role of scientific knowledge within the governance ecosystem. This role is diverse and operates at many levels. Scientific knowledge can be useful for both indicating and articulating social and ethical aspects (agenda setting), in formulating a policy design and determining possible action (policy making) and reflecting on the implementation of policies. Ethical reflection (Ladikas et al. 2015) or ethical analysis and foundation (Parliamentary Papers II 1990-1991, 21319, no. 12) is also a relevant form of scientific knowledge in the governance ecosystem. By that we refer to the deeper thinking about ethics and underlying standards, as is often done by ethicists and philosophers at universities. Scientific knowledge for policy is provided by a network of advisory councils and public knowledge organizations.

The historical review showed that during the first decade of this century, the amount of focus and funding increased for research into the integration of knowledge on ethical, legal and social aspects of technology and science with the technological developments. For example, this resulted in the creation of the Center for Society and Genomics (CSG) as part of the Netherlands Genomics Initiative or the risk assessment and technology assessment (RATA) research programme as part of the national nanotechnology research program NanoNextNL.

4.8.4 Politics and administration

The fourth domain in the framework concentrates on the role of politics and administration in the governance ecosystem. We roughly distinguish three processes in the overall policy where ethical and social issues on technology play a role: the agenda setting, policy making and political decision making and policy implementation. We discuss these three stages in more detail below, illustrating for each stage a number of organizations actively involved in the field of bio-ethics.[79]

Agenda setting

With agenda setting, the identification and articulation of ethical and social issues on new developments in science and technology play an important role. This also involves professional advisory bodies, whose remit is to indicate new societal and ethical issues, put them on the agenda and advise policymakers and politicians accordingly. In addition, civil society organizations, public perceptions, citizens and the media all play their part. This phase is also called "ethical deliberation" (Ladikas et al. 2015). Minister Ritzen referred in this context to the indicating and articulating role (Parliamentary Papers II, 1990-1991, 21319, no. 12). Important at this stage is as broad as possible

[79] We thank Boukje van der Zee for compiling an overview of relevant organizations and bodies in this field. For a more detailed overview of the history and individual descriptions of the councils and bodies involved, see Zoeteman & Widdershoven-Heerding (2007) and Rerimassie & Brom (2012).

representation of different views, arguments and interests. Democratic values and the quality of the exchange of views and interests are pivotal.

During this preparatory phase an *aggregation process* can take place (Stemerding & Kater 2005; Van der Meulen & Rip 1998), in which "intermediary bodies" (in between government, science and citizens) voice their visions and concerns about new technologies, make suggestions and raise awareness in the political arena. They translate the indications of potential ethical and social issues regarding new developments in science and technology into the current policy context and put these on the policy agenda.

In the field of bioethical and biomedical issues, for example the Health Council (founded in 1902) and the Council for Public Health and Society (RVS) play an official role at this stage. The Health Council and RVS give substance to their indicator task via the Centre for Ethics and Health (CEG) established in 2003. The Commission on Genetic Modification (COGEM) advises the government on the potential risks of production and handling genetically modified organisms (GMOs) for people and the environment.

Policymaking and political decision making

Deliberation can lead to policymaking and political decision making: a phase in which (political) decisions are prepared and made on the identified social and ethical issues. To make this possible, it has to be made clear *who* can make decisions, for example a regulator or review committee (what Ritzen called the "authoritative allocation of values"). The subject of the decisions should also be clear, for example, that new legislation is required. In a democratic society there are always differences in insight, opinion and belief on how to deal with social and ethical issues. Thus parliament's political decision-making is vital. The phase of policymaking and political decision making can lead to establishing or amending regulatory frameworks and to decisions on other policy instruments, such as making a trend analysis, forming a temporary committee, setting up a social dialogue, deciding on information campaigns and providing research funding.

In the field of bioethics and biomedical issues, several ministries are involved in drafting policy and associated regulatory frameworks, such as Health, Welfare and Sport (VWS), Economic Affairs and the Infrastructure and the Environment. Ministries like VWS have their own ethics section that deals with ethical issues. Parliament plays a powerful and supervisory role, regularly highlighting the need for social dialogue around a particular technology, or fine-tuning existing frameworks.

Implementing policy

A third phase consists of the policy implementation when the above decisions are put into practice. Here, too, all kinds of intermediary bodies are involved, steering or actually implementing the agreed policies. Think of regulators who maintain regulatory frameworks, the judiciary, or ethical review committees, who, based on regulatory frameworks and protocols, assess time after time whether parties have adhered to these frameworks.

In the field of bioethics and biomedical issues, the historical review discussed the various committees for animal experiments (DECs and CCD), and animal testing policy (NCad). For clinical trials involving humans, accredited ethics committees (METCs), often linked to a local hospital, play a role. The Central Committee on research involving human subjects (CCMO) oversees the work of the METCs and in some situations conducts the reviews itself.

4.9 To conclude: Long term dynamics in the governance ecosystem

On the basis of the above, we can conclude that addressing the ethical and social issues surrounding science and technology is a long-term commitment. First of all, it can take a long time before scientific inventions and technological developments are adopted on a wide scale in society. After the discovery of recombinant DNA technology in the mid-1970s, initially a small group of experts focussed on the risks and ethical issues arising in genetic engineering. The debate focused mainly on the modification of micro-organisms within closed systems (which do not enter the environment). It took until the 1990s before possible applications in the field of plants, animals and people featured in the media. This heightened visibility moving towards society and politics seems to be necessary in order to widen the debate and speed up the political urgency.

Another reason why building up a governance ecosystem is a lengthy process is because developing new fundamental rights, new legislation, and the professional development of a monitoring system often takes decades. Animal trials are a case in point; it took twenty years for the first animal experiment committees to professionalize the system and finally legally embed it with the amended Act on animal trials (Wod) in 1996, placing the animal’s intrinsic value at its heart. We see the same thing with research involving humans. The first local medical-ethical review committees were set up in the 1970s. However, it took until 1998 before this practice was legally regulated.

The two dynamics combined – making new developments visible and open to discussion along with the safeguarding of public values – can be problematic. That means it can take a long time before advances in science and technology find their way to the social and political agenda; and subsequently yet again a long time before we finally have a governance ecosystem to deal with ethical and societal issues. In the next chapter, we examine how the governance ecosystem in the Netherlands deals with the ethics of digitization.

5 Blind spots in the governance landscape

5.1 Introduction

In Chapter 3 we reviewed the major ethical and social issues that arise as a result of digitization.[80] In this chapter we will look at how these issues are being handled in the current governance landscape and indicate the blind spots. We do this by using the governance framework set out in Chapter 4 (see Figure 4.1). Just as in the previous chapter, we look at governance and meta-governance issues: in other words, which issues are identified and put on the agenda; who is identifying these issues and what role do these actors play in the governance ecosystem? That gives us a clear indication of where the blind spots are in the governance ecosystem and on which themes. This analysis will enable us to respond to the Gerkens motion whether it is desirable to have a committee that can advise on the ethical side of our digitizing society.

This chapter follows the same structure as the framework in Chapter 4. We begin by describing the three domains and their roles: science (section 5.2), fundamental and human rights (5.3) and actors in society (5.4). We then zoom in on the political-administrative domain, to examine the following processes:

a. agenda setting (5.5)
b. policymaking and political decision making (5.6)
c. policy implementation (5.7), and then conclusions (5.8).

Methodology and scope of the analysis
We now turn to the initiatives related to digitization and the relevant social and ethical issues. For all the domains in the governance framework, we identify which actors are putting which issues (related to the technological areas identified in Chapter 2) on the agenda and which actions or initiatives they recommend. Our focus is limited to actors and reports concerning digitization *and* societal and ethical issues. Our description provides a comprehensive but not exhaustive overview, aiming to cover the most relevant actors and issues at stake. Our analysis focuses on the Netherlands, but also includes interesting developments taking place in other countries up until October 2016. We describe various organizations' initiatives based on their institutional position, for example what the ministries are doing regarding 'policymaking' in section 5.6 and the Personal Data Authority (AP) 'policy implementation' in section 5.7. Obviously these bodies also undertake activities outside their own domain, such a ministry's efforts to stimulate social dialogue. We provide a brief overview of the activities that various organizations and actors propose, prepare, initiate or undertake in order to address social and ethical issues related to the digitization of society. We end

[80] We described issues such as the protection of personal privacy and emotion recognition technology, discrimination by algorithms that advise judges, and digital security for wireless pacemakers that can be hacked. We came up with seven key themes: privacy, autonomy, security, control over technology, human dignity, justice and the balance of power.

each section with a table summarizing the most relevant initiatives per domain. A more detailed description of the organizations concerned and their activities can be found in appendix A.

5.2 The role of science

Here we discuss what science contributes to the governance ecosystem in terms of indicating and articulating the ethical issues evoked by digitization.

In politics and administration
With knowledge and reflection on technological developments – where the humanities and social sciences play an important role – science feeds the social and political-administrative debate. Scientists contribute directly to the political-administrative process when they are asked to provide scientific knowledge to support politicians and policymakers. This takes place in the form of studies, or when individual scientists and experts are consulted during a hearing or roundtable discussion in parliament. Our analysis in Appendix A shows that science often plays an important role in the articulation of concepts. The 1995 Hamad study led to a discussion on the concept of 'confidential communication' which culminated in setting up the State Committee Franken (Parliamentary Papers II 1996-1997, 25 443, no. 1/2). Also the meaning of privacy is largely fed by scientific discussion on this concept (see for example Solove 2002). The research project conducted by Professor B.J. Koops illustrates the digital inviolability of the home as a new concept of privacy (Martijn 2016).

In societal debate
Scientists also contribute to the public debate through the media. In the British newspaper *The Guardian,* Hawking and other scientists warned about the existential dangers of artificial intelligence (Hawking et al. 2014). With their calculations on the automation of certain jobs, Frey and Osborne (2013) formed the starting point for discussions on the relationship between technology and labour. In the Netherlands, science also plays an important role in fuelling the social and the political debate. Professor of philosophy Verbeek did that for example by questioning how far companies may go in applying persuasive technology in the workplace (Verbeek 2016). Studies by Professor of computer security B. Jacobs' research group (Radboud University 2016) led to discussions and questions in parliament about digital security.

In the socially responsible use of innovation
Apart from providing knowledge, science also comes up with innovations that can solve societal and ethical issues, such as solutions in the area of privacy by design, or new cryptographic techniques for making the Internet safer. In research funding, the societal benefits of innovation are considered through concepts such as *Responsible Research and Innovation* and S*ocially Responsible Innovation* [*Maatschappelijk Verantwoord Innoveren*, MVI]. An important factor in this philosophy is that the ethical aspects of innovation are identified at an early stage, and can thus be included in the ethically responsible development of science and innovation. In the science vision (Parliamentary Papers II, 2014-2015, 29338, no. 141) and letter to parliament on ethical aspects of innovation policy (Parliamentary Papers I 2015-2016, 33009, no. 16) the NWO's MVI programme is seen as a significant way of dealing with ethical and social issues concerning innovation already in the research stage. In addition, the world of science is also questioning if they themselves are handling the growing data collections in their scientific research in a responsible way. The Royal Netherlands Academy of Arts and Sciences (KNAW) recommends establishing an *Ethical Review*

Board Informatics to assess whether computer science research is handling personal data responsibly.

Conclusion

Throughout the entire governance eco-system, the world of science enables us to reflect and gain knowledge about the ethical and social aspects of digitization. It thereby exercises influence on three domains: politics and administration, society and fundamental rights. The issues that science identifies – described in Chapter 3 – form an important basis for the advisory bodies and research institutes engaged in setting the agenda for the political-administrative process. Moreover, as we have seen, science also directly influences the political and societal debate and thus contributes to putting the ethical and social issues of digitization on the agenda.

5.3 The role of fundamental and human rights

Fundamental and human rights form the basis of our societal values and fundamental freedoms. These rights are laid down in the EU Charter of fundamental rights, the Dutch Constitution and international treaties ratified by the Netherlands such as the United Nations Universal Declaration of Human Rights (1948). They embed important values such as human dignity, freedom, security, equity and equality. In Chapter 3, we saw that as digitization touches many basic human values, it has led to discussions on the protection of human rights in the digital age. This begs the question what developments are taking place in the Netherlands in the field of fundamental rights and whether they have made provision for new ethical and social issues.

The Netherlands

The emergence of the Internet has been an important driving force for the debate on fundamental rights and digitization in the Netherlands. Two state committees (Franks and Thomassen) have spoken out about whether the Dutch Constitution is still adequate for the digital age. Both committees base their arguments on Articles 7 (freedom of expression), 10 (respect for private privacy) and 13 (confidential communication) of the Constitution. Both committees were seeking a technology-neutral interpretation of these fundamental rights in order to future-proof the Constitution. The procedure for amending Article 13 is currently ongoing. There is also a long-running debate on Article 120 (prohibiting constitutional review).[81] Removing that Article would give citizens and civil society organizations more opportunities to review various laws in the Constitution, for example if they infringe privacy.

Europe

At European level, in particular the Bioethical Commission (DH-BIO) and the Parliamentary Assembly of the Council of Europe (PACE) are working actively on the relationship between digitization and fundamental rights. Both bodies are acutely aware that the broad range of emerging technologies at this time entails numerous ethical issues, which can have all kinds of consequences for human rights. Technological convergence ensures that the usual dividing lines within the ethical

[81] Constitutional review by a court means that the court determines (or may determine) whether laws are in accordance with the Constitution. The debate is split into two camps. Proponents of constitutional reviews call for lifting the review ban (Article 120), whereas opponents argue in favour of an article that makes it impossible to review international treaties.

debate and between the frameworks we have created to deal with ethical issues and human rights are no longer self-evident. PACE is going to investigate in which way converging technologies, artificial intelligence and robotics evoke ethical issues and challenge various human rights. This involves questioning whether it is appropriate to draw up a treaty that specifically addresses the protection of human rights in relation to digitization, parallel to the way the Oviedo Convention[82] does for biotechnology (Van Est and Gerritsen, forthcoming).[83] Having previously dealt primarily with developments in biotechnology and information technology relating to privacy, the Council of Europe’s current interest in converging technologies, robotics and artificial intelligence is greatly broadening its perspective on technology and human rights.

World-wide

At global level, the United Nations Human Rights Council is involved with the protection of human rights in the digital world. The so-called Internet Resolution of 2012 reaffirmed that international human rights conventions also apply to the digital world. These treaties were thus declared to be technology-neutral. However, the Internet Resolution does not guarantee that human rights remain intact in the digital world. The UN Human Rights Council sets its sights specifically on privacy, also in light of increasing surveillance and freedom of speech and expression. In 2015 the UN appointed a special envoy for privacy, whose task is to collect information and draft recommendations to promote the right to privacy (UN resolution 28/16). Within UNESCO, the International Bioethics Committee (IBC) and the World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) report on respectively the ethics of big data and health, and on robotics.

Conclusion

Since the emergence of the Internet in the mid-1990s, the Netherlands has looked at what this means for various fundamental rights, especially privacy, confidential communication and freedom of expression. Amid concerns about the potential impact of new technological developments, the constantly recurring question is whether fundamental rights are still adequately protected. The process to amend Article 13 of the Dutch Constitution (confidential communication) is ongoing. However, there is not much focus on the impact of the Internet of Things, robotics and AI, nor on the potential need to create new fundamental rights in order to cope with this new wave of digitization. In recent years we see that authorities at a global level have been stepping up their focus considerably, as table 5.1 shows.

[82] The Oviedo Convention was drawn up on the initiative of the Council of Europe and opened for signature in 1997. This treaty is based on the European Convention on Human Rights and provides for the protection of human dignity among other things in regard to biomedicine.

[83] Technological convergence, artificial intelligence and human rights. Motion for a resolution. Doc. 13833, 24 June 2015. Parliamentary Assembly of the Council of Europe. See: assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21951&lang=en

Table 5.1 Activities in the area of fundamental and human rights

Who	Technology	Issue	Action
State Commission Thomassen	Digitization	Specifically: freedom of expression, privacy, confidential communication	Proposal to amend Constitution Art. 7, 10, 13
Government	Digitization	Specific: confidential communication	Constitutional Amendment Art. 13
UN Human Rights Council	Internet	Broad: human rights on the Internet	Internet resolution L13
UN Human Rights Council	Internet	Specific: right to freedom of speech and expression	Special envoy freedom of speech
UN Human Rights Council	Digitization	Specific: right to privacy	Special envoy privacy
UNESCO, IBC	Big data & health	Broad: ethical issues	Prepare report
UNESCO, COMEST	Robotics	Broad: ethics of robotization	Prepare report
Parliamentary Assembly of the Council of Europe (PACE) motion	NBIC convergence & artificial intelligence; digitization	Broad: impact NBIC on human rights	Need to research expanding work area from bio-ethics to NBIC ethics
Review of fundamental and human rights	Specific case by case	Specific case by case	NGOs and individuals refer to fundamental rights

Rathenau Instituut

5.4 Role of social actors

Social actors play an important role in the governance of social and ethical issues concerning digitization. Citizens, enterprises and social organizations' actions shape the way digital technology finds its place in society. Here we look at the actions they undertake to address the ethical aspects of digitization.

Political and social discussions

Various civil society organizations have a major influence on the social and political digitization debate. Their main focus is privacy and digital security. Examples are Bits of Freedom's Big Brother Awards which led to questions in parliament (Parliamentary Papers 2013-2014, 211), or the letter from the Privacy coalition to the minister of justice (Parliamentary Papers II 2013-2014, 32761, no. 83). In addition, public events, workshops and websites contribute to the public debate on privacy and digital rights, and the skills users need to protect themselves (for example Bits of Freedom's online Toolbox). Privacy First Foundation go down more of a legal route to focus attention on privacy infringements, by initiating proceedings on things like taking finger prints under the Passport Act, process controls and the retention obligation for telecom data. In this way, Privacy First is demonstrating that civil society organizations can play a role in maintaining legislation and protecting public interests. Moerel and Prince (2016) argue that these types of procedures can be an important addition to enforcement by regulators. Regarding privacy and data protection, there is a growing focus on so-called *class actions* – procedures that are initiated on behalf of a group of people.

The consumers association (De Consumentenbond) also focusses actively on the topic of privacy, for example by mapping how fitness apps handle user data. With its 'Digidwang' campaign, the association is opposing the trend that more and more organizations are forcing digitization on consumers. In November 2015, ANWB (Dutch touring club), together with its European sister organizations, launched the campaign 'My car, my data' to raise public awareness and to advocate regulating the data that manufacturers collect from smart cars.

Society and enterprise

Civil society organizations such as ECP (Platform for the information society) form a link between the authorities and the business world. ECP collaborates with enterprises and government to strengthen the social and economic value of information technology. With campaigns, research and debate, they bring stakeholders together and support the implementation of certain policy objectives. A major theme is stimulating and improving digital literacy and security, not only in companies but also for government and consumers. This was done for example with the programmes 'Digiveilig Digivaardig' and also 'CodePact' which gives as many children as possible the opportunity to learn programming.

The business world also undertakes activities to deal responsibly with the ethical side of the digitizing society. Some companies explicitly profile themselves as offering privacy-friendly services. The QIY Foundation for example is working on a system that gives users more control over their own data. The search engine Ixquick gives people the option to surf the web without compromising personal information. Internet service providers such as XS4All and Greenhost are committed to an open and free internet and digital security. In addition, there are also industry-wide initiatives to take social responsibility for digitization. One example is the Dutch Association of Insurers, that on behalf of its members concluded an agreement on how to handle data, and it annually monitors the impact of big data on social solidarity (Verbond van Verzekeraars 2016). At the same time, there is also regular criticism of companies, for example about the way they deal with user information. Large technology companies like Google, Apple and Facebook are sometimes the target of criticism or concerns. But also banks, insurance companies, electronics manufacturers and apps developers have had their fair share of negative publicity in recent years.[84] Although the above mentioned

[84] See for example http://www.volkskrant.nl/tech/-facebook-werkt-aan-censuurwapen-om-toegang-tot-china-te-krijgen~a4420772/
http://www.volkskrant.nl/media/google-en-facebook-nemen-maatregelen-tegen-nepnieuws-na-kritiek~a4415610/
http://www.volkskrant.nl/tech/achmea-biedt-korting-in-ruil-voor-privedata~a4154347/
http://www.volkskrant.nl/tech/apple-music-bindt-in-na-protest-taylor-swift~a4085852/
http://www.volkskrant.nl/tech/airbnb-uber-ze-hebben-maling-aan-alles~a3795584/ or in Parliamentary Papers: II, 2013-2014, no. 2008; II, 2013-2014, no. 2912; II, 2015-2016, no. 2377.

activities show that the business world is paying more attention to the social and ethical issues surrounding digital products and services, what is still lacking is a structural focus and accountability for the ethical and social impact of digitization.

International

Whistle-blower Snowden's revelations about data collection and surveillance by NSA and other international security services have led to many social and political discussions since 2013, firmly planting the themes of surveillance and privacy on the social agenda. At the international level, various social organizations' campaigns and initiatives aim to protect and entrench digital rights. In order to protect the rights of internet users, Berners Lee, the founder of the world wide web, called for a digital Magna Carta[85] (Kiss 2014). Striking the same chord as Berners Lee, there are initiatives in the UK to come up with a *Digital Bill of Rights.*[86] In the run-up to the European elections in 2014, the European Digital Rights Initiative (EDRi), a group of civil rights organizations including Bits of Freedom, launched a campaign on digital rights. And the Global Commission on Internet Governance initiated by various international think-tanks, is calling for the protection of digital citizens' fundamental rights (GCIG 2016).

Apart from the public debate on privacy, discussions are now taking place on autonomous technology. They are focussing on matters like control, transparency and human autonomy and there are calls for new forms of supervision. In February 2016, innovation foundation NESTA advocated setting up a *Machine Intelligence Commission* in the UK (Mulgan 2016). NESTA bases its recommendations on experiences with previous commissions for environmental pollution and embryo use, which have played an important role in stimulating public debate on ethical boundaries, creating and securing public trust, and enabling economic development. Such a commission would have no formal role in certifying or approving algorithms, but would require strong competencies for accessing information and carrying out research. The Institute of Electrical and Electronics Engineers (IEEE) – the International Organization for technical professionals – is working on an initiative to support developers of autonomous systems in making ethically responsible choices (IEEE 2016). In September 2016, the British Standards Institute (BSI) published a series of guidelines for the ethically responsible design and application of robotics (BSI 2016); some companies are setting up committees to deal with ethical issues. Similarly, Rabobank has an Ethics Office (*Bureau Ethiek*) dealing with the subject of digitization, and Google has set up an ethics committee for the development of artificial intelligence. However, nothing has yet been revealed about the role and composition of Google's committee (Shead 2016).

Conclusion

In the Netherlands various social organisations – Bits of Freedom, Privacy First, Consumentenbond and ECP – along with several socially responsible companies, play their part in the debate on the impact of digitization. The social issues that arise are to do with privacy, digital security and the associated digital literacy (see also table 5.2). People are very much aware of issues such as digital coercion, exclusion and an open and free Internet. In civil society organizations, however, there seems to be less awareness of issues like justice, autonomy and human dignity.

[85] The Magna Carta is one of the first treaties that limited the power of the King of England in the Middle Ages and laid down a number of fundamental rights. The Magna Carta is seen as an important historical step in the development of the modern democratic regime.

[86] cybersalon.org/digital-bill-of-rights-uk

As far as technology is concerned, the key focus is on the Internet, apps, government services and consumer electronics. Dutch civil society organizations still do not have a clear role in stimulating discussions on AI, robotics and emerging technologies. This is possibly because such technologies are still barely visible in people's everyday lives. The advances in robotics, smart algorithms and IoT can change all that in the short to medium term. Organizations such as ECP and companies like Google realize that new developments require ethical reflection on topics like autonomy, data discrimination and human dignity. On the international scene, we see the establishment of ethical working groups and committees and the first signs of seeking ethical guidelines for developers and companies, such as the initiatives of the Institute of Electrical and Electronics Engineers (IEEE) and the British Standards Institute (BSI). There are calls for new forms of supervision and in light of the increasingly autonomous technology, people are questioning if we will (still) be able to check how smart algorithms work. In the public domain, global discussions are ongoing about human rights in the digital age, like initiatives for a *Digital Bill of Rights* in the UK. The online domain is key, and above all autonomy on the Internet.

Table 5.2 Activities at societal level

Who	Technology	Issue	Action
ECP	Digitization	Security, privacy	Programmes for digital skills & security, working group ethics & ICT
Bits of Freedom	Internet, digital communication	Privacy, security	Big Brother awards, privacy coalition, internet freedom toolbox
Privacy First	Digital communication, e-government	Privacy	Legal actions
Consumer association	Apps, consumer technology	Privacy, inclusivity	Campaign privacy awareness. Call manufacturers to account on privacy
EU and international			
EDRi (EU)	Internet, digital communication	Human rights online	Campaign promise protection digital rights from legislative candidates
Nesta (UK)	AI, algorithms, robotics	Autonomy, control of technology, trust	Call for Machine Intelligence Commission
Global Commission on Internet Governance	Internet, digital communication	Human rights online	Report with call to protect digital rights
IETF (int.)	Internet, digital communication	Human rights	Human Rights Research Group investigating if protocols can take account of rights

IEEE (int.)	AI, algorithms, robotics		Initiative to help designers of autonomous systems make ethical choices

Rathenau Instituut

5.5 Agenda setting

We described the various ethical and social aspects emerging from discussions in the field of science and law and in society. In the political-administrative domain, advisory boards and institutes put the aspects identified on their agendas. Many organizations meet to discuss the subject of digitization, but only a limited number look at the associated ethical and societal issues. In recent years, in particular the Scientific Council for Government policy (WRR), the Advisory Council on International Affairs (AIV), Council for the environment and infrastructure (Rli) and Rathenau Instituut have examined the relationship between digitization, society and ethics. The question is whether the ethical and social issues identified – as described in Chapter 3 – have also made it onto the agenda.

Role in the governance landscape

The advisory boards and institutes provide information and advice at the request of policymakers and parliament as well as unsolicited advice to put certain topics on the agenda. The Rli and the AIV voice their opinions on digitization in relation to their work domain, respectively the environment and foreign policy on human rights, peace and security. The WRR's role is to advise the government on long term developments which affect society.[87] As such, the WRR has looked into digitization in a number of studies. The topic is addressed most structurally in the work carried out by Rathenau Instituut as part of its contribution to the social and political debate on issues associated with scientific and technological developments such as digitization.[88] Rathenau Instituut has discussed many aspects of digitization in recent years and conducted more than 20 studies on this topic. The institute looks at both the political-administrative and public debate on the impact of digitization.

Identified ethical and social questions

Table 5.3 shows how organizations are tackling a wide range of digitization issues. The analysis in Appendix A confirms that generally speaking, all the ethical and social matters we flagged up in chapter 3 are included on their agendas. We see ethical issues such as privacy and security frequently reappearing, but also topics like autonomy human dignity, social inclusion, transparency, control of technology, justice and discrimination are covered. These issues are mostly raised to address current technological developments or practices such as big data, robotization, e-government or autonomous weapon technology.

[87] Institutional Law WRR, Art. 2. 30 June 1976.

[88] Newspaper Staatscourant. 24 November 2009

Governance options

In the various reports and advice on the governance of ethics in digitization, we see that the organizations' recommendations fall roughly into three categories: intensify policymaking and political decision making and also political debate; increase supervision; and support the public debate on technology.[89] Various studies call for shaping a parliament-wide vision on big data, the Internet, robotics and intimate technology. They emphasize the need for an interdepartmental approach. The AIV does that in relation to internet policy (AIV 2014), the Rli in relation to data and digitization (Rli 2014). Rathenau Instituut calls for a vision on robotics (Van Est & Royakkers 2012) and intimate technology (Van Est & Rerimassie 2014). In addition, various councils advice increasing the surveillance of big data and algorithms (WRR 2016; AIV 2014; Dratwa 2014). The WRR (2016) has identified that there is a mismatch between big data and the current legislation which is mainly directed at collating data. The WRR, just like Rathenau Instituut (Van 't Hof et al. 2012b; Kool et al. 2015), argues that there should be more focus on the data analysis stage and how the applications of this analysis affect individuals.[90] This is in line with what is being identified in the world of science, thus demonstrating the link between scientific knowledge and agenda setting. Finally, various bodies put forward recommendations in their reports to stimulate public debate and foster a more digital and media savvy citizenship (see for example Rli 2015; Van Est & Rerimassie 2014).

At European level, since its founding in 1991, the European Group on Ethics in Science and New Technologies (EGE) has examined ethical issues arising from new technology. Initially concentrating on biotechnology and medical research, nowadays this group is focussing more on ethical issues in information technology. In its reports on the ethical aspects of ICT (Salvi 2012) and surveillance (Dratwa 2014), the EGE calls for protecting fundamental rights in the digital era.

Conclusion

As we can see in table 5.3, the current regime of advisory councils and institutes does have most of the ethical and social issues we identified in Chapter 3 on its political-administration agenda. The councils each play their individual role, based on a decree establishing their responsibilities and tasks. Besides privacy and data collection, their agenda includes major issues such as justice, autonomy, control over technology and human dignity. Most of the policy advice the councils and institutes are asked to provide, has to do with specific technological practices such as healthcare technology or cyber intelligence. This begs the question how the government should create a comprehensive view of digitization, a recurring question posed in recommendations for vision forming and interdepartmental coordination.

[89] A detailed analysis of this advice can be found in Appendix A.

[90] For example how individuals are treated differently based on group profiles and how they are protected against incorrect analyses.

Table 5.3 Agenda-setting activities in the political-administration domain

Who/what	Technology	Issue	Advice/action
Scientific Council for Government policy (WRR)			
iGovernment	Digitizing government	privacy, transparency, autonomy, control	Awareness of transformative impact of ICT on government. Establish IAuthority and iPlatform to improve citizens' resilience
Public core of the Internet	Internet infrastructure	Security, censorship, free access	Determine the public core of the Internet in international treaties
Mastering the robot [Robot de Baas]	Robotics	work, inclusion, equality, autonomy	Establish complementary cooperation people and robotics
Big data in a free and safe society	Big data and algorithms	privacy, security, autonomy, discrimination, right to fair trial	Stronger focus on use of data, surveillance of algorithms, new tasks for regulators
Advisory Council on International Affairs (AIV)			
The Internet	Internet infrastructure	Internet freedom, privacy, surveillance, information security	Protect internet freedom. Interdepartmental coordination and vision of internet policy
Autonomous weapon systems	Autonomous weapon systems	Control of technology, responsibility	Meaningful human control when using autonomous weapon systems
Council for the environment and infrastructure (Rli)			
Technological innovation in the the environment	Digitization (AI, data infrastructure, drones, robotics, IoT, VR)	Privacy, transparency, security, access, control of algorithms, autonomy	Data development requires cabinet-wide vision and public debates about impact on fundamental values
Rathenau Instituut (selection of publications)			
Just Ordinary Robots	Robotics, AI	privacy, autonomy, human dignity, control of technology	Policy vision of which tasks can be transferred to robots, do not automate life and death decisions
Working on robot society	Robotics, AI, platforms	Unemployment, human dignity, inclusivity	Training, including innovation, safeguard against monopolization and exploitation digital platforms
Data driven society	Big data, algorithms	privacy, transparency, control of algorithms, autonomy, discrimination, balance of powers	Control of algorithms, protecting autonomy and equality. Data is not neutral: stimulate data literacy
Sincere support	Health apps, wearables, persuasive technology	privacy, autonomy, reliability of technology, transparency, balance of powers	Protect privacy and autonomy, certification for reliable e-coaches, mandatory burden of proof government's commitment to influencing behaviour

Intimate technology	Broad digitization	privacy, autonomy, human dignity	State-wide approach to the impact of digitization on fundamental rights, foster technological citizenship
European Group on Ethics in Science and New Technologies			
Ethics of Information and Communication Technologies	Broad digitization	privacy, human dignity, autonomy, freedom of speech, access to technology	Access to tot ICT. Stimulate digital skills, free online identity development and responsible personal use of ICT
Ethics of Security and Surveillance Technologies	Big data, surveillance security technology	Security, privacy, human dignity, autonomy, discrimination	Obligatory to make explicit assumptions of algorithms. Do not exchange human dignity for other values such as security

Rathenau Instituut

5.6 Vision forming and political decision making

Translating policy-preliminary reports and advice into visions, policies, regulations and laws, and their political approval takes place at the policymaking and provision stage. Here we take a look at the actors institutionally responsible for policy and political decision-making: the cabinet, the ministries and parliament consisting of the Senate and the House of Representatives.

We see in table 5.4 that privacy, data protection and security issues play a prominent role in policymaking and political decision making. Questions about protecting privacy and creating a vision on the subject are regularly asked in the Senate and House of Representatives (see Appendix A). Actions are undertaken through the various departments, for example to strengthen the capacity of the Personal Data Authority. There are often calls to increase this Authority's budget as well as the powers for imposing fines.[91] New legislation and regulations – at national and at European level – strengthen the protection of the individual, but the regulator's capacity and competency remain important topics of discussion: are they adequately equipped to deal with the challenges of big data, profiling and smart algorithms? Ongoing education and training are often quoted as key to meeting the challenge of digitization. The Ministry of Education, Culture and Science stated in its letter on Education 2032 that digital skills should become part of the core curriculum in education (Parliamentary Papers II, 2015-2016, 31293, no. 278). Its letter on future-proof regulations highlights the tension between creating space for innovation while also keeping an eye on the protection of public values (Proceedings II 2014-2015, 33009, no. 10).

The ministries and parliament actively seek advice on the best way to deal with new technological developments. For example the Cabinet sought advice from WRR on big data and security, the Ministry of Social Affairs and Employment asked the Social and Economic Council of the Netherlands (SER) for advice on robotization and labour, and the Ministry of Economic Affairs had the high level expert group for big data and profiling look at the impact of these developments on

[91] See Parliamentary Papers II 2015-2016 32 761, no. 102

the fundamental rights to privacy and to equal treatment. Parliament wishes to conduct well informed debates on the public and ethical aspects of digitization. The House of Representatives requested that Rathenau Instituut study the scientific knowledge available regarding technology and labour. The motion Ester (Parliamentary Papers I, 2013-2014, 33750 XIII) required the Ministry of Economic Affairs to report annually on the role of ethics in innovation policy to enable a structurally recurring political-ethical debate in the Senate. The Ester and Gerkens motions both show that the Senate recognizes the impact and the importance of keeping abreast with digitization.

Parliament regularly calls on the government to form an overall vision on the impact of digitization, for example on privacy (Parliamentary Papers II 2013-2014, 89, no. 83 and no. 32761). The D66 party's paper 'Techvisie' says the current policy is too highly incident-driven and recommends appointing a Minister of Economics, Technology and Privacy. The idea of an overarching approach to digitization also features in international initiatives to establish digital rights. For example in France's *Republique-Numerique* bill and the UK's call for a *Digital Bill of Rights*. We also see a global focus on the ethical aspects of the self-driven car. Germany's Minister of Transport has set up an Ethics Committee in this field (Ramthun & Schlesiger 2016) and in the US, the Federal Government has established rules for (highly) automated vehicles, focussing on ethical issues (USDoT 2016). To spur the European Commission to take action on the social and ethical aspects of Robotics and AI, the European Parliament's Committee on Legal Affairs is preparing a report on robotics and artificial intelligence (2015/2103 INL). The draft report contains a proposal for a code of ethics for robot builders, a code for research ethics committees, and a model for users on acts permitted with robots.

Conclusion

It is clear that a great deal of attention is focussed on privacy at the policymaking and implementation stage. Ministries and parliament actively seek information, so that from a policy point of view, they know how to address the emerging technologies: the new responsibilities inherent in digitization and how to give innovation the space it needs and bear in mind public values. Parliament wants to be kept up to date by the government to enable well-informed parliamentary debates. We see parliamentarians regularly asking the government to form an integral vision on privacy.

The political-administrative interest in issues like autonomy, justice and human dignity, albeit relatively limited, seems to be growing. Topics such as big data, the use of algorithms, autonomous weapon systems and self-driving cars are putting issues like justice, discrimination and autonomy more in the public eye. On the international scene, we see gradual political-administrative steps being taken by the European Parliament's Committee on Legal Affairs (see table 5.4).

Table 5.4 Policymaking activities within the political-administrative domain

Who/what	Technology	Issue	Action
Ministry of Economic Affairs			
Vision Telecommunication	Internet, digital communication	Free, open internet, freedom of choice	Stimulate security, neutrality and continuity
Letter Big data & profiling	Big data, profiling, algorithms	Privacy and equal treatment	High level expert group
Letter Future-proof regulations	Digital platforms	Public values such as consumer security, fair competition	Experimental space in regulations, bearing in mind public values
Letter Ethical aspects of innovation policy	Digitization	Merging people & tech; privacy and autonomy	Focus on ethics in research; annual reporting on enterprise policy
Ministry of Security and Justice			
Brouwer-Korf Commission	Digitization, digital communication	Security and privacy	Mandatory notification data breaches; extend AP authority to impose fines
Memo Freedom & security in the digital society	Digitization, digital communication	Security and privacy	Stimulate privacy by design, mandatory *Privacy Impact Assessment* for new legislation, digital resilience campaign. Request WRR advice on big data
Bill computer criminality III	Digitization	Security	New powers security services
Cabinet's position on encryption	Encryption	Confidential communication, privacy	Legal restriction of encryption not desirable
Ministry of Education, Culture and Science			
Letter Education 2032	Digitization, robotization	Digital skills, privacy, security, online behaviour	Digital literacy in core curriculum. Ongoing training
Ministry of Social Affairs and Employment			
Letter Technological developments and labour market	Robotization, automation	Human dignity, technological unemployment	Request investigation Rathenau, SER, CPB (Bureau for Economic Policy Analysis)
Letter Working on robot society	Robotization, automation	Human dignity, technological unemployment	Commit to good education, life-long learning, retraining and transitions
Ministry of Foreign Affairs			
Letter Foreign internet policy	Internet	Fundamental rights: freedom, privacy, equality	Interdepartmental vision on internet policy, fundamental rights also apply online

Human rights reporting 2015	Internet, algorithms	Fundamental rights: freedom, privacy, equality	Focus on digital rights, ethics and algorithms at GCCS Conference
Letter Autonomous weapon systems	Autonomous weapon systems	Human dignity, control of technology	Assign responsibility part of design stage. AIRCW review of meaningful control
Ministry of Internal Affairs			
Letter iGovernment	Digitization of the government	Citizens' resilience, control of technology	Embed awareness impact of digitization in government
Bill Wiv (intelligence & security services	Digitization communication	Security	New powers security services
Parliament			
Parliamentary questions and motions	Various partial aspects digitization	Various ethical issues, high focus on privacy	Questions on vision, position, policy, legislation and regulation
VVD Robot agenda	Robotization	Human dignity; unemployment	Commitment to education. Investigate value of National Ethics Committee
D66 Techvisie	Digitization, Internet	Privacy, surveillance, net neutrality, security, confidential communication	Minister of Economics, Technology & Privacy, digital skills, strengthen regulators, internet giants' duty of care
EU and international			
EU – Onlife initiative	Broad Digitization	Broad range ethical issues	Onlife Manifesto informs research agenda
EU – General Data Protection Regulation	Data collection and protection	Privacy, data protection, transparency	Strengthen regulator, rights of internet users and data processor obligations
European Parliament – Draft Report on Civil Law rules on Robotics	Robotization and AI	Security, privacy, integrity, human dignity and autonomy	Resolution proposal for European Parliament to create ethical principles and a European Agency for robotics and AI
UK – Campaign for Digital Bill of Rights	Digitization, Internet, digital communication	Privacy, surveillance, balance of powers	Proposal for property rights data. Equal Internet access
France – Republique Numerique Bill	Digitization, Internet, digital communication platforms	Privacy, net neutrality, transparency, balance of powers	The right to be forgotten. Transparency with business model platforms. Rights of data after death

5.7 Policy implementation

At the policy implementation stage, we examine how regulators and review committees ensure that the rules, standards and laws determined in the policymaking and political decision making stages are implemented and upheld. A supervisory body is a government-appointed, independent and impartial institution that supervises compliance with legislation and regulations. Based on regulatory frameworks and protocols, review committees assess, mostly case by case, if a particular action – such as the purchase of an autonomous weapon system – complies with the established frameworks.

From data protection to digital ethics

One supervisor with a clear role in digitization is the Dutch Data Protection Authority (AP). As its supervision is specifically geared to privacy and data protection, it plays an important role in the evaluation of new legislation and checking privacy policy. As of 1 January 2016, the AP's budget and powers have expanded, among other things with stronger penalty jurisdiction and supervision of the obligation to report data breaches (AP 2016). The AP's key focus is the user's well informed consent and control. We see in our analysis that big data and the emergence of the Internet of Things are putting pressure on this perspective. We are also aware of suggestions that the AP should play a stronger role in regulating the application of big data and algorithms: the WRR (2016) advises strengthening the competencies of the AP and the Supervisory Committee on the Intelligence and Security Services (CTIVD) in this area.

The European Data Protection Supervisor (EDPS) has widened its focus beyond the realm of privacy. With its opinion paper *Towards a new digital ethics* (EDPS 2015) and the establishment of an *Ethics Advisory Group,* it is examining the relationship between human rights and digital technologies such as algorithms, AI, big data and the Internet of Things. With this step towards digital ethics, EDPS is gaining much more insight in issues such as discrimination, human dignity and autonomy. The Netherlands Institute for Human Rights (CRvdM) plays a role in terms of discrimination and the protection of human rights. In its strategic plan, however, CRvdM does not yet refer to how technological developments affect human rights (CRvdM 2016).

In the field of digital security, the National Cyber Security Center and the Cyber Security Council play a prominent part in stimulating a safe and resilient digital society. Regulators such as the CTIVD and the Advisory Committee on International Law and Conventional Weapon Use operate in specific areas, respectively the security services and use of weapons. The Authority for Consumer and Markets (ACM) focuses on the protection of the digital consumer and in that capacity looks at aspects of privacy. In addition, the ACM indicates it will look at how companies expand their dominance on the Internet by using personal data. They can thus play a role in discussions about monopoly-forming on platforms like Airbnb and Facebook and the *lock-in effect* that occurs when users cannot switch providers easily enough. Also other regulators not traditionally involved in digitization are having to face these issues. The Human Environment and Transport Inspectorate (ILT), for example, was confronted with the rise of Uber and decided that the UberPop service, whose drivers do not have a taxi licence, would be banned in the Netherlands. Because different regulators are dealing with digitization, it is also important that an agreement is reached between the various parties – such as through the Market Supervisors Council (Markttoezichtsberaad) – on how the supervision is organized and where the responsibilities lie for the various regulators.[92]

Conclusion

Our research shows that supervision has been developed the most in the areas of privacy and data protection. For other ethical issues concerning digitization such as discrimination, autonomy, human dignity and unequal balance of power, the supervision is not as well organized. The CRvdM is the point of contact for discrimination, but digitization is not yet explicitly on its agenda (CRvdM 2016). At the same time, there seems to be an increasing focus on other issues than privacy. The most telling example is the EDPS initiative to establish an ethics advisory group.

Both the public and political debates call for stronger and broader supervision, for example when it comes to algorithms. In section 5.4 we discussed that in 2016 the British Innovation Foundation Nesta called for setting up a Machine Intelligence Commission, which should be given enhanced powers to investigate the working of algorithms and gaining access to information.

Table 5.5 Policy implementation activities within the political-administrative domain

Who/what	Technology	Issue	Action
AP	Digitization (services that process personal data)	Privacy, data protection	Supervise data processing government and businesses
ACM	Internet, apps	Privacy, balance of powers	Awareness raising campaign for privacy, power internet providers
CRvdM	-	Human Rights (special focus discrimination)	-
CTIVD	Security technology	Privacy, data protection, security	Supervision of security services
NCSC / CSR	Digitization	Security	Stimulate secure and resilient digital society
AIRCW	Weapon technology	Autonomy, control of technology, human dignity	Advice on meaningful human control of weapon systems
National ombudsman	Digital government services	Autonomy, human dignity	Complaints about digital government systems that go wrong

[92] The Market Supervisors Council previously focussed on the topic of Big data, see: https://www.acm.nl/nl/publicaties/publicatie/13819/Agenda-Markttoezichthoudersberaad-2015/

EU and international			
EDPS	Digitization (services that process personal data)	Broadening privacy to autonomy, human dignity, discrimination	Advisory group digital ethics, recognition impact of digitization on human rights

Rathenau Instituut

5.8 Conclusion

In this chapter we examined whereabouts there are blind spots in the governance of the ethical and social aspects of digitization. We looked at whether the issues we identified in Chapter 3 are being adequately addressed in different domains of the governance-ecosystem. In doing so, we looked at the actors in the fields of: fundamental and human rights, science, society, politics and governance. This concluding section sketches an integral picture arising from the question: which issues are identified and put on the agenda; and are the actors involved capable of dealing with these issues?

Focus on social and ethical issues surrounding digitization
The emerging Internet of Things, robotics, biometry, persuasive technology, big data, digital platforms, artificial intelligence, augmented and virtual reality, are all part of a new wave of digitization. The information society has thus reached a new phase, bringing new social and ethical issues along the way, such as privacy, security, autonomy, justice, human dignity, control of technology and the balance of powers. Our analysis shows that, at present, most of the public and political focus is on privacy issues (especially personal data protection) and digital security. The major challenges are the search for digital inviolability of the home and the protection of privacy with the emergence of the Internet of Things. We also see a growing focus on issues like justice and the balance of powers. Regarding the former, the focus is on big data, algorithmic profiling, the impact on the right to equal treatment and presumption of innocence. In addition, the dominant position of large internet companies is becoming a hot topic of debate. Autonomy, human dignity and control of technology are still less popular topics in the public debate and are only being flagged up to a limited extent by social organizations and in policy-making and political decision making circles. Consequently, these are the areas where we identify blind spots in the governance landscape. These issues are identified in science and communicated to policymakers at the agenda setting stage, but there has not yet been an adequate response. Below we will elaborate per domain on these conclusions.

Science
In science we see a keen interest in the social and ethical side to this wave of new technologies (see chapter 3). Via the media, some scientists attempt to arouse public and political interest in the various issues regarding digitization. Prominent scientists like Hawking (Hawking et al. 2014) highlight the impact of developments in AI. Based on its knowledge position, science has a responsibility to raise awareness of these risks. The Royal Dutch Academy of Arts and Sciences (KNAW) recommends setting up an *Ethical Review Board Informatics* in order to assess whether computer science research is handling personal data responsibly. Since the beginning of this

century, the notion of socially responsible innovation is gaining in popularity. The aim is to take into account the social and ethical issues of new digital applications in the research phase already.

Fundamental and human rights

The discussions on fundamental rights in the digital age already date back many years. In the historical chapter we saw that discussions on privacy have been going on since the 1971 census. In the 1990s, with the emergence of the Internet and digital services, the debate took on a new dimension. Now we are confronted with a new wave of digital technologies such as the Internet of Things, robotics, big data and AI. At international level, initiatives by the Council of Europe, the UN and UNESCO show that these developments need to be viewed from a human rights perspective. The analysis shows that in the Netherlands, discussions on safeguarding human rights in relation to this new wave of digital technologies have not yet got off the ground. So here is a blind spot in the governance landscape. It requires policy attention to safeguard fundamental rights in relation to digitization, whereby a link can be sought with on-going European initiatives that tie in with the protection of fundamental rights relating to digitization.

Society

Various social organizations are involved with privacy and digital security and know how to drive the political-administrative discussions. Actions by Bits of Freedom (like the Big Brother Award) and the Privacy Coalition have led to various questions in parliament. The Netherlands does not, however, have any established social organizations that raise discussions on AI, robotics and emerging technologies, nor ethical issues regarding autonomy, discrimination and human dignity. There is more happening with these topics at international level, namely initiatives to protect and determine digital rights such as the action for a *Digital Bill of Rights* in the UK. There are also numerous specific actions. The British innovation foundation NESTA advocates wetting up a commission for regulating algorithms (Mulgan 2016). The British standardization organisation has developed ethical guidelines for designers of autonomous systems and robotics (BSI 2016). Companies like Google have formed internal ethical committees to keep an eye on AI developments. Although these company initiatives demonstrate that the focus on the impact of digitization is growing, there is still a lack of structural focus and responsibility on the part of the business world to safeguard public values. This has led to a blind spot concerning companies' responsibilities for the governance of societal and ethical issues arising from digitization. The lack of a critical public counter-message on the new wave of digitization – and the opportunities for citizens and civil society to organize this – have also created a blind spot in the governance landscape's social domain.

Political-administrative domain

The ethical and social issues which the scientific literature identifies, are also on the political-administrative agenda. A broad spectrum of technological developments and practices play a role: from the arrival of the smart car, big data and profiling to armed military drones. Rathenau Instituut has played a specific role in this, and in their institutional role, advisory bodies provide an important contribution with advice and reports. In this way we can see that the issues identified in science are also reflected in the agenda setting.

The step from agenda setting to policymaking still seems to present a challenge. Not all the issues on the agenda are reflected in policies. Currently the major focus is the issue of privacy. The new

Data Protection Regulation does provide a clear legal framework in that area. However, the control of personal data is not sufficient to protect privacy as a human right. We also need to look at digital security, for example in a national cybersecurity strategy. Relatively little attention is paid to the other identified issues and even then there is still a need for knowledge on what is involved in the technology and the potential social and ethical significance. The Gerkens and Ester motions show that parliament also requires better discussions on the social and ethical aspects of digitization, and a structural embedding of this discussion on the cabinet's agenda.

Regulators are challenged to respond to the digitization trend. Digitization questions whether the current supervisory bodies are able to fulfil their task and if their mandate is still adequate. The Consumer and Market Authority is for example looking into how to deal with large internet companies' strong position in the market. As point of contact for discrimination, the Human Rights College has not (yet) shown much interest in for example data discrimination. In the political debate we see the call for more room for the Personal Data Authority (AP) and new forms of supervision, certainly for algorithms. An example is the EDPS initiative to set up an *Ethics Advisory Group*. The regulators themselves are even wondering how to deal with ethical issues such as autonomy, discrimination and human dignity.

We thus see various blind spots that demand attention in the political administrative domain. Firstly in the area of policymaking, where there is a lack of translating identified issues into policy and a need for coherence and interdepartmental coordination for digitization. What is the best way to align existing responsibilities and legislation with the digital world? Where are new responsibilities arising and how can these best be allocated? Secondly in the political debate, a structural discussion on the impact of digitization is lacking. Thirdly in the area of supervision, there is a need to strengthen the supervision and improve the collaboration between the various regulators involved in different ways with digitization.

From incident to structural political-administrative approach

The Gerkens motion asked if a committee was desirable that can advise on the ethical side of the digitization society. If we look at how the governance ecosystem for the social and ethical side of digitization works, we see that action is required in all the various areas where we previously had committees (fundamental rights, advice, debate, review – see chapter 4).

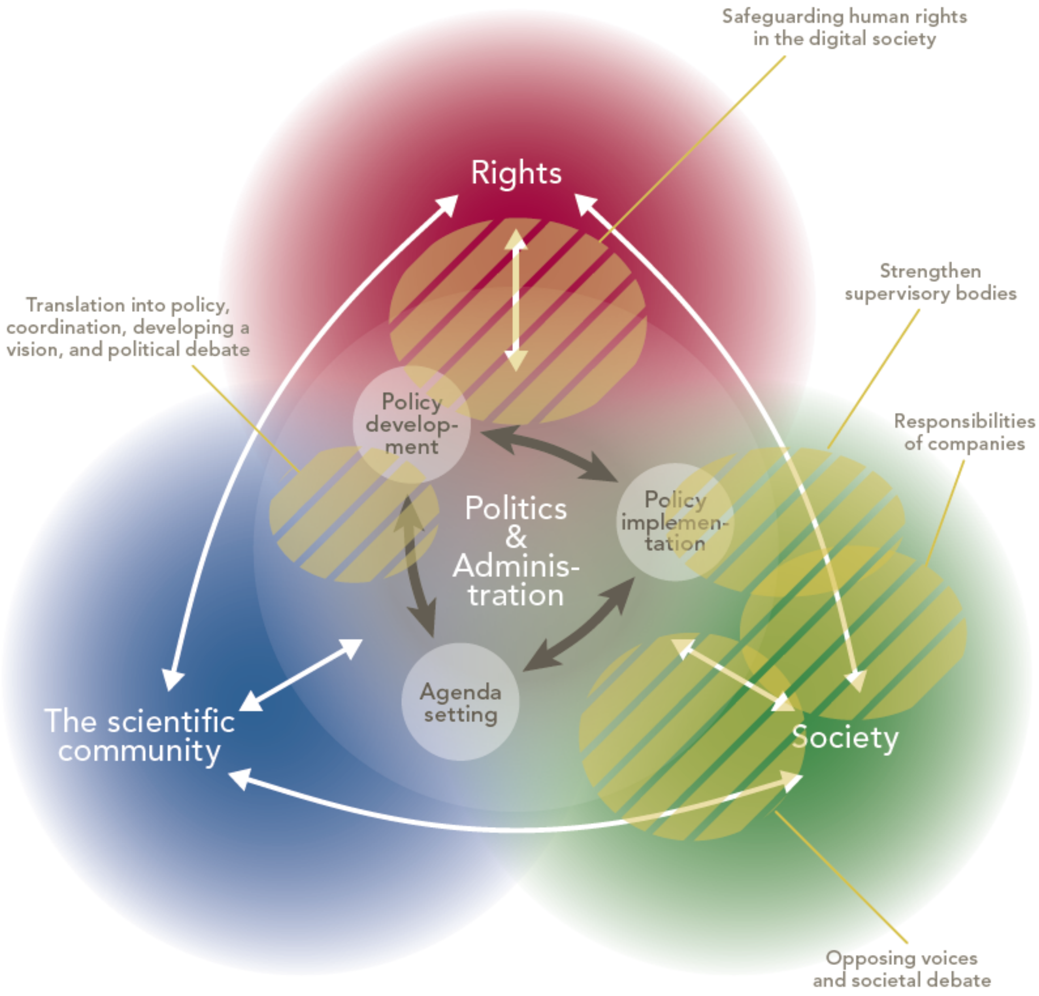
In various places we notice initiatives attempting to get to grips with new and emerging ethical and societal issues. At an international level, the discussion is filtering through to the domain of human rights. There we see an upsurge in the discussions on the impact of new technologies such as AI and robotics on fundamental rights. In the Netherlands, except in universities, the discussion has not yet reached the political-administrative domain. The same applies to the public debate. Broader civil society in the Netherlands is mainly involved in issues such as privacy, data protection and digital security.

Our investigation shows that wide-ranging ethical and social issues form the list of items that make it to the political-administrative agenda. The step to policymaking and political decision making, however, is still a formidable hurdle. There is political awareness of the impact van digitization, but the debate is mostly driven by incidents. Finally, we pose the question, to what extent can the current review regime adequately continue to institutionally safeguard important human values and rights in the digital age. In conclusion, we find the five following blind spots (see Figure 5.1):

- The translation of new social and ethical issues into policy, interdepartmental consultation on digitization; and the political debate on new issues.
- The safeguarding of fundamental and human rights in the digital society.
- Strengthening supervisory bodies and ensuring mutual agreement.
- New responsibilities for developers of digital services and products.
- Organizing public debate and 'opposing voices': strengthen civil society, citizens' knowledge and skills and public debate on digitization.

On account of these blind spots in the governance landscape, the protection of essential public values in the digital society is currently falling short. A structural approach is required to substantially strengthen the governance landscape in these five areas in order to cope with the social and ethical challenges of the digital society and adequately protect Dutch citizens. We will elaborate on this approach in the following chapter.

Figure 5.1 Blind spots in the governance landscape


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

Rathenau Instituut

6 Conclusion: Safeguarding public values in the digital society

6.1 Introduction

At the request of the Ministry of the Interior and Kingdom relations and the Senate, Rathenau Instituut studied the social and ethical issues that arise due to the digitization of society, and whether it is desirable to have a committee that can advise on these matters. This was as a result of a motion tabled by Gerkens, a member of the Senate (motion Gerkens 23 September 2014, see box). This motion refers to the emergence of the Internet of Things that poses opportunities as well as threats. The motion confirms the feeling in the Senate that digitization is compromising important values, underlined by the fact that they talk not only about the technological effects of digitization, but also the 'social, socio-legal and socio-psychological' implications. This study by Rathenau Instituut confirms the Senate's observations.

Box 6.1 Motion tabled by Senator Gerkens on 23 September 2014

The Senate, having heard the deliberations, concludes that the digital technology involved in '*The Internet of Things'* will connect everything and everyone with each other; it further concludes that this unstoppable development will present opportunities for society, but also threats; it considers that the impact of this digital development on society is not just technological, but also societal, socio-legal and socio-psychological; it asks for the government to request that Rathenau Instituut investigates the desirability of a committee which can advise on the ethical aspects of digitalising society, and proceeds with the days' agenda.

Signed by Senators Gerkens, Franken, K.G. de Vries, Strik, Duthler, Van Boxtel.

The motion asks whether it is desirable to have a committee that can advise on the ethical aspects of the digitizing society. That question indicates the underlying concerns in the Senate about whether the current legal frameworks, review arrangements and social resilience still have adequate powers to deal with the emerging ethical and social issues surrounding digitization. In this study we have approached the question in the motion from the perspective of these underlying concerns. We investigated which technologies are expected to shape digital society in the coming years, and which social and ethical challenges they will bring. Subsequently we studied to what extent the approach to dealing with these challenges is also institutionally embedded, or rather we investigated the *governance* of ethical and social challenges concerning digitization. The key sub-questions we posed were: how did people deal with social and ethical issues arising from technological developments in the past? How do we shape the current governance landscape surrounding social and ethical digitization issues? To which issues are Dutch institutes and actors responding or not, and in what way? Can we identify blind spots? What role can a committee play? The motion does not go into detail about what type of committee is meant. For our analysis we have therefore looked at what sort of committees in the past dealt with ethical and societal issues concerning technology, and what role they fulfilled in governance.

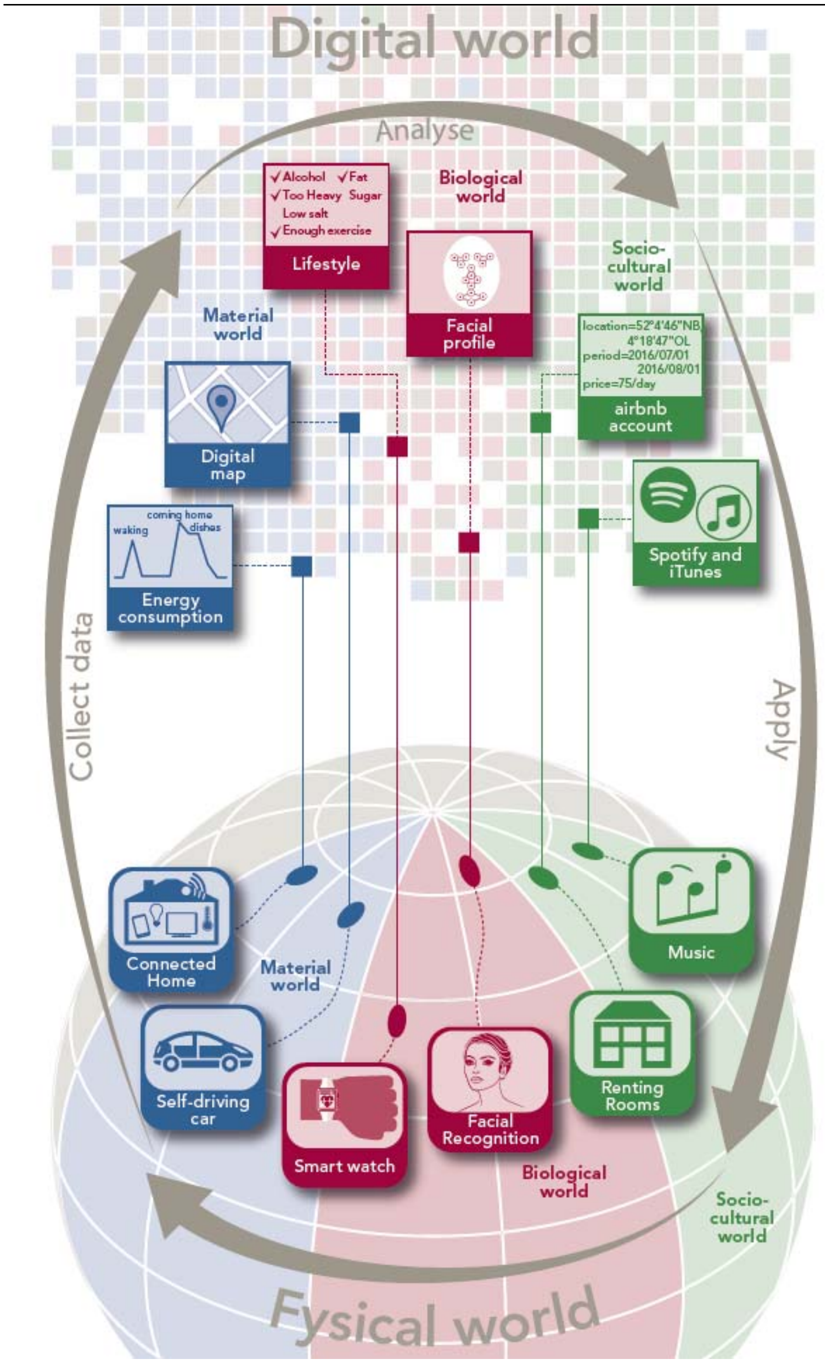
In this chapter we first briefly summarize our study findings. In section 6.2 we discuss the technology areas that are creating a new phase in the digitizing society. The ensuing major social and ethical issues are described in section 6.3. Then section 6.4 takes a look back at the most important lessons from the past on building up a governance landscape around social and ethical issues in technology. In section 6.5 we point out where the blind spots have occurred in the governance landscape around social and ethical digitization issues. On this basis, section 6.6 proposes actions for various players, and we answer the question whether it is desirable to have a committee that can advise on societal and ethical issues in the digitizing society.

6.2 A new digital wave: digitization as cybernetization

The terms digitization and Internet of Things in the Gerkens motion refer to a large cluster of digital technologies. Chapter 2 listed eight areas of technology that are expected to shape the digital society in the coming years: robotics, Internet of Things, biometry, persuasive technology, digital platforms, augmented reality and virtual reality, artificial intelligence, big data and algorithms. Together they are presenting a new wave of digitization. More and more parts of our physical world are being represented virtually.

Chapter 2 showed that the digitization of the biological, material and socio-cultural world is resulting in an expanding digital world. There is continual feedback between the physical and digital world, whereby products or services are directly modified based on an analysis of digital data (see Figure 6.1). Think of the smart energy meter in a *connected home*, which measures the occupants' energy consumption, analyses it digitally, and based on that profile, subsequently adjusts the thermostat. Think of the smartwatch, which keeps track of the wearer's activities, analyses these and gives personal advice on the user's lifestyle. Or think of the new digital platforms for hiring rooms or taxis, which (in the case of Uber) continually measure and analyse supply and demand, and thus use smart software dynamically to adjust prices and control that supply and demand.

Figure 6.1 Cybernetic loop between the physical and digital worlds



Rathenau Instituut

Although digitization has been going on for decades, we say in chapter 2 that we are on the brink of a new phase in our digital society. This new phase has as distinguishing features: a *cybernetic loop* (collecting data), profiling (analysing data) and intervention (applying data). This cybernetic loop makes it possible to (re)direct realtime in the physical world and create an increasingly major starting point for new digital services and products.

The cybernetic *feedback loops* between the physical and digital world are visible in all sorts of areas: the production process, the environment, our bodies and our behaviour. They come in the form of data surveillance on the Internet that dishes up 'appropriate' information, news feeds, products or prices based on users' surfing behaviour. They are the train manufacturers who use sensors to continually measure and analyse train engines' performance, and can thus determine where to place their rail engineering technicians. They are the smart street-lights that 'measure' aggression and use light to try and influence the atmosphere. In the public sector we see for example digital learning platforms that track pupils, and on the basis of their performance, offer new tasks. Or police officers carry out extra patrols based on big data reports that show where many burglaries or acts of violence have been committed previously.

6.3 Public values at stake

The new wave of digitalization and the ensuing cybernetic loop bring new social and ethical challenges. Important public values are at stake, closely linked to fundamental and human rights. These include the right to equal treatment, privacy, autonomy and human dignity. You can also see in chapter 3 that the three processes in the cybernetic loop evoke different societal and ethical issues (see table 6.1).

The process of data collection and processing – measuring – is the main reason people are discussing privacy protection. The enhanced opportunities to collect and process (new) data are posing a threat to new dimensions of privacy. One example is emotion recognition technology, which is causing concern regarding the protection of mental privacy: the freedom to think and feel what you want. The advances in the Internet of Things force us to radically review our understanding of privacy, for example regarding the home as private domain and organizing our physical safety. Related to privacy, there are ongoing discussions about the ability to develop an independent identity into an autonomous individual in a world of continual digital monitoring.

The process of data analysis – profiling – and the new techniques that are applied for this such as self-learning algorithms, are causing concern for example regarding the right to equal treatment and the role of people versus computers. Software is playing a more and more dominant role in making decisions about people. Does someone fit the profile or not? Is someone a credit risk or not? Knowingly or unknowingly, *data analytics* provide undesirable forms of exclusion and discrimination. Software programmes assist judges in the US by calculating the chance that a suspect will reoffend. This can cause discrimination and incorrect conclusions to be drawn. Moreover, using data analytics can result in a *bias* in the analysis. Applying software to determine where extra police presence is required can lead to a self-fulfilling prophecy: where there is more police, you see more offences. The computer integrates the data again in its analysis, which makes the programme expect to see more criminality at that location. And because technology is taking over human decisions, we should ask ourselves what this means for the autonomy of individuals, and what possibilities the individual has to rectify an automatic system's incorrect decisions.

During the feedback process to the physical world – intervention and (re)directing – discussions arise about how far the technological influence may go, how to protect autonomy, and who to what extent still has control of the technology. Deploying robots and software in health care, justice, banking and other sectors, also raises the urgent question of what we want to let robots do, and what the minimum human involvement must be, if we want to think in terms of meaningful, dignified care or being held accountable. Another factor is that public services are becoming increasingly dependent on software developed by private parties, making it difficult to find out what choices the software makes and the potential impact. Will the judge or doctor in one county who uses system X reach different conclusions than another judge or doctor who uses system Y?

Table 6.1 Social and ethical issues in relation to the cybernetic loop in digitization

	Collect (measure)	**Analyse (profile)**	**Implement (intervention)**
Privacy	▨	▨	
Security	▨		
Autonomy	▨	▨	▨
Equity and inequality		▨	▨
Human dignity			▨
Control of technology			▨
Balance of powers	▨	▨	▨

Rathenau Instituut

6.4 Lessons from the past

In chapter 4 we looked at how the social and ethical aspects of science and technology were dealt with in the past, focussing on four areas: biotechnology, ICT, clinical trials and animal experiments. This resulted in a conceptual framework of how a governance ecosystem for science and technology should look, which parties and institutes play a role, and how this system develops. Obviously in order to answer the question in Senator Gerkens' motion, (whether it was desirable to have a committee advising on the ethical aspects of digitalization), it was relevant to examine not just a partial aspect of the governance system but also a broad gamut of governance activities in the areas of digitization, ethics and society.

Our review of past practices highlights that societal discussion on the significance of new technology only takes place once the applications of that technology are widely visible in society, and that it still takes many years, sometimes decades, before an adequate governance system gets off the ground. We also saw that in the past, various types of committees, with diverse roles, were established to consider the governance of ethical and social issues in technology. The state commission Franken for example advises the government on amending the Constitution, or advisory committees such as the Rathenau or DNA commissions who advise the government on specific technological developments, or committees that aim to organize social dialogue such as the Commission for Social Dialogue on Nanotechnology, or review committees that regulate and supervise research, such as the Central Committee for Human Research (CCMO), that expresses views on clinical trials and embryo research.

Finally our historical review showed that the Gerkens motion ties in with a parliamentary tradition to question the sustainability of the existing governance system for societal and ethical issues in technological developments. In recent decades, parliament has spoken several times about the adequacy of how the political administration deals with societal and ethical issues pertaining to science and technology. This usually followed new breakthroughs in science or technology.

6.5 Blind spots in the governance of ethical and social digitization issues

In chapter 5 we applied the conceptual framework to digitization issues. This charted the initiatives, actions and actors in the governance landscape and how they deal with various societal and ethical issues. It is clear that blind spots exist all over the governance landscape. The actors clearly identify certain issues and work on initiatives connected with the first two processes in the cybernetic loop (measuring and profiling). In recent years, privacy, data protection and online security have become the most hotly debated aspects of digitization. Consequently, over the years a governance system has been formed, equipped with scientific knowledge on the significance of new digital technologies for privacy, and where policymakers translate these issues into policies, laws and regulations. There are supervisory and enforcement bodies, while social organizations actively work on topics like privacy and security. This governance system is certainly not yet fully developed, as demonstrated by the requests in parliament for policy visions on privacy, or the calls for tighter supervision and stronger societal debate on these topics. Actors in the governance system are being challenged by the new privacy and security issues. Major new challenges include digital inviolability of the home and protecting personal privacy and security with the emergence of the Internet of Things.

For other social and ethical issues linked to developments in AI, robotics and the Internet of Things, the governance system is less well established. We see increasingly more interest in justice issues especially algorithmic profiling, the impact of the right to equal treatment and the presumption of innocence. Regarding the unequal distribution of power, increasingly more discussions are taking place about the dominant position of large internet companies. The topics autonomy, human dignity and control of technology are scarcely addressed by social organizations. These new issues are being studied at a scientific level and flagged up by policymakers (for agenda setting), but it is not yet clear how these issues should be translated into concrete policies. The step to political decision making is therefore still a challenge. Political awareness of the impact of digitization is visible, but the debate is mainly driven by incidents. Ultimately it is obvious that the current supervisory regime is not institutionally adequate to (continually) safeguard human values and rights in the digital era.

The five areas in the governance landscape where we identified blind spots are:

1. Translating new societal and ethical issues into policy, inter-ministerial consultation and coordination on digitization and the political debate on these new issues.
2. Safeguarding fundamental and human rights in the digital society.
3. Strengthening supervisory bodies and ensuring they consult each other.
4. New responsibilities for companies developing digital services and products.
5. Enabling ‘opposing voices’ and societal debate: strengthening civil society, citizens’ knowledge and skills and the public debate on digitization.

These blind spots demonstrate that the protection of fundamental public values is currently falling short. That is why for now and for the future, these essential values require a structural and integrated approach to address the governance of social and ethical issues and thus offer Dutch citizens adequate protection. It is not always necessary to create new rules. Digitization often leads to conceptual confusion about which rules are relevant, and about how these should be applied. For that reason we see instances of existing standards, rules and (legal) frameworks not being (initially) implemented even though they are applicable. The Human Environment and Transport Inspectorate regulating the UberPop service proves that existing frameworks also apply to new digital services. In other cases we see that digitization requires new frameworks for the way in which important values are safeguarded in the digital society. For example, a new fundamental right is needed to protect human contact meaningfully in a care environment that is becoming further digitized (see Van Est en Gerritsen 2017). In the next section we explain, based on our analysis, which measures are required to safeguard public values in the digital society.

6.6 Upgrade: an action programme for a responsible digital society

Digital innovations are evolving at such an incredible pace that digitization is now running in the veins of society. The ongoing technical upgrades create a host of new opportunities for the economy and society. But they also lead to fundamental societal and ethical issues. Consequently, the digitization of society is putting pressure on essential public values. Every sector of our society is facing digitization issues and the accompanying ethical and societal challenges. It is time to sit up and take notice of the impact that digitization is having on society and do something about ensuring that public values and fundamental rights are safe. This requires an upgrade or enhancement of the current governance system. This enhancing implies a much-needed strengthening of the governance landscape by structurally securing social and ethical values.

Such an enhancement needs all the parties in society to make a collective effort and put digitization on the right track. It is irresponsible for government, the business community and society to turn a blind eye to the fundamental impact of digitization. The responsibility lies with all these actors to deal with the societal and ethical aspects of digitization. Although the government needs to launch such an action programme, the business world and civil society should be taking steps at the same time.

Our main conclusion then is that the Senate's concerns stated in the Gerkens motion, on the ethical and societal impact of digitization, are justified. Regarding the desirability to set up a committee to advise on these issues, our analysis shows that in order to safeguard **essential public values, the governance of several societal and ethical areas of digitization should be substantially strengthened**.

Setting up a committee will not solve the problems identified in our analysis. In the 1970s and 1980s, a few scientific experts on committees were asked to study societal and ethical issues in new technologies. By the 1990s, people were starting to take more notice of citizens' wishes and concerns. The committees included a broader range of experts so that they could conduct a better public debate. Addressing complex problems nowadays demands a joint commitment by multiple actors. After agreeing on a goal (for example to reduce CO2 emissions), the greatest challenge lies in determining how parties collectively can best go about implementing that goal. In the context of energy for example, more than forty parties signed up to an 'Energy Agreement', committing themselves to lower energy consumption.

One committee on its own would not be able to solve the blind spots in the governance landscape. A complex task like strengthening the governance system demands that all parties take responsibility and make a collective effort to safeguard public values in the digital society. The inherent risk of appointing a committee, is that practical issues will be 'parked' with the committee, while parties in the field and at political-governance level adopt (too much of) a wait-and-see attitude. Moreover, the present study has already completed much of the groundwork that a committee of this kind would normally carry out. The study identifies which societal and ethical digitization issues we are facing and the blind spots in the governance landscape we need to address. It also suggests a range of actions that all the parties involved could pursue to strengthen the governance system.

Accordingly, the Rathenau Instituut's key message is that the government, industry and civil society must take action now to strengthen the governance landscape, thus ensuring that public values in the digital society will continue to be properly safeguarded.

The five-part action programme we propose will enable policymakers, companies and civil society organizations to responsibly upgrade the governance landscape:

1. Appoint an interdepartmental working group charged with shaping the government's vision on addressing the societal and ethical significance of digitization, and with ensuring coordination in political governance.
2. Strengthen the role and position of supervisory bodies.
3. Draw up a 'Digitization Agreement' formulating the commitments 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 digitization for safeguarding public values.
5. Schedule regular political debates in the Senate and House of Representatives on the governance of societal and ethical digitization issues.

Each part is subdivided into a number of specific action points, which we explain below.

1. Appoint an interdepartmental working group charged with shaping the government's vision on addressing the societal and ethical significance of digitization.

Action points for the interdepartmental working group:

- Coordinate activities to develop an overarching vision of the societal and ethical impact of digitization and to safeguard public interests.
- Explore ways of safeguarding fundamental rights in the digital age. In this context, it is important to seek links with initiatives at European level, for example within the Council of Europe.

Coordination and creating a vision

Translating the identified ethical and societal issues into a coherent and cross-domain policy is a painstakingly slow process. To rise above the fragmented nature of the debate, an interdepartmental working group is needed. This working group can shape the government's vision on the governance of societal and ethical digitization issues, and incorporate this strategically into governmental structures. It can also ensure the coherence of any cross-domain policy issues and raise awareness within the government of the implications of digitization in terms of safeguarding public values. Moreover the group can encourage various ministerial departments to reflect and address the significance of emerging societal and ethical questions in their fields.

Safeguarding fundamental rights

In terms of what digitization signifies, the political-administrative domain is responsible for monitoring the safeguarding of fundamental rights. In the Netherlands, the discussions on protecting these fundamental rights have focused on whether and how the right to privacy, confidential communication and freedom of expression, should be modified in light of digitization. Recent initiatives at European level (by the Council of Europe and the European Parliament) are exploring the impact of technologies such as big data, AI, robotics, and the Internet of Things on the protection of fundamental rights. How can we continue to safeguard these rights in the digital era? In 1997, the Council of Europe initiated a separate treaty (Oviedo Convention) for biotechnology and genetic engineering. Despite the wide application of the European Convention on Human Rights, the Council of Europe found it necessary to focus on new scientific and technological developments; a balance has to be found between progress and human dignity. Now the question is whether we need a similar treaty to protect fundamental rights in the context of the new wave of digitization (Van Est & Gerritsen 2017). The Netherlands should also explore the significance of digitization for fundamental rights, noting (and seeking links with) European initiatives in this area. This, too, is a task for the interdepartmental working group.

2. Strengthen the role of supervisory bodies

Action points:

- Supervisory bodies: be aware of emerging societal and ethical issues.
- Supervisory bodies: based on the current mandate, explore ways of addressing these emerging issues: what rules apply, what tools do regulators have at their disposal, what capacity/knowledge is required?

- Supervisory bodies: in the context of collective consultations, agree on who is responsible for what, and take collective action where necessary.
- Government: incorporate conditions, and take on the role of launching customer.

Every regulator is facing new digitization issues, whether these involve privacy, discrimination, the balance of power, or human dignity. All the regulators such as the Personal Data Authority, the Consumer and Market Authority, the Human Rights College, the Human Environment and Transport Inspectorate or The Dutch Healthcare Authority should familiarize themselves with the question of how, in their own fields and within the scope of their current mandate, they can address emerging ethical and societal digitization issues in practice. Close coordination is vital. As digitization spans a wide range of sectors, the different regulators' enforcement domains will often overlap. Regulators should therefore update one another on what digitization issues they are facing, on how regulation is organized, and where the focus of their individual areas of responsibility lies.

The Personal Data Authority and the Consumer and Market Authority have already carved out clear roles for themselves in privacy and data protection. However, they too are having to deal with new issues. For example the European Data Protection Supervisor is examining its role regarding the ethics of digitization. It is not only looking at newly emerging issues, but also how it can address these issues under its current mandate.

The supervisory bodies' roles are less sharply defined for issues such as discrimination through software, the application of software, robots and maintaining human dignity, and the growing power struggles between consumers, industry and government. For example, who supervises the potential discriminatory effects of software programmes? Who identifies whether the various producers' software programmes may be giving different advice on the likelihood of reoffending, or on the diagnosis of diseases?

Familiarization with digital issues does not necessarily mean that a new regulator, or a new legislative framework, is needed. Existing regulatory frameworks often provide adequate scope or act as a starting point. For instance, General Data Protection Directive 95/46/EC and its successor – the General Data Protection Regulation – provide a framework for scrutinising decisions made automatically by algorithms.[93] Sometimes a regulator's current mandate and tools will suffice, on other occasions adjustment may be required.

To strengthen the supervisory boards' position, important factors to bear in mind are not only building up the awareness and capacity to deal with these new issues, but also questioning whether the pre-conditions are adequately fulfilled to achieve this. The government can set in place standard-setting frameworks – systems need to comply with these regulatory frameworks regarding purchase, design and structure. Supervisory bodies and enforcers can use them as reference to review IT systems from businesses and government organisations. For example, governments

[93] Article 15 of the Directive 95/46/EC, the so-called 'Kafka provision', prohibits certain fully automated decisions with far-reaching effects, which are not only 'legal effects' but also decisions that 'significantly affect a person'.Article 13-15 of the GDPR mandates that data subjects receive meaningful information about the logic involved in automated processing. Article 22 states that individuals have the right not to be subject to a decision solely based on automatic processing . Discussions are ongoing about the limitations of these articles and whether or not they provide a feasible 'right to explanation' (see for example Wachter et al. 2017).

could determine transparency requirements for automated or self-learning algorithms, in order to hold software developers accountable for the operation of such systems. This would enable software developers to incorporate such features into their system design at an early stage.There is even a greater need to specify requirements for (semi)public services and digital systems in healthcare, education, the justice system and so forth. The government should act as custodian of public interests. Due to increasing *servitization* (whereby products are offered as services, see chapter 3), public service systems are mostly in the hands of private parties, and consequently the government, supervisory and enforcement bodies have neither a sufficient overview of the operations and effects of these systems, nor the possibility to manage them. It should be possible to control the system's design and its effects. The government must take these possibilities into account when contracting digital systems and determine conditions beforehand.

3. Draw up a 'Digitization Agreement' formulating the commitments and responsibilities of businesses, government and civil society actors with regard to safeguarding public values in the digital society.

Action points for the Digitization Agreement:

- Businesses: give priority to the duty of care, bearing in mind societal and ethical issues with digital products and services.
- Businesses and trade associations: develop practical ways of addressing the duty of care through codes of conduct.
- Businesses, trade associations and science: explore and learn from existing tools and structures that can help the business community deal with ethical impacts. Privacy impact assessments can serve as models for an ethical impact assessment.
- Government and science: invest through research funding and innovation policy in exploring and tackling the societal and ethical implications of new technology.
- Government: explore ways of strengthening opposing voices from non-governmental organizations and citizens (e.g. through class actions, or by exploring the pros and cons of revoking the ban on constitutional scrutiny).
- Government, businesses and civil society: expand digital skills in education (to young people and professionals)
- Government, businesses and civil society: expand media literacy (insight in workings of new technology).

Industry, civil society and citizens, together with government will have to take steps to safeguard public values in the digital society now and in the future. It is recommended that these parties make a joint 'Digitization Agreement', drawing up details of how they will collaborate to give the digital society a 'human face'. A wide support base of businesses and participating stakeholders is essential for drawing up this agreement. The process can be modelled on the approach to reach previous agreements, such as the Energy Agreement.

The importance of a 'Digitization Agreement'

For the Netherlands, it is crucial to conclude and implement such an agreement. As with biotechnology, societal and ethical issues become key success and failure factors for innovation. Failing to take timely action to protect public values can undermine the trust of consumers and citizens, and lead to failed innovations and costly processes. An example is when the Senate blocked two smart metering Bills (due to privacy concerns among other things), which significantly delayed the introduction of this equipment (Cuijpers and Koops 2012). If it was able find an appropriate way to safeguard public values in future IT innovations, the Netherlands could serve as a model for other countries and create opportunities for Dutch industry.

In various places we see recent collaborations and parties working hard to create 'the digital society'. What all the calls have in common, is their emphasis on establishing digitization in a responsible way, giving the Netherlands a unique opportunity to take the lead. They identify the current fragmentation in digitization policies on the part of the government, calling on more government direction. The development of digital literacy is a recurring theme. At the same time, only some of the necessary parties are represented in the existing calls or there is only a limited focus on social and ethical digitization issues. One example is the 'Manifesto: together towards a sustainable digital society'' signed by 27 parties (industry, knowledge institutions and umbrella organizations) during the annual ECP Congress on 17 November 2016 (VNO-NCW 2016). The manifesto draws attention to the importance of the sustainable digitization of society, and to concerns such as employment, cyber resistance and privacy. However, it contains no structural focus on the 'new' social and ethical digitization issues such as equal treatment, human dignity and autonomy. In addition, the signatories are mainly parties and (umbrella) organizations in industry or science, and are two organizations representing citizens' interests. Other calls come from specific sources, for example asking the employers organisations VNO-NCW Netherlands, LTO-Netherlands and SMEs to make a 'digital quantum leap' in the Netherlands: make better use of the opportunities arising from digitization and continue to guarantee public interests through regulation (NL next level 2016). By public interests, they refer to employment, privacy and security, not yet the ethical and social effects across the board. Another call is from the world of science, namely the Association of Universities the Netherlands (VSNU) indicates that in the coming years they will be working on 'people-oriented information technology' and make particular mention of the topics privacy and security.

Many parties seem to be fully aware of the importance to reap the benefits of digitization in a responsible way, and are prepared to join forces to achieve this. The challenge lies in extending the existing initiatives, not only to calling for the protection of privacy and ensuring online safety, but also the protection of all the fundamental rights and public values that are affected by digitization. Along with this substantive broadening, it is also vital to extend the number of civil society organizations, especially including a stronger representation of organizations that promote the interests of citizens.

Steps to complete a Digitization Agreement

Any 'Digitization Agreement' should define and document the responsibilities of the parties concerned. Companies' responsibilities are an important element. IT products and services are no longer *gadgets*: they have a major impact on our society, affecting fundamental as well as human rights. IT developers have to be fully aware of the societal and ethical impact of their products, and should make every effort to protect human and fundamental rights. Corporate responsibility to respect human rights is incorporated in documents such as the OECD's Guidelines for Multinational

Enterprises. Businesses should actively work on identifying any risks of human rights violations by themselves (or parties in their supply chain), and where possible, prevent such violations.

International standards can be implemented in everyday practice by applying industry association codes of conduct. They give guidance on how to deal with societal and ethical issues. We can learn from existing structures and tools in the field of data protection, such as privacy impact assessments and privacy by design. For example, *ethical impact assessment* is a way of identifying societal and ethical bottlenecks other than privacy issues at an early stage of product development. The government can contribute by specifically creating sufficient scope in its research funding and innovation policy to address the societal and ethical implications of new technology (Hessels en Deuten, 2012).

In addition, the Digitization Agreement should focus on promoting 'technological citizenship'. This could be achieved in practice by expanding media literacy in education and creating scope for programming and other digital skills. It applies not only to future citizens' primary and secondary education, but precisely for training today's professional people. From healthcare to the judicial system, it is important that professionals are aware of how the new wave of digitization is impacting public values.

Finally, it is important that the Agreement documents ways to more effectively support non-governmental organizations (NGOs) and citizens' counter-arguments, for example through class actions, or that it examines the desirability to lift the ban on constitutional review.

4. Hold a national debate to strengthen technological citizenship

Action points:

- Government, industry and civil society: support technological citizenship by holding a national debate on emerging societal and ethical digitization issues.

The public debate on the societal and ethical significance of the new wave of digitization is still limited, particularly with regard to emerging issues such as equal treatment, human dignity, autonomy, and the new balances of power between companies and consumers, between companies and government, and between members of the public and government. This highlights the importance of organizing a national debate to address these developments. Although it is up to the government be the initiator and driving force, it does not need to be responsible for holding the debates. To be successful, the dialogue requires the cooperation of all the parties involved in the field. The experience gained from holding previous debates in the Netherlands, such as the public debate on nanotechnology, will prove useful.

The dialogue, together with encouraging digital skills, form the core of technological citizenship (see above). This means that citizens are aware of the technological culture around them and understand how that technology impacts their daily lives (Van Est 2016). 'Technological citizens' know how the technology works, can think critically about those workings and the significance for their environment, and on that basis make an informed choice about which technology they can, cannot or want to use. As a result, people understand for example how profiling and self-learning algorithms work, how that affects them, and that they are able to defend themselves against undesirable influences and choose alternatives. Technological citizenship therefore needs us to improve our societal awareness and encourage opinion-forming on the impact and meaning of the new wave of digitization.

5. Schedule regular political debates in the Senate and House of Representatives on the governance of societal and ethical digitization issues

Action points:

- Regular debates on the governance of societal and ethical digitization issues.

One knock-on effect of an overarching government vision for addressing the societal and ethical significance of digitization is that this subject will appear regularly on the political agenda. This will address the request from parliament that a periodic and systematic debate is held on societal and ethical digitization issues. That request is reflected in regular calls from the Senate and the House of Representatives, asking the government to formulate an integrated vision in areas such as privacy, or the role of ethics in innovation policy. The motions by Senator Gerkens (section 6.1) and Senator Ester (Parliamentary Papers I, 2013-2014, 33750 XIII) are examples of this. The latter asks the Ministry of Economic Affairs to report annually on the role of ethics in innovation policy and also endeavours to facilitate a systematically recurring political-ethical debate on this topic in the Senate. Up till now, the political debate has been mainly driven by incidents. Having the topic regularly on the government’s agenda (preferably not limited to a single committee) will transcend the debate’s current fragmentized and incidental character; then we can check whether the actions undertaken to strengthen the governance landscape have truly borne fruit: is the landscape sufficiently strengthened? Are there any new blind spots? Do we need more activities?

6.7 Finally

The digitization of society is entering a new phase. For all kinds of essential services and products, we make increasingly more use of digital technologies and we are becoming increasingly more dependent on digital systems: in healthcare, banking, media, education or the justice system. The emergence of the Internet of Things has blurred the distinction between online and offline: we are onlife. Big data and algorithms help to make decisions in the public and private sectors, from detecting fraud or the likelihood of reoffending, to medical diagnoses. In some areas, software is already taking over decision-making from people, for example with armed drones, or in smart cars. Persuasive technology, embedded in advisory apps on our smartphone of in smart street lights, influences our behaviour and autonomy in subtle ways.

This study shows that the new wave of digitization is putting pressure on public values. ICT services and products are no longer *gadgets*: they are having a radical impact on our society. It is time to recognise the implications and to ensure that our public values and fundamental rights are safeguarded in the new digital era. One important comment here is that technology in itself is never good or bad, or neutral (Kranzberg 1986). Technology can have diverse social and ethical implications, but these vary greatly depending on the context and practices in which the technology is used and how it is designed. The building blocks and the infrastructure for the new digital society are materializing now. But the governance system to deal with the resulting social and ethical issues falls short in several dimensions, as this study reveals. Roles and responsibilities have become vague in some areas. Although social and ethical issues appear on the agenda, they are not being translated into policies that protect public values in practice. Supervisory bodies do not have enough insight in the emerging digitization issues. Likewise, civil society organizations and citizens are not sufficiently aware of the new digital developments, nor do they realise how they will be affected; the possibilities to defend themselves are too limited.

At the same time we are obviously not sitting empty-handed. Existing standards, rules and laws can often be applied in the online world. The importance of protecting public values and fundamental rights is widely recognised; they are laid down in the Dutch Constitution, the EU Charter of Fundamental Rights and international treaties ratified by the Netherlands, such as the UN Universal Declaration of Human Rights (1948). The main task ahead of us is to effectively safeguard these widely acknowledged public values in our new digital society's everyday practices. Unless government, industry, civil society and members of the public act now, there is a risk that while we are trying to get to grips with the new digital world, the frameworks to protect public values are meanwhile losing their relevance.

Bibliography

Acquisti, A., R. Gross & F. Stutzman (2014). Face recognition and privacy in the age of augmented reality. In: *Journal of Privacy and Confidentiality* 6(2), Article 1.

AIV (2014) Het Internet. Een wereldwijde vrije ruimte met begrensde staatsmacht. No. 92. Den Haag: Adviesraad Internationale Vraagstukken.

Andorno, J. (2006) Global bioethics at UNESCO: In defence of the Universal Declaration on Bioethics and Human Rights. In: *J Med Ethics* 33(3), pp. 150–154.

Andrade, N. (2014) Computers are getting better than humans at facial recognition. In: *The Atlantic,* 09-06-2014.

Anthes, G. (2006) Bits to Atoms (and Atoms to Bits). In: *Computerworld*, 03-04-2006.

AP (2016) *AP Agenda 2016.* Den Haag: Autoriteit Persoonsgegevens.

Arkin, R. (2010) The Case for Ethical Autonomy in Unmanned Systems. In: *Journal of Military Ethics*, Vol. 9, Issue 4, pp. 332-341.

Barbry, E. (2012) The internet of things, legal Aspects: What will change (everything)… In: *Communications & Strategies* 87(3), pp. 83-100.

Benkler, Y. (2006) *The Wealth of Networks: How Social Production Transforms Markets and Freedo*m. New Haven: Yale University Press.

Bogaard, van den A., H. Lintsen, F. Veraart & O. de Wit (red.) (2008) *De eeuw van de computer: de geschiedenis van de informatietechnologie in Nederland.* Deventer: Kluwer – Stichting Historie der Techniek.

Borenstein, J. & Y. Pearson (2010). Robot caregivers: harbingers of expanded freedom for all? In: *Ethics and Information Technology* 12(3), pp. 277-288.

Boxsel, van, J.A.M. (red.) (1991) *Ethische aspecten van wetenschap en technologie.* Den Haag: NOTA.

Boyd, D. (2014) *It's Complicated: The Social Lives of Networked Teens*. New Haven, CT: Yale University Press.

Bresnahan, T.F. & M. Trajtenberg (1995) General Purpose Technologies. Engines of Growth? In: *Journal of Econometrics* 65, pp. 83-108.

Brinkman, B. (2015). Ethics and pervasive augmented reality: Some challenges and approaches. In: K.D. Pimple (red.), *Emerging Pervasive Information and Communication Technologies,* Dordrecht: Springer, pp. 149-175.

Bronstein, J., Tagliati, M., Alterman, R.L., Lozano, A.M., Volkmann, J., Stefani, A. et al. (2012) Deep Brain Stimulation for Parkinson Disease. An Expert Consensus and Review of Key Issues. In: *JAMA Neurology* 68(2).

Brynjolfsson, E. & A. McAfee (2014). *The Second Machine Age. Work, Progress, and Prosperity in a Time of Brilliant Technologies*. New York: WW Norton.

BSI (2016) Robots and robotic devices. Guide to the ethical design and application of robots and robotic systems. BS 8611:2016. London: BSI.

Burkeman, O. (2014) Can I increase my brain power? In: *The Guardian*, 04-01-2014.

Carr, N. (2010) *The Shallows. What the Internet Is Doing to Our Brains*. New York: W.W. Norton.

Castells, M. (1996) *The Rise of the Network Society. The Information Age: Economy, society and culture* 1. Cambridge, MA: Blackwell Publishing Ltd.

Cate, F., P. Cullen & V. Mayer-Schönberger (2014). *Data Protection Principles for the 21st century: Revising the 1980 OESO guidelines*'. Oxford: Oxford Internet Institute

Citron, D.K. & F. Pasquale (2014) The scored society: Due process for automated predictions, *Washington Law Review* 89(1).

Coeckelbergh, M. (2010). Health care, capabilities, and AI assistive technologies. In: *Ethical Theory and Moral Practice* 13(2), pp. 181-190.

College voor de Rechten van de Mens (2015) *Strategisch Plan 2016-2019*. Utrecht: College voor de Rechten van de Mens.

Compen, N., J. Ham & A. Spahn (2014) Duurzaamheidscoaches. Een beter milieu begint met jouw coach. In: L. Kool, J. Timmer & R. van Est (red.) *Eerlijk advies – De opkomst van de e-coach*. Den Haag, Rathenau Instituut, pp. 111-128.

Cuijpers, C. M. K. C., & Koops, E. J. (2012). Smart metering and privacy in Europe: Lessons from the Dutch case. In S. Gutwirth, R. E. Leenes, P. de Hert, & Y. Poullet (Eds.), *European data protection: Coming of age*. (pp. 269-293).

D66 (2016) *Concept-verkiezingsprogramma. Samen sterker – kansen voor iedereen*. Den Haag: D66.

Datta, A. & M.C. Tschantz, & A. Datta (2015) Automated experiments on ad privacy settings. A tale of opacity, choice, and discrimination. In: *Proceedings on Privacy Enhancing Technologies*, 2015(1), pp. 92–112.

De Hert, P.J.A. & A.C.J. Sprokkereef, (2012) Second generation biometrics: The ethical, legal and social context. In: E. Mordini & D. Tzovaras (red.) *Biometrics, Privacy and Agency*, Berlijn: Springer, pp. 81-101.

De Vriend, H. (2006) *Een Raad voor Ethiek en Biotechnologie: Verslag van een conferentie (Den Haag, 4 december 2006).* Rijswijk: LisConsult.

Deloitte (2014) *De impact van automatisering op de Nederlandse arbeidsmarkt. Een gedegen verkenning op basis van Data Analytics.* Deloitte

Diakopoulos, N. (2016) Accountability in algorithmic decision making. In: *Communications of the ACM* 59(2), 56-62.

Dijk, van J. (1997) *De netwerkmaatschappij. Sociale aspecten van nieuwe media*. Houten: Bohn Stafleu Van Loghum

Dotson, T. (2014) Authentic virtual others? The promise of post-modern technologies. In: *AI & Society* 29(1), pp. 11-21.

Dratwa, J. (Ed) (2014) Ethics of Security and Surveillance Technologies. Opinion No 28 of the *European Group on Ethics in Science and New Technologies*. Brussels, 20 May 2014.

Dwoskin, E., Rusli, E. (2015) The Technology that Unmasks Your Hidden Emotions. In: *Wall Street Journal*. 28-01-0215. wsj.com/articles/startups-see-your-face-unmask-your-emotions-1422472398#:bLk8dH_DkLSJvA

EC (2011) *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*. https://ec.europa.eu/anti-trafficking/publications/european-commission-sector-guides-implementing-un-guiding-principles-business-and-hum-0_en

EDPS (2015) Towards a new digital ethics: Data dignity and technology, *Opinion* 4/2015. Brussels: European Data Protection Supervisor.

EDPS (2016) *Press Release: EDPS starts work on a New Digital Ethics,* EDPS/2016/05. Brussels.

Eskens, S., J. Timmer, L. Kool, & R. van Est (2016) *Beyond control. Exploratory study on the discourse in Silicon Valley about consumer privacy in the Internet of Thing*s. The Hague: Rathenau Instituut.

Est, R. van, D. Stemerding, V. Rerimassie, M. Schuijff, J. Timmer & F. Brom (2014) *From Bio to NBIC convergence – From Medical Practice to Daily Life*. Report written for the Council of Europe, Committee on Bioethics. The Hague: Rathenau Instituut.

Est, R. van, & L. Kool (ed.) (2015) *Werken aan de robotsamenleving. Visies en inzichten uit de wetenschap over de relatie technologie en werkgelegenheid.* The Hague: Rathenau Instituut.

Est, R. van, & V. Rerimassie (2014) *Strijd om onze intimiteit. Het Bericht.* Den Haag: Rathenau Instituut.

Est, R. van, m.m.v. V. Rerimassie, I. van Keulen & G. Dorren (2014). *Intieme technologie. De slag om ons lichaam en gedrag.* Den Haag: Rathenau Instituut.

Est, van R., & Kool, L. (ed.) (2015) *Werken aan de robotsamenleving. Visies en inzichten uit de wetenschap over de relatie technologie en werkgelegenheid*. Den Haag, Rathenau Instituut.

Est, R. van, J. Timmer, L. Kool, N. Nijsingh, V. Rerimassie & D. Stemerding, (2016) *Rules for the digital human park. Two paradigmatic cases of breeding and taming human beings: Human germline editing and persuasive technology*. Background Paper for the 11th Global Summit of National Ethics Committees, Berlin.

Van Est, R. en Gerritsen, J., with the assistance of L. Kool (2017). *Human rights in the robot age. Challenges arising from the use of robotics, artificial intelligence, virtual and augmented reality*. Export report written for Council of Europe, Parliamentary Assembly, Committee on Culture, Science, Education and Media. Rathenau Instituut: The Hague.

Van Est, R. (2016). *Technologisch burgerschap als dé democratische uitdaging van de eenentwintigste eeuw.* Christen Democratische Verkenningen. 2016(3). Amsterdam: Boom Uitgevers.

Floridi, L. (red.) (2013) *The Onlife Manifesto. Being Human in a Hyperconnected Era*. New York: Springer Publishing.

Fogg, B.J. (2002) *Persuasive Technology: Using Computers to Change What We Think and Do.* Boston: Morgan Kaufmann.

Ford, M. (2015) *The Rise of the Robots. Technology and the Threat of a Jobless Future*. New York: Basic Books.

Frenken, K., T. Meelen, M. Arets & P. van de Glind (2015).Wat is nu eigenlijk deeleconomie? In: *Me Judice*, 27 March.

Frey, C.B. & M.A. Osborne (2013) *The Future of Unemployment. How Susceptible Are Jobs to Computerization.* Oxford: Oxford Martin Publication.

Future of Life Institute (2015) *Autonomous Weapons: An open letter from AI & Robotics researchers,* futureoflife.org/open-letter-autonomous-weapons/

Gartner (2015). *Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015*. Gartner Press Release. November 10, 2015. gartner.com/newsroom/id/3165317

GCIG (Global Commision on Internet Governance) (2016) *Our Internet.* Ontario / London: Centre for International Governance Innovation / Chatham House.

Geser, H. (2010). Augmenting things, establishments and human beings. In: *Sociology in Switzerland: Towards Cybersociety and Vireal Social Relations* (Zurich, March 2010) (socio.ch/intcom/t_hgeser24.pdf).

Gezondheidsraad (2006) *Betekenis van nanotechnologieën voor de gezondheid*. Den Haag: Gezondheidsraad.

Gibbs, S. (2014) Elon Musk: artificial intelligence is our biggest existential threat. In: *The Guardian.* 27-10-2014.

Gibbs, S. (2015) Samsung's voice-recording smart TVs breach privacy law, campaigners claim. In: *The Guardian*, 27 February 2015. theguardian.com/technology/2015/feb/27/samsung-voice-recording-smart-tv-breach-privacy-law-campaigners-claim

Gillespie, T. (2014). The relevance of algorithms. In: T. Gillespie, P.J. Boczkowski & K.A. Foot (eds.) *Media Technologies: Essays on Communication, Materiality, and Society*. MIT Press Scholarship Online (doi:10.7551/mitpress/9780262525374.001.0001).

Goodall, N.J. (2014). Ethical decision making during automated vehicle crashes. Transportation Research Record. In: *Journal of the Transportation Research Board* 2424, pp. 58-65.

Goodwin, T. (2015) The Battle Is for the Customer Interface. In: *TechCrunch*, 3 March 2015 techcrunch.com/2015/03/03/in-the-age-of-disintermediation-thebattle

Greenberg, A. & K. Zetter (2015). How the Internet of Things Got Hacked. In: *Wired*, 28 December 2015. Available online: wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked

Ham, J., C. Midden & F. Beute (2009) *Unconscious Persuasion by Ambient Persuasive Technology. Evidence for the Effectivity of Subliminal Feedback*. Edinburgh: Proceedings of Artificial Intelligence and Simulation of Behaviour Conference.

Harris, D. (2015) Google: Our new system for recognizing faces is the best one ever. In: *Forbes*, 17-03-2015.

Hawking, S., S. Russell, M. Tegmark & F. Wilczek (2014) Stephen Hawking: Transcendence looks at the implications of artificial intelligence - but are we taking AI seriously enough? In: *The Independent*. 01-05-2014.

Heimo, O.I., A. Hakkala & K.K. Kimppa (2012). How to abuse biometric passport systems. In: *Journal of Information. Communication and Ethics in Society* 10(2), pp. 68-81.

Helbing et al. (2015) Digitale Demokratie statt Datendiktatur. Digital Manifest. In: *Spektrum der Wissenschaft*, pp. 50-61.

Hern, A. (2014) Hacker fakes German minister's fingerprints using photos of her hands, *The Guardian*, 30-12-2014. theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

Hessels, L. en Van Deuten, J. (2012). *Coördinatie van publiek-privaat onderzoek. Van variëteit naar maatwerk.* Rathenau Instituut: Den Haag

Hildebrandt, M. (2012). The dawn of a critical transparency right for the profiling era. In: J. Bus (red.), *Digital Enlightenment Yearbook 2012*. Amsterdam: IOS Press. pp. 41-56.

Hildebrandt, M. (2015). *Smart technologies and the end(s) of law: Novel entanglements of law and technology*. Cheltenham, UK: Edward Elgar publishing.

Hildebrandt, M. (2016) Data gestuurde intelligentie in het strafrecht'. In E.M.L. Moerel, J.E.J. Prins, M. Hildebrandt, T.F.E Tjong Tjin Tai, G-J. Zwenne en A.H.J. Schmidt, Homo Digitalis. In: *Handelingen Nederlandse Juristen-Vereniging 146e jaargang/2016-I*, pp. 137-240, Wolters Kluwer, Beschikbaar op: njv.nl/wp-content/uploads/2011/04/Preadviezen-NJV-2016.pdf

Hill, K. (2015) This guy's light bulb performed a DoS attack on his entire smart house. In: *Fusion*, 03-03-2015. Online beschikbaar: fusion.net/story/55026/this-guys-light-bulb-ddosed-his-entire-smart-house/

Hilty, L.M. (2015) Ethical issues in ubiquitous computing – Three technology assessment studies revisited. In: K. Kinder-Kurlanda & C. Ehrwein Nihan (red.), *Ubiquitous Computing in the Workplace*. Dordrecht, Springer.

Hof, C van 't., C. Daemen, R. van Est (red.) (2010) *Check-in, check-out. De digitalisering van de openbare ruimte.* Den Haag: Rathenau Instituut.

Hof, C. van 't, J. Timmer & R. van Est (red.) (2012a) *Voorgeprogrammeerd: hoe internet ons leven leidt*. Boom Lemma.

Hof, C. van 't, J. Timmer & R. van Est (2012b) *Het Bericht: Voorgeprogrammeerd – Online keuzevrijheid onder druk*. Den Haag: Rathenau Instituut.

IBM (2013). *IBM Research Unveils Two New Watson Related Projects from Cleveland Clinic Collaboration*. ibm.com/press/us/en/pressrelease/42203.wss

IDC (2011) *Extracting Value from Chaos*, IDC Digital Universe study. Online beschikbaar: emc.com/about/news/press/2011/20110628-01.htm

IDC (2014) *Digital Universe of opportunities: Rich data and the increasing value of the Internet of Things*. IDC Digital Universe study.

IEEE (2016) *The Global Initiative for Ethical Consideration in the Design of Autonomous Systems*. IEEE. standards.ieee.org/develop/indconn/ec/ec_about_us.pdf
is-all-for-the-customer-interface/

Ismail, I., M.S. Malone & Y. van Geest (2014) *Exponential Organizations. Why New Organizations Are Ten Times Better, Faster, and Cheaper than Yours (and What To Do About It).* New York: Diversionbooks.

ITU (2005) *The Internet of Things.* itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf

Janssen, A., L. Kool, en J. Timmer (2015) *Dicht op de huid. Gezichts- en emotieherkenning in Nederland.* Den Haag: Rathenau Instituut.

Juul, N.C. (2015) Recommendation on the use of biometric technology. In: P. Campisi (red). *Security and Privacy in Biometrics*. Londen, Springer Verlag, pp. 415-433.

Kaptein, M. & D. Eckles (2012) Heterogeneity in the Effects of Online Persuasion. In: *Journal of Interactive Marketing* 25, pp. 176-188.

Kaptein, M., Markopoulos, P., Ruyter, B. de, Aarts, E. (2015) Personalizing persuasive technologies: Explicit and implicit personalization using persuasion profiles. In: *International Journal of Human-Computer Studies* 77, pp. 38-51. doi:10.1016/j.ijhcs.2015.01.004

Karppinen, P. & H. Oinas-Kukkonen (2013) Three approaches to ethical considerations in the design of behavior change support systems. In: *PERSUASIVE'13 Proceedings of the 8th international conference on Persuasive Technology*, Heidelberg, Springer-Verlag, pp. 87-98.

KEMO (2004) *Kerncommissie Ethiek Medisch Onderzoek (KEMO) 1993-1999*. Den Haag: KEMO.

Kiss, J. (2014) An online Magna Carta: Berners-Lee calls for bill of rights for web. In: *The Guardian*, 12-03-2014. theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web

Kizza, J.M. (2013) *Ethical and Social Issues in the Information Age*. Heidelberg, Springer.

KLPD – Dienst Nationale Recherche (2008) *Schone schijn: De signalering van mensenhandel in de vergunde prostitutiesector*. Driebergen: KLPD.

Knight, W. (2015) Inside Amazon’s Warehouse, Human-Robot Symbiosis. In: *Technology Review*. 07-07-2015. technologyreview.com/news/538601/inside-amazons-warehouse-human-robot-symbiosis

Kollanyi, B., P.N. Howard & S.C. Woolley (2016) Bots and Automation over Twitter during the First U.S. Presidential Debate. In: *Computational Propaganda Data Memo* 2016.1, 14-10-2016

Kool, L., J. Timmer & R. van Est (2014) *Eerlijk advies. De opkomst van de e-coach*. Den Haag: Rathenau Instituut.

Kool, L., J. Timmer & R. van Est (2015) *De datagedreven samenleving. Achtergrondstudie.* Den Haag, Rathenau Instituut.

Koops, E. J. (2011) Digitale grondrechten en de staatscommissie: Op zoek naar de kern. In: *Tijdschrift voor constitutioneel recht* 2(2), pp. 168-185.

Koops, E. J. & Prinsen, M. M. (2005) Glazen woning, transparant lichaam: een toekomstblik op huisrecht en lichamelijke integriteit. In: *Nederlands Juristenblad* 80(12), pp. 624-630.

Koops, E.J. (2014) Privacy, informatieveiligheid en een onzichtbare medaille. In: S. Kok et al. (red.) *Informatieveiligheid*. Taskforce Bestuur & Informatieveiligheid Dienstverlening, pp. 57-73.

Kosinski, M., D. Stillwell & T. Graepel (2013) Private traits and attributes are predictable from digital records of human behavior. In: *PNAS* 110(15), pp. 5802–5805.

Kramer, A.D.I, J.E. Guillory & J.T. Hancock (2014). Experimental evidence of massive-scale emotional contagion through social networks. In: *PNAS* 111(24), pp. 8788-8790.

Kreijveld, M., J. Deuten & R. van Est (red.) (2014) *De kracht van platformen. Nieuwe strategieën voor innoveren in een digitaliserende wereld*. Den Haag/Deventer: Rathenau Instituut/ Vakmedianet.

Ladikas, M., S. Chaturvedi, Y. Zhao & D. Stemerding (ed.) (2015) *Science and technology governance and ethics: A global perspective from Europe, India and China,* Heidelberg: Springer

Li, X., X. Hong, A. Moilanen, X. Huang, T. Pfister, G. Zhao & M. Pietikäinen (2015) *Reading Hidden Emotions: Spontaneous Micro-expression Spotting and Recognition.* arXiv:1511.00423 [cs.CV]

Louv, R. (2005) *Last child in the woods: Saving our children from nature-deficit disorder*. Chapel Hill, NC: Algonquin Books.

Maan, S., B. Merkus, J. Ham & C. Midden (2011). Making it not too obvious. The effect of ambient light feedback on space heating energy consumption. In: *Energy Efficiency* 4(2), pp. 175-183.

Madary, M. & T.K. Metzinger (2016) Real virtuality: A code of ethical conduct. Recommendations for good scientific practice and the consumers of VR-technology. In: *Frontiers in Robotics and AI* 3 (19 February).

Martijn, M. (2016) Deze professor probeert privacy opnieuw uit te vinden en dat is broodnodig. In: *De Correspondent,* 8 August. decorrespondent.nl/5043/Deze-professor-probeert-privacy-opnieuw-uit-te-vinden-en-dat-is-broodnodig/155102508-199b13c9

Mayer-Schonberger, V. & K. Cukier (2013) *Big Data: A Revolution that Will Transform How we Live, Work and Think*. Houghton: Mifflin Harcourt.

Meelen, T. & K. Frenken (2014) UberPop is geen voorbeeld van deeleconomie. In: *Het Parool*, 10 October.

Melson, G.F., P.H. Kahn, A. Beck & B. Friedman (2009) Robotic pets in human lives: Implications for the human-animal bond and for human relationships with personified technologies. In: *Journal of Social Issues* 65(3), pp. 545-569.

Meulen, van der, B. & A. Rip (1998) Mediation in the Dutch science system. In: *Research Policy* 27(8) pp. 757-769.

Michael, K. & M.G. Michael (2013) The future prospects of embedded microchips in humans as unique identifiers: the risks versus the rewards. In: *Media Culture and Society* 35(1), pp. 78-86.

Ministerie van Binnenlandse Zaken (2013) *Visiebrief digitale overheid 2017,* rijksoverheid.nl/documenten/kamerstukken/2013/05/23/visiebrief-digitale-overheid-2017

Misa, T.J., P. Brey & A. Feenberg (ed.) (2003) *Modernity and Technology*. Cambridge, MA: The MIT Press.

Moerel, L. (2015) Zo behouden alleen de rijken hun privacy. In: *NRC Handelsblad*, 28 november. nrc.nl/nieuws/2015/11/28/zo-behouden-alleen-de-rijken-hun-privacy-1561104-a579887

Morozov, E. (2013) *To Save Everything, Click Here: The Folly of Technological Solutionism*. London, PublicAffairs.

Mul, de, J. (1999) The Informatization of the Worldview. In: *Information, Communication & Society* 2(1), pp. 604-629.

Nanopodium (2011) *Verantwoord verder met nanotechnologie. Bevindingen maart 2009 – januari 2011*. Eindrapport Commissie Maatschappelijke Dialoog Nanotechnologie.

Negroponte, N. (1995) *Being Digital*. New York: Alfred A. Knopf.

NL next level (2016) *Investeren in een digitale kwantumsprong.* Uitgave van VNO-NCW, MKB-Nederland, LTO-Nederland, september 2016. nl-nextlevel.nl/wp-content/uploads/2016/09/de_digitale_kwantumsprong.pdf

Nouwt, J., P.H. Blok, B.J. Koops, M. Schellekens, E. Schreuders & M. de Vries (2000) Grondrechten in het digitale tijdperk. In: *Nederlands Juristenblad* 75(27), pp. 1321-1327.

NSOB & PBL (2014) *Leren door doen. Overheidsparticipatie in een energieke samenleving*. Den Haag. Den Haag: NSOB & PBL

O'Brolchain, F., T. Jacquemard, D. Monaghan, N. O'Connor, P. Novitzky & B. Gordijn (2016) The convergence of virtual reality and social networks: Threats to privacy and autonomy. In: *Science and Engineering Ethics* 22(1), pp. 1-29.

O'Reilly, T. (2005) *What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software*. 30/9/2005 oreilly.com/pub/a/web2/archive/what-is-web-20.html

OESO (2013), *Building Blocks for Smart Networks*, OECD Digital Economy Papers, No. 215, OECD Publishing. oecd-ilibrary.org/science-and-technology/building-blocks-for-smart-networks_5k4dkhvnzv35-en

Owen, R. P. Macnaghten & J. Stilgoe (2012) Responsible research and innovation: From science in society to science for society, with society. In: *Science and Public Policy* 39(6), pp. 751-760.

Pariser, E. (2011) *The filter bubble: What the Internet is hiding from you*. New York, Penguin Press.

Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge MA: Harvard University Press.

Peck, D. (2013) They're watching you at work. In: *The Atlantic,* December 2013. theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681

Peppet, S.R. (2014) Regulating the Internet of Things: First steps towards managing discrimination, Privacy, Security and Consent, 93. In: *Texas Law Review* 93, pp. 85-176.

Pereira, A.G., A. Benessia & P. Curvelo (2013) *Agency in the Internet of Things*. Luxembourg: Publications Office of the European Union.

Podesta, J., P. Pritzker, E. Moniz, J. Holdren & J. Zients (2014) *Big Data: Seizing opportunities, preserving values*. Washington: Executive Office of the President.

Poel, M. (2010) *Verbreding en vervlechting van het Nederlandse ICT-beleid. Rationale, beleidsinstrumenten en beleidscoördinatie*. Essay op uitnodiging van het Ministerie van Economische Zaken, Directoraat Generaal Energie en Telecom.

PWC (2013) *Omvang van identiteitsfraude & maatschappelijke schade in Nederland*. PricewaterhouseCoopers.

Radboud Universiteit (2016) *Bart Jacobs zet digitale beveiliging op de kaart*. ru.nl/onderzoek/over/vm/onderzoeksthema'/informatica-digitale/vm/professor-bart

Ramthun, S. & C. Schlesiger (2016) Dobrindt gründet Ethikkommission für automatisiertes Fahren. In: *Wirtschafts Woche*. wiwo.de/politik/europa/selbstfahrende-autos-dobrindt-gruendet-ethikkommission-fuer-automatisiertes-fahren/14513384.html

Rani, A. (2013) The Japanese men who prefer virtual girlfriends to sex. In: *BBC*, 24 October 2013. bbc.com/news/magazine-24614830

Renaud, K., A. Hoskins & R. von Solms (2015) Biometric identification: Are we ethically ready? In: *Information Security for South Africa (ISSA)*. Johannesburg, August, pp. 12-13.

Rerimassie, V. & F. Brom (2012) Science and technology ethics structure in the Netherlands. In: *Global Ethics in Science and Technology Deliverable D1.1 Ethics state of the art EU Debate*, p. 55-61.

Rli (2015) *Werkprogramma 2015-2016*. Den Haag: Raad voor de leefomgeving en infrastructuur.

Rli (2015a) *Verkenning technologische innovaties in de leefomgeving. Januari 2015*. Den Haag: Raad voor de leefomgeving en infrastructuur.

Rogers, B. (2015) The Social Costs of Uber. In: *The University of Chicago Law Review Dialogue* 82(85), pp. 85-102.

Roman, R., J. Zhou, & J. Lopez (2013) On the features and challenges of security and privacy in distributed Internet of Things. In: *Computer Networks* 57(10), pp. 2266-2279.

Royakkers, L. en R. van Est (2016) *Just ordinary robots. Automatation from love to war.* Boca Raton, FL: CRC Press.

RVS (2016) *Over de RVS*. raadrvs.nl/raad/over-rvs

Von Schomberg, R. (2011) Prospects for Technology Assessment in a framework of responsible research and innovation. In: M. Dusseldorp & R. Beecroft (ed.) T*echnikfolgen abschätzen lehren: Bildungspotenziale transdisziplinärer Methode*. Wiesbaden: Springer, pp. 39-61.

Scholz, L.H. (2016a) Algorithmic contracts. In: *Stanford Technology Law Review* (forthcoming).

Scholz, T. (2016b) *Platform cooperativism. Challenging the corporate sharing economy*. New York: Rosa Luxemburg Stiftung.

Seddon, R.F.J. (2013) Getting ‘virtual’ wrongs right. In: *Ethics and Information Technology* 15(1), pp. 1-11.

Sharkey, A. (2014) Robots and human dignity: A consideration of the effects of robot care on the dignity of older people. In: *Ethics and Information Technology* 16(1), pp. 63-75.

Sharkey, N. (2010) Saying ‘no!’ to lethal autonomous targeting. In: *Journal of Military Ethics* 9(4), pp. 369-383.

Shead, S. (2016) The biggest mystery in AI right now is the ethics board that Google set up after buying DeepMind. In: *Business Insider*, 26 March 2016. uk.businessinsider.com/google-ai-ethics-board-remains-a-mystery-2016-3

Sloot, van der, B. (2014). De noodzaak om privacy als publiek belang te herformuleren. In: *Christen Democratische Verkenningen* 3, pp. 125-132. Amsterdam: Boom Uitgevers

Smids, J. (2012) The voluntariness of persuasive technology. In: M. Bang & E.L. Ragnemalm (red.) *PERSUASIVE 2012. LNCS* 7284, Springer, Heidelberg, pp. 123–132.

Solove, D.J. (2002) Conceptualizing Privacy. In: *California Law Review* 2002(4), pp. 1087-1156.

Spahn, A. (2011) And lead us (not) into persuasion...? Persuasive technology and the ethics of communication. In: *Science and Engineering Ethics* 18(4), pp. 1-18.

Spahn, A. (2013) Ideas in motion. Moralizing mobility? Persuasive technologies and the ethics of mobility. In: *Transfer* 3(2), pp. 108-115.

Steiner, C. (2012) *Automate This: How Algorithms Came to Rule Our World*. London: Penguin Books.

Steltman, M. (2016). Aftappen ICT maakt Nederland niet veiliger. In: *Financieel Dagblad* (16 januari 2016).

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.

Stone, B. (2009) Amazon Erases Orwell Books From Kindle. In: *New York Times*, 17 July 2009. nytimes.com/2009/07/18/technology/companies/18amazon.html?_r=1

Strawser, B.J. (red.) (2013) *Killing by remote control: The ethics of an unmanned military*. Oxford: Oxford University Press.

Subirana, B., S. Sarma & E. Fleisch (2006) High resolution management. Improving Management Vision. In: *IESE Alumni Magazine*, July-Sept, pp. 8-13. ee-iese.com/102/ingles/pdf/subirana.pdf.

Sullins, J.P. (2012) Robots, love and sex: The ethics of building love machines. In: *Affective Computing* 3(4), pp. 398-409.

Sutrop (2010) Ethical issues in governing biometric technologies. In: A. Kumar & D. Zhang (red.). *Ethics and Policy of Biometrics* (Vol. 6005 of the series Lecture Notes in Computer Science). Heidelberg: Springer, pp. 102-114.

Sutrop, M. & K. Laas-Mikko (2012) From identity verification to behavior prediction: Ethical implications of second generation biometrics. In: *Review of Policy Research* 29(1), pp. 21-36.

Swart, J., J. Wolters & H. Zwart (red.) (2004) *DECs in discussie: De beoordeling van dierproeven in Nederland.* Budel: DAMON.

The Economist (2015) Artificial intelligence. The rise of machines. In: *The Economist*, 9 May 2015.

Timmer, J., L. Kool & R. van Est, (2015) Ethical issues in emerging applications of persuasive technologies. In: T. MacTavish & S. Basapur (red.) *Persuasive Technology. 10th International Conference, PERSUASIVE 2015*, Chicago, IL, USA, June 3-5, 2015, Proceedings, pp. 196-201.

Turkle, S. (2011) *Alone together: Why we expect more from technology and less from each other.* New York: Basic Books.

Turkle, S. (2015) *Reclaiming conversation. The power of talk in a digital age*. New York: Penguin Press.

UNESCO (2005) *Explanatory memorandum of Preliminary Draft Declaration on Universal Norms on Bioethics*. Paris: UNESCO.

US Department of Transport (2016) *Federal Automated Vehicles Policy. Accelerating the Next Revolution in Roadway Safety*. September 2016. transportation.gov/AV/federal-automated-vehicles-policy-september-2016

Veldhuis, R.N.J. (2014) *Biometrie – Op de grens tussen techniek en mens*. Oratie, 17 april, Enschede: Universiteit Twente.

Verhey, L.F.M. (2011) Grondrechten in het digitale tijdperk:driemaal is scheepsrecht? In: *Tijdschrift voor constitutioneel recht*, maart 2011, pp. 152,167.

Verbeek, P.P. (2016) Mag de baas je stiekem naar de sportschool loodsen? In: *Tubantia,* 7 juni 2016.

VNO-NCW (2016) Manifest: Samen naar een duurzame digitale samenleving. VNO-NCW. vno-ncw.nl/sites/default/files/ManifestSamennaareenduurzamedigitalesamenleving.pdf

Vrijenhoek, T. & M. Radstake (2016) Genen meten nieuwe stijl. Op weg naar genetische zorg van de toekomst. In: I. Geesink (red.) *De meetbare mens. Digitaal meten van het zieke en gezonde lichaam*. Den Haag: Rathenau Instituut.

Walker, S. (2016) Face recognition app taking Russia by storm may bring end to public anonymity. In: *The Guardian*, 17 May 2016. theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte

Walsh, K. (2016) Nest Reminds Customers That Ownership Isn't What It Used to Be. In: *EFF*, 05-04-2016. eff.org/deeplinks/2016/04/nest-reminds-customers-ownership-isnt-what-it-used-be

Weber, R. (2011) Accountability in the Internet of Things. In: *Computer Law & Security Review* 27(2), pp. 133–138.

Went, R., M. Kremer, A. Knottnerus (red.) (2015) *De robot de baas. De toekomst van werk in het tweede machinetijdperk*. WRR. Den Haag/Amsterdam: Amsterdam University Press.

Werson, H. (2012) *De fatale fuik: Achter de schermen van mensenhandel en gedwongen prostitutie in Nederland*. Amsterdam: Uitgeverij Carrera.

Wolf, M.J., F. Grodzinsky & K. Miller (2015) Augmented reality all around us: Power and perception at a crossroads. In: *SIGCAS Computers & Society,* 45(3), pp. 126-131.

Wright, A. & P. de Filippi (2015) *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. ssrn.com/abstract=2580664

WRR (2016) *Big data in een vrije en veilige samenleving.* Rapport 95. Amsterdam: Amsterdam University Press.

Zarksy (2013) *Transparent Predictions*. SSRN, papers.ssrn.com/sol3/papers.cfm?abstract_id=2324240

Zoeteman, C. & I. Widdershoven-Heerding (2007) Bio-ethiek: uniformiteit of maatwerk? In: *COGEM Jaarverslag 2006*, pp. 30-33.

Zureik, E. & L. Harling Stalker (2010) The cross-cultural study of privacy. In: Zureik, E. et al. (ed.) *Surveillance, privacy and the globalization of personal informatio*n. Montreal/London/Ithaca: McGill-Queen’s University Press.

Appendix A: Comprehensive analysis of the governance ecosystem

Introduction

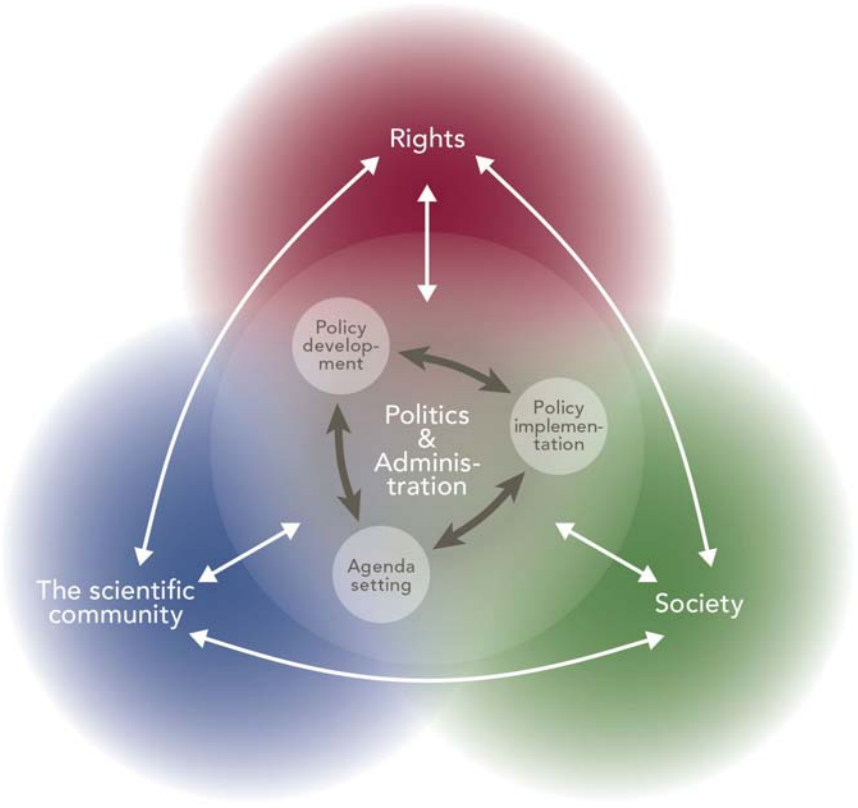
In this appendix, we describe how the governance of ethical and societal issues surrounding digitization has been shaped (and discussed) in the past five to ten years. We do that by applying the conceptual framework developed in chapter 4 (see Figure 1). First of all we outline the three domains: law, science and society. Subsequently, we focus on the political administrative domain, examining the processes of setting the agenda, shaping and implementing policy. This chapter is therefore structured as follows:

- Fundamental and human rights (section 1.2)
- Science (1.3)
- Society (1.4)
- Politics and administration
  - a. Setting the agenda (1.5)
  - b. Shaping and determining policy (1.6)
  - c. Implementing policy (1.7)

In each section we are looking for the actors or organizations that fulfil an institutional role in their domain. Our analysis focuses on developments in the Netherlands, but also features some interesting developments in other countries. Regarding fundamental and human rights, we look at the Thomassen state commission and also the activities of the UN Human Rights Council (UN HRC) and the Council of Europe. In the 'political and administration' domain, our description of an organization is linked to its institutional position in the policy cycle. The ministerial actions are discussed under section 1.6 'Shaping policy' and those of the personal data authority in section 1.7 'Implementing policy'. That does not mean that the ministries and the personal data authority as respectively policy shaping and policy implementing organizations, cannot carry out preparatory actions for policies.

In this appendix we only discuss initiatives involving societal and ethical issues with digitization. We briefly describe the organization concerned, indicating which technology it has applied. Their activities can concentrate on a specific technology, such as drones or self-driving cars, but also robotics or even digitization in general. We then review which ethical and societal aspects of digitization that particular organization has considered, to check whether the issues identified in chapter 3 are being addressed or not. Finally we describe what governance actions the various organizations propose, prepare, initiate or carry out in order to respond to the societal and ethical issues in our digitizing society.

Figure 1 Framework for the governance ecosystem



Rathenau Instituut

Fundamental and human rights

Fundamental and human rights form the basis for determining social values and basic freedoms. These rights are laid down in international treaties ratified by the Netherlands, such as the United Nations Universal Declaration of Human Rights (1948), or in the Dutch Constitution. They embed important values for the Netherlands such as human dignity, freedom, security, equality and justice. In chapter 3 we saw that digitization can affect many fundamental human values and rights. Here we describe the ongoing discussion in the Netherlands about whether and in what way the Dutch Constitution should be amended in line with the digital era. We show that similar discussions are being held in other countries and mention the activities around human rights and digitization within the Council of Europe and the UN HRC.

Digitization and the Dutch Constitution[94]

The Cabinet under prime minister Balkenende assigned the state commission Thomassed on 9 July 2009 to advise on a possible constitutional review. This included a request about the interpretation of fundamental rights in the digital age. In its 2010 final report, the commission advised updating several points in the Constitution. In a technology neutral way, the proposed amendments were aimed at Article 7 (freedom of expression), Article 10 (honouring personal privacy) and Article 13 (confidential communication). The Cabinet decided to only amend Article 13 (Parliamentary Papers II 2010-2011, 31570, no. 20). This amendment is still pending.[95] The commission's advice and the proposed constitutional amendment evoked a wider debate on fundamental rights in the digital era. Various authors argue that digitization requires a broader consideration of the question how we should deal with technological change from a constitutional perspective (Koops 2011; Prins 2015).

The discussions on what the Dutch Constitution should protect included how to acheive that protection. In order to strengthen the normative effect of the Constitution, the commission advised dropping the ban on reviewing the Constitution (Article 120). This advice was not adopted, but is still a topic of debate (Dommering 2011; Council for the Judiciary 2014; Parliamentary Papers II 2013-2014, 32334, no. 8). A review of the Constitution could namely offer individual citizens, NGOs and citizens rights organizations more opportunities to pursue justice concerning rights protected by the Constitution, such as honouring personal privacy. NGO Privacy First has indicated that a constitutional review could be a important means of protecting privacy under human rights.[96] In order to appeal for the right to honour privacy, currently people often revert to the European Convention on Human Rights (ECHR). Opponents argue that reviews of international treaties should be banned (Parliamentary Papers II, 2013-2014, 33 359, no. 5). Alongside the judiciary, the Netherlands Institute of Human Rights also seeks to improve the human rights situation by investigating, advising, raising awareness and carrying out individual assessments in matters of discrimination. This Institute could play a role in cases where digitization affects human rights, but this subject does not explicitly feature on its agenda (Netherlands Institute for Human Rights 2016).

International developments

United Nations: Protecting human rights in the digital world

In particular the *Human Rights Council* (HRC) examines the relationship between digitization and human rights. In 2011, La Rue, Special Reporter for the HRC from 2008 to 2014, argued for the promotion and protection of the right to freedom of expression – legal guarantees for universal internet access. Countries like Germany, Finland and Estonia took tentative steps in this direction (Prins 2015). On 6 July 2012, the HRC unanimously agreed to Resolution L13 *The promotion, protection and enjoyment of human rights on the Internet.* This Internet Resolution[97] stated that the rights people have in the physical world (*offline*) should also be protected in the digital world (*online*). Thus the UN Universal Declaration of Human Rights of 1948, as well as other relevant

[94] In chapter 4 we reported that discussions to update the Dutch Constitution began in the second half of the 1990s, with the establishment of state commission Franken (1999-2000). The proposed amendments to the Constitution based on this commission's advice were not adopted following crticism by the Council of State in 2004 (Verhey 2011; Koops 2011). See Parliamentary Papers II 2000-2001, 27460, no. 1 and the Franken commission's report 'Commissie grondrechten in het digitale tijdperk' (2000).

[95] For the current status, see: denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vjlnml176ini

[96] Discussion with Privacy First, 24 May, 2016.

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

international human rights treaties have been very clearly reconfirmed for the digital age. In 2015 the UN HRC appointed Joe Cannataci as its first Special Reporter and he was given the task of gathering information and drawing up recommendations to promote the right to privacy (Resolution 28/16). In 2013 the General Assembly had voiced its concern about the negative impact of surveillance on human rights (Resolution 68/167). Within UNESCO, the International Bioethics Committee (IBC) and World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) will be publishing reports on respectively big data & health and robotics in late 2017.

Council of Europe: Expansion of ethics domain due to technological convergence [98]

The Council of Europe[99] is also focussing more on the impact of digitization. It was one of the first institutes to put the protection of privacy on the international agenda in the 1980s, describing various key principles for protecting and dealing honestly with personal data (Bennet & Raab 2006). Since the 1990s, the Council of Europe has played an important part in the areas of ethics, biotechnology and medicine. In 1991 the Parliamentary Assembly of the Council of Europe (PACE) had a Convention organized on bio-ethics. This led in 1997 to the so-called Oviedo Convention regarding human rights and biomedicine.

Since 2013, the Council of Europe's Committee on Bioethics (DH-BIO) examines the numerous implications that the combination of various technological developments – including nanotechnology, cognitive sciences and information technology – has for human rights and human dignity (Forus 2014). [100] One of the implications of this technological convergence is that biomedical technology is being applied not just for medical purposes but more and more outside the world of medicine (Van Est et al. 2014). This raises questions about upholding human rights. As we saw in the historical chapter, ethical supervision of applied biomedical technology for example in medical practice has been institutionalised in many different ways. Article 14 of the Oviedo Convention forbids for example choosing the gender of a child for non-medical reasons.[101] In medical practice there are provisions to safeguard this right to non-discrimination.[102] In cattle breeding, gender selection is taking place on a large scale already, using *lab-on-a-chip* technology. It is easy to foresee that this cheap and relatively simple technology will become commercially available in non-medical domains. The question is how to maintain the right to non-discrimination.

In May 2015 the Committee on Bioethics organized the international conference *Emerging technologies and human rights* (Whittall et al. 2015). In line with this, on 24 June 2015, PACE adopted a resolution on *Technological convergence, artificial intelligence and human rights*.[103]

[98] Rathenau Instituut is closely involved with Council of Europe discussions. In 2013, the Council's Committee on Bioethics asked Rathenau Instituut to explore, from a human rights perspective, which ethical and legal challenges are linked to emerging technologies (Van Est et al. 2014). In June 2016, Rathenau Instituut assigned PACE to write an expert paper on the impact of converging technnologies on human rights.

[99] The Council of Europe was formed in 1949 to promote democracy, the rule of law and human rights in Europe. The Council's 47 member states have accepted the ECHR. Via The European Court of Human Rights (ECtHR), individuals, groups, organizations and countries can submit a complaint against a member state, by applying to the ECHR.

[100] See: coe.int/en/web/bioethics/emerging-technologies

[101] Article 14 *Non-selection of sex* of the Oviedo Convention states: "The use of techniques of medically assisted procreation shall not be allowed for the purpose of choosing a future child's sex, except where serious hereditary sex-related disease is to be avoided."

[102] Article 11 *Non-discrimination* of the Oviedo Convention states: "Any form of discrimination of a person based on his or her genetic heritage is prohibited."

[103] Technological convergence, artificial intelligence and human rights. Motion for a resolution. Doc. 13833, 24 June 2015. Parliamentary Assembly of the Council of Europe. See: assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21951&lang=en

According to the resolution, technological convergence, artificial intelligence (AI) and robotics are becoming increasingly important for society and require early discussions on how they affect human rights and freedoms. As stated above, PACE kicked off the Oviedo Convention in 1991. The 2015 resolution on artificial intelligence advises that PACE should fulfil a similar role for digitization, because human dignity, identity, the right to privacy and freedom of expression are important priorities. The resolution therefore seems to imply that PACE sees its domain extending: from bio-ethics (ethical issues related to biotechnological and biomedical developments) to ethics of converging technologies, whereby digitization forms the key driving force. A special PACE working group is going to investigate this motion further and hopes to have recommendations by March 2017 so that the Parliamentary Assembly can make a decision.

Table 1 Activities in the domain of fundamental and human rights

Who/what	Technology	Issue	Action
State Commission Thomassen	Digitization	Specific: freedom of expression, privacy, confidential communication	Proposal to amend Constitution Art. 7, 10, 13
Government	Digitization	Specific: confidential communication	Amend Art. 13
UN Human Rights Council	Internet	Broad: human rights on the Internet	Internet Resolution L13
UN Human Rights Council	Internet	Specific: right to freedom of speech and freedom of expression	Special Reporter Freedom of expression
UN Human Rights Council	Digitization	Specific: right to privacy	Special Reporter Privacy
UNESCO, IBC	Big data & health	Broad: ethical issues	Prepare report
UNESCO, COMEST	Robotics	Broad: ethics of robotization	Prepare report
Parliamentary Assembly of Council of Europe (PACE) motion	NBIC convergence and artificial intelligence; digitization	Broad: impact NBIC on human rights	Investigate need to extend work domain from bio-ethics to NBIC ethics

Science

The domain of science and knowledge feeds the social and political-administrative discussion with information, concepts and insights. Science contributes by signalling and articulating the ethical issues that digitization evokes. Scientific analyses assist politics and administration for formulating an opinion or determing an agenda for action. And science enables a reflection on the governance system and policy implentation. Based on the scientific literature, we listed in chapter 3 the ethical issues identified with digitization. In this section we will describe the role that science plays in the governance ecosystem. Box 1 contains a brief overview of recommendations and actions for governance, as mentioned in the scientific literature we referred to in chapter 3.

Politics and administration
Science contributes directly to the political-administrative process by providing scientific knowledge when asked to support politicians and policymakers, often in the form of studies, or when scientific experts are consulted during a hearing or roundtable discussion in the House of Representatives. Science often plays an important role in articulating concepts. The discussion that led to establishing the Franken state commission was the result of a dissertation by Hofman in 1995 on the concept ‘confidential communication’ (Parliamentary Papers II 1996-1997, 25 443, no. 1/2). Also the meaning of the concept privacy is greatly influenced by scientific debate on this topic (see Solove 2002). Illustrative of the meaning of privacy in the twenty-first century is a research project by Prof. dr. B.J. Koops. With the emergence of technology such as smart phones and IoT, Koops wants to rediscover the meaning of privacy for an era in which the distinction between public and private space has changed (Martijn 2016).

Societal debate
Scientists also add to the societal debate through the media. Think of the previously mentioned column in the British newspaper *The Guardian* by Hawking, where he and other prominent scientists warn about the dangers of artificial intelligence (Hawking et al. 2014). Or the study by Frey and Osborne (2013), whose calculations on the automation of various jobs sparked a discussion on the relationship between technology and labour. Stanford University in the US recently published the initial results of 100 years’ research on the effects of AI on society, with an important recommendation that governments need more technological expertise to make policies effective. In the Netherlands, science also plays an important role in boosting societal and political debate. Professor in Computational Social Sciences Helbing wrote in the newspaper NRC that we are creating a data dictatorship because governments are increasingly allowing themselves to be led by big data (van Noort 2016). Professor of Global ICT Law Moerel argues that delivering privacy for a trade-off ensures that privacy is only for the rich (Moerel 2015). And Jacobs, professor in computer security showed with his research group, that the security on things like the Dutch public transport smart card [*OV-chipkaart*] is not adequate (Radboud University 2016).

Socially responsible innovation
Alongside feeding the discussions, science also provides innovations in response to societal and ethical issues, such as solutions for privacy by design, or new cryptographic techniques that can make the Internet safer. Research financing takes into account the societal additional value of innovation with concepts like *Responsible Research and Innovation* and *Socially Responsible Innovation* (MVI). A important part of this philosophy is that the ethical aspects of innovation are

identified at an early stage, and can thus be included in an ethically responsible development of science and innovation. In its science vision (Parliamentary Papers II, 2014-2015, 29338, no.141) and letter to parliament on ethical aspects of the innovation policy (Parliamentary Papers I, 2015-2016, 33009 no. 16), the NWO [Netherlands Organization for Scientific Research] MVI programme is seen an important step in addressing the ethical and societal issues concerning innovation. In addition, scientists themselves are looking to see if their own research is dealing with the growing amount of databases responsibly. The Royal Netherlands Academy of Science (KNAW) advises setting up an *Ethical Review Board Informatics* to assess whethers informatics research is handling personal data in a responsible way.

Box 1 Recommendations in scientific literature

The scientific literature referred to in chapter 3, describing the wide range of ethical and societal aspects of digitization, includes several authors' recommendations for the governance of these aspects. The scientists point to the important role for companies who can develop their technology in such a way that it is applied in an ethically responsible way, so-called *ethics by design*. This could mean incorporating transparency, protection of privacy and legal protection in the technology. Technologies can be designed in such a way that values such as privacy and autonomy are safeguarded, for example using special encryption measures or by making the data tangible again. With *digital agents* such as robots and AI, companies have significant responsibility to develop technology that makes decisions in an ethically responsible way. This is, however, not an easy task, considering that in a certain situation, it is not always clear-cut what adequately ethical action means precisely. In addition it is deemed important to incorporate flexibility in the technology. Technological components have to be able to keep up with the times, so that they can be adapted in line with technological developments and potentially changing moral views.

Some scientists feel that citizens must have a say in the debate on digitization and should get more insight, control and ownership of their data. How this should happen and what technology can be used to achieve this are topics that we should be addressing. Citizens should also be aware of their own responsibilities, because as users, they too need to safeguard their own data. Collectively, citizens should even be able to halt undesirable technological developments, by creating alternatives themselves or setting up opposition movements.

When it comes to regulating digitization, general as well as specifically applicable rules are required. As technological developments may be intrusive and at the same happen incredibly quickly, robust rules are required that can be rapidly adjusted. This means that within the decision-making process, there must be scope to evaulate and adapt these rules. Other wide policy options are for example granting subsidies for initiatives specifically aimed at safeguarding public values, at stimulating the development of national and international privacy and transparency standards for government and industry, and educating the public on the potential risks linked with their own responsibility. The government is often asked if it can act as supervisor, to guard for example citizens' autonomy or privacy.

Naturally scientists say we need more research. This should be done in various areas. Importantly, as much research as possible should be carried out on the anticpated consequences of technology for people and society, as well the actual consequences. Then an ethical analysis must be made. In addition, research is needed on how *digital agents* can make ethical decisions. This requires more insight into ethics and the way moral views could change in the future. Methodological research could point out how we can better anticipate technology (for example through scenario studies) and intervene when necessary.

Civil society actors and debate

Civil society actors play an important part in the governance of societal and ethical issues concerning digitization. Companies and technology developers shape digital technology and make their own, sometimes moral, choices. By means of self-regulating mechanisms such as internal ethical committees, codes of conduct and covenants, companies define how they want to act. Civil society organizations feed the political-administrative discussion on digitization and can in this way contribute to awareness raising and probably digital empowerment of individuals. And by making their own choices, individuals are also shaping what place digital technology can take in society. Here we give an outline of a few relevant actors and their initiatives. Although this is not a comprehensive overview, it does sketch a picture of the type of actions undertaken by civil society actors.

ECP - Platform for the information society
ECP's mission is to support a reliable, successful digital society in the Netherlands. As independent platform, ECP acts as driver and liaison between public and private parties such as ministries, telecom companies and social organizations like the Consumers Association. Through projects, events, research and debate, ECP has the social and economic importance of digitization high on its agenda. A major element of ECP's remit is to stimulate and improve digital security for companies, government and individual citizens. In recent years, ECP has been involved in various programmes on safe online behaviour such as the AlertOnline campaign, the 'Digivaardig Digiveilig' programme and the 'Veilig Internetten' site where users can find information on how to handle online privacy and passwords securely. ECP also chairs the Internet Safety platform where strategic negotiations take place between private and public parties on how to improve internet security.

Another essential theme for ECP is stimulating digital skills. It does this by raising awareness – for example through campaigns on internet security – but also through activities such as CodePact for teaching programming. CodePact aims to give as many children as possible the opportunity to learn programming, for example by organizing training during the annual Codeweek. In 2015, ECP set up the working group Ethics and Information Society that examines the ethical dillemas that we face with technology and digitization. An essay collection on this subject will be published at the end of 2016.[104] In its vision document '*De volwassen informatiesamenleving' [The adult information society]* ECP advocates a discussion on ethics, not based on the contrast between man and technology, but recognising that man is a technological being (ECP 2015).

Bits of Freedom

The Dutch foundation Bits of Freedom is a citizens rights movement that since 1999 has focussed on protecting freedom and privacy on the Internet. In Bits of Freedom's view, privacy and freedom of communication are both fundamental rights that are unmissable for personal development and democracy. The foundation promotes these values with campaigns and lobbying, in an attempt to ensure that 'government and industry overturn weak governance and implement good policies'.

One of their best known campaigns is the annual Big Brother Awards. These awards are presented to companies or government organizations that have been guilty of privacy breaches. In 2013 the former minister of Security and Justice Ivo Opstelten received a Big Brother Award, which led to questions from MPs Schouw and Verhoeven (Proceedings 2013-2014, 211). In 2015 minister Plasterk of Foreign Affairs received a Big Brother Award for the Bill proposing the new intelligence and security services Act (Wiv). Bits of Freedom also speaks out in legislative processes. It responded to the internet consultation for the Wiv Act, and a special website explained the legal text, making it more accessible and therefore easier for the public and organizations to comment on the proposed legislation.

As initiator of the Privacy coalition of 32 parties, Bits of Freedom called for the minister of Security and Justice to form a vision on privacy protection in 2015.[105] The minister was to facilitate a public debate and was asked to suspend dealing with new laws that have an impact on privacy until there was indeed a clear vision. The minister invited the Privacy coalition to discuss their proposal, further explaining the cabinet's touchstones regarding privacy protection (Parliamentary Papers II 2013-2014, 32761, no. 83). Although the minister did not respond to the request to suspend Bills, he commited to involving the Privacy coalition in future dialogue on the issue of privacy, for example with the cabinet's response to the WRR report on big data (WRR 2016).

Bits of Freedom aims to improve digital skills and awareness in the public at large. For that reason it launched Internet Freedom Toolbox, giving users practical advice, tips and links to applications in order to strengthen their privacy, confidential communication and data security. Through projects in conjunction with journalists, the foundation provides insight into data brokers' practices in the Netherlands, or the Dutch lobby on the European General Data Protection Regulation (Bits of Freedom 2015).

[104] For more information, see the ECP annual reports on: ecp.nl/jaarverslag

[105] This call was also backed by the Dutch Association of Jurists, SETUP, Privacy First, Open State Foundation, Stichting Digitale Infrastructuur Nederland (DINL), Waag Society, Publeaks, Kennisland, Privacy Barometer, Internet Society Nederland (ISOC.nl). For an overview, see: bof.nl/2015/04/02/persbericht-brede-coalitie-vraagt-visie-privacybescherming-ard-van-der-steur

Privacy First

Privacy First was set up in 2008 as an independent foundation to preserve and promote the right to privacy. It attempts to counteract privacy breaches via political lobbying, public campaigns or legal actions and lawsuits. Important topics in recent years have been biometry, camera surveillance, the public transport smart card, medical privacy, mobility and anonymity in public spaces (Privacy First 2015). Most of the attention regarding these issues is directed at the government, however in the coming years, Privacy First intends to focus more on companies.

Legal procedures are a means for Privacy First to take firm action against privacy violations. The foundation has brought proceedings against storing fingerprints under the Passport Act, number plate parking, average speed checks and the Dutch Telecommunications Data Retention Act (Wbt). Regarding this Act, in 2015 The Hague Court judged that the Act is in violation of the right to privacy and must be revoked.[106] This judgement is in line with the European Court of Justice's ruling on an almost identical European Data Retention directive. In legal cases, Privacy First collaborates with law firms, civil society organizations such as the Dutch Section of the International Commission of Jurists (NJCM) and sometime individual citizens. It also aims to provide information to citizens who have queries about privacy protection. Occasionally individual citizens' cases are adopted or supported, but the foundation indicates it only has a limited capacity for this (Privacy First 2015).

Finally the Privacy First Solutions initiative has tried since 2014 to raise awareness of privacy-friendly actions by government and industry; for example by encouraging the application of *privacy by design* and awarding prizes for privacy-friendly services and products (Privacy First 2015).

Consumers Assocation

The Consumers Association (Consumentenbond) is an independent association that promotes the interests and rights of consumers through campaigns, actions, research and providing information. This Association is also involved with consumers' privacy. Research shows that 54 percent of consumers sometimes or seldom read privacy protection conditions, whereas 95 percent find the protection of personal data (very) important. Having examined various products, including eleven well-known Dutch Android apps, the Consumers Association found that their conditions are often far too vague and consumers are poorly informed. The Association helps users via a step-by-step plan to better manage the privacy settings on their mobile phones. It also criticizes the data protection conditions with many smart TVs, which led to manufacturers making adjustments. As a result of research carried out by the Norwegian Consumers Association into dating and fitness apps, the Dutch consumers association, along with Norway, Sweden and Slovenia, are pushing for the creators of such apps to provide better terms and conditions.[107]

With its campaign 'Digidwang' the Consumers Association opposes that more and more organizations are forcing consumers to go digital. It campaigns on behalf of consumers who do not want to or are not able to go with digitization, speaking out against plans for example by the tax office in the long term to only send digital mail. In the Consumer Association's view, everyone

[106] Claimants in this case were Privacy First, the Dutch Association of Criminal Lawyers (NVSA), the Dutch Association of Journalists (NVJ), the Dutch Section of the International Commission of Jurists (NJCM), internetprovider BIT and telecom providers VOYS and SpeakUp, headed up by Boekx Lawyers in Amsterdam.

[107] See: Consumentenbond (2015) and consumentenbond.nl/campagnes/privacy

should be able to choose in which way they are contacted. Also the national ombudsman, the FNV (Trade Unions) and associations for seniors such as KBO, ANBO and PCOB (a Christian organization) speak out against digitization coercion. In the coming years, the Consumer Association wants to focus on the trade in personal data and its adverse effects such as the emergence of 'risk profiles' linked to people. Currently it receives scores of notifications every year of data discrimination; people denied something or having to pay an additional fee due to a 'problematic' data profile. In addition, the Consumer Association is going to investigate where improper and too much data is collected or shared with third parties, and where necessary, confront companies about inappropriate collecting or sharing of data.

Other social organizations

We will name just a few of the other organizations that are involved with the ethical and societal aspects of digitization. The Dutch Association of Jurists recently issued a preliminary report ‘Homo Digitalis’, outlining the impact of digitization on the law and from a legal persepctive (NJV 2016). The Dutch Section of the International Commission of Jurists (NJCM) is dedicated to the protection of human rights in the Netherlands. As such, it comments on Bills such as the amendment to the intelligence and security services Act (Wiv), challenging violations of privacy. The Dutch touring club ANWB together with its sister organizations in Europe launched the campaign *My car, my data* to make the public aware and to plea for regulations on the data that manufacturers collect from smart cars. SIDN, the foundation for Internet Domain Registration in the Netherlands, annually stimulates initiatives aiming to strengthen the Internet, reinforce the position of users and increase the additional social value of the Internet.[108] The NLNet foundation supports people and organizations (such Bits of Freedom) that contribute to strengthening and protecting an open and free Internet. Various cultural organizations such as V2_, Waag Society and SETUP provide workshops, lectures and exhibitions for a critical reflection on digitization in the cultural domain, and their activities strengthen digital literacy among the general public.

Business world

There are various companies that profile themselves as providing privacy-friendly services. Examples of these are the QIY foundation that is working on a system to give users more control of their own data. Search engine Ixquick offers people the ability to search the web without disclosing their personal data. Internet providers like XS4All and Greenhost are working towards an open and free internet along with digital security. Business sectors are also coming up with initiatives regarding privacy. Members of the Association of Insurers have drawn up a data protection convenant. Recently the Association issued a green paper *Grip op data* analyzing the effects of digitization in their sector, and are announcing a solidarity monitor to keep track of how data influences social solidarity (Verbond van Verzekeraars 2016). Industry and employers organizations VNO-NCW together with SMEs are fully committed to raising awareness of digital security.[109] Companies are establishing internal structures to consider the ethical aspects of digitization. The Rabobank has an Ethics Committee and an Ethics office, where digitization is a current topic.[110]

[108] sidnfonds.nl/wat-we-doen

[109] vno-ncw.nl/nieuws/versnelling-aanpak-cybersecurity-hard-nodig

[110] Interview Francoise Rost, 22 April 2016

The responsbility of companies to respect human rights is contained in the Organization for Economic Cooperation and Development Guidelines for Multinational Companies (OECD guidelines).[111] They adopt the concept of *due diligence* from the *United Nations Guiding Principles on Business and Human Rights* (UNGPs).[112] This constitutes the process whereby businesses can identify, reduce and prevent the actual and potential negative effects of their activities, and whereby they can be accountable for their approach to these effects as an integral part of their decision-making process and risk management systems. Companies have to make an effort to acknowledge their own and the parties in their chain's risks of violating human rights and where possible prevent violations. Notifications of alleged infringements of the OECD guidelines can be made through *Nationaal Contactpunt* (NCP). Up till now, it has not received any notifications in connection with digitization.[113]

On the initiative of the European Commission, member states draw up plans to implement the UNGPs at a national level. In the Netherlands that is the NAP (National Action Plan for businesses and human rights, 2013. Parliamentary Papers II 2012-2013, 26485, no. 174). One of the NAP's activities is to further investigate the regulation of Dutch companies' duty of care. This research was completed in 2016 and highlighted: 'the practical and procedural thresholds for holding companies accountable, such as high costs, lack of evidence and limitations in the possibilities to engage in collective actions' (Parliamentary Papers II 2015-2016, 26485, no. 219). The cabinet has indicated that when civil law and burden of proof are reviewed, it will take into account this duty of care research.

To make the information on *due diligence* accessible for companies, the European Commission has had *Sector Guidances* drawn up for three sectors, including ICT (EC 2011). The guidelines advise companies on their responsibilities to respect human rights and how they can implement these in their day-to-day operations.

International developments

At an international level, we can see a lively ongoing debate on the ethics of digitization. Various organizations and persons have called for digital rights, new forms of protection, ethics committees and codes of conduct. Scientist Hawking, Tesla CEO Musk and Apple founder Wozniak supported the call to ban autonomous weapons (Future of Life Institute 2015). Berners Lee, the founder of the world wide web, appealed for a digital Magna Carta, to protect the rights of internet users (Kiss 2014). To celebrate the 800th centenary of Magna Carta, the British Library launched a crowdsourcing initiative – in response to Berners-Lee's appeal for a Magna Carta for the web – to enable people to put forward their suggestions for a digital Magna Carta.[114]

[111] OECD guidelines for Multinationals (OECD 1976; 2011) regarding business ethics issues and relevant codes of conduct. The Dutch government has underpinned theses guidelines; it expects companies to undertake socially responsible entrepreneurship (TK 2012-2013).

[112] . The UNGPs were developed under the leadership of UN Special Representative John Ruggie (hence the name Ruggie Principles). The three pillars of these principles are as follows: The first reconfims the obligation of states to protect human rights. The second is aimed at companies' responsibility to respect human rights. The third is the necessity to give victims of human rights violations as a result of companies' activities the opportunity to recover and/or compensation (Parliamentary Papers II 2015-2016, 26485, no. 219). The UNGPs do not impose legal constraints but set an authoritatve international standard.

[113] oesorichtlijnen.nl/meldingen. The OECD MVO guidelines are based on human rights as described in the Universal Declaration of Human Rights.

[114] bl.uk/my-digital-rights

Not only organizations play a role in the public debate on digitization. In recent years, certain individual citizens have sparked a social debate with their revelations or actions. The revelations of whistleblower Snowden led to many social and political discussions on government data collection and surveillance. The Austrian privacy activist Schrems caused a sensation by ordering a 1200-page document of personal data from Facebook, and with an action before the EU Court of Justice, managed to ensure that the *Safe Harbor* decision (2000/520/EC) – regulating data exchange between Europe and the United States – was declared invalid. This spurred the European Commission to reach a new agreement in which European citizens' data was better protected when exchanged with companies in the US.

There is often strong interaction between social players' activities and the initiatives taking place in the political-administrative domain. The discussion about digital rights, fuelled by among other things Berners-Lee's appeal, as described in section 5.5, led to political initiatives for bringing about a Digital Bill of Rights in the UK. The European Digital Rights Initiative (EDRi) launched a campaign, together with other civil rights organizations such as Bits of Freedom, in the run-up to the European elections in 2014. With the campaign 'We Promise', the candidates for the European Parliament were asked to abide by a Treaty of ten principles to protect digital rights (EDRi 2014).

In 2014 a British and a Canadian think-tank took the initiative to set up an international commission for developing a future vision of internet governance. The Global Commission on Internet Governance (GCIG) consists of 29 stakeholders. In 2016, the Commission proposed a number of recommendations to keep the Internet accessible, open, secure and reliable (GCIG 2016). The fundamental rights of citizens, such as privacy and confidential communication, must be protected, governments must not force companies to incorporate loopholes in software, decisions by algorithms must be controllable, and producers of software and digital services must be liable for the quality of the technology they produce.

In 2016 the British innovation foundation Nesta called for setting up a *Machine Intelligence Commission* (Mulgan 2016). According to Nesta, such a Commission is necessary to protect public interests when using algorithms and artificial intelligence and to maintain the public's trust. Nesta also thinks that the Commission should have no formal role in certifying or approving algorithms, but strong powers to investigate and gain access to information. Importantly, it will need to have good technical skills and the capacity to develop software itself in order to test computer systems. The Commission would have to look at applications in several key sectors – such as health, mobility, finance – and make recommendations to various enforcement authorities. NESTA bases its recommendations on the experience of previous commissions in the UK regarding environmental pollution and use of embryos. Such commissions have played an important role in stimulating public debate about ethical boundaries, creating and securing public trust, and enabling economic development (Mulgan 2016).

Finally, there are also initiatives aimed directly at the development of technology. The Internet Engineering Task Force (IETF), which develops Internet protocols and standards, has recently established a Human Rights Protocol Considerations Research Group (HRPC) together with the human rights organization Article 19. The Group examines how human rights can be taken into account when creating web protocols and standards (Ten Oever & Cath 2016). The Institute of

Electrical and Electronics Engineers (IEEE), the international organization for technical professionals, launched an initiative to develop methods for ethics when designing autonomous systems (IEEE 2016). The first step is to list the most significant ethical issues with the help of the IEEE community and formulate recommendations. This should end up becoming a living document that helps designers to make ethical choices when creating autonomous systems. Some companies have set up committees to deal with ethics issues. In 2004, Google set up an Ethics Board that looks at things like artificial intelligence. However, hardly anything about the Commission's role and composition is revealed (Shead 2016). In response to the public outcry that Facebook had to confront after the experiment influencing users' emotions, the company set up an ethics board, which will assess the company's research on the social network from an ethical perspective (Boka 2016).

Table 2 Activities at civil society level

Who/what	Technology	Issue	Action
ECP	Digitization	Security, privacy, inclusiveness	Programme for digital skills and security, working group ethics & ICT
Bits of Freedom	Internet, digital communication	Privacy, security	Big Brother awards, privacy coalition, internet freedom toolbox
Privacy First	Digital communication, digital government	Privacy	Legal actions
Consumers association	Apps, consumer technology	Privacy	Campaign privacy awareness. Call companies to account on privacy
OECD guidelines Corporate social responsibility	Specific case by case	Specific case by case	Companies have a duty of care to respect human rights
EU and international			
EDRi (EU)	Internet, digital communication	Human rights online	Campaign legislative candidates' commitment to protect digital rights
Nesta (UK)	AI, algorithms, robotics	Autonomy, control of technology, trust	Call for a Machine Intelligence Commission
Global Commission on Internet Governance	Internet, digital communication	Human rights online	Report with call for protection of digital rights
IETF (int.)	Internet, digital communication	Human rights	Human Rights Research Group investigates how protocols can include rights

IEEE (int.)	AI, algorithms, robotics	-	Initiative to assist designers of autonomous systems to make ethical decisions

Rathenau Instituut

Agenda setting

When it comes to agenda setting, various advisory councils and institutes play a role. We will only discuss those organizations that identify ethical and social issues in the field of digitization. We leave to one side the opinions that focus on the financial, economic or technical aspects of digitization.[115] Our overview cannot be comprehensive. We discuss in succession some of the national activities of the Scientific Council for Government policy (WRR), the Advisory Council on International Affairs (AIV), the Council for the environment and infrastructure (Rli) and Rathenau Instituut. We also look at the European Group on Ethics in Science and New Technologies.

Scientific Council for Government Policy

The Scientific Council for Government Policy (WRR) is an independent advisory body that ‘provides scientifically substantiated information on developments that can have a long term impact on society’.[116] In recent years WRR has published a number of reports highlighting diverse ethical and social challenges with digitization. These looked at government digitization (2011), public values on the Internet (2015), robotization and work (2015) and big data (2016).

The *iOverheid* report (WRR 2011) describes how digitization is fundamentally changing the government. ICT is not only a way for the government to carry out its work, it also changes the way tasks and processes are organized. This creates new challenges in the field of privacy, transparency in government processes, control and correction of information pollution and the resilience of citizens. WRR therefore recommends among other things to establish an iPlatform to improve transparency and an iAutoriteit to assist citizens having problems with iOverheid [igovernment]. Its 2015 report *De publieke kern van internet* (WRR 2015), looked at the core public issues due to the fact that the Internet is becoming increasingly important: cybercrime, vulnerability of vital infrastructures, states’ increasing grip and regulation of the Internet. WRR advocates raising the Internet as spearhead of foreign policy and establishing the public core of the Internet in international treaties. The report *De robot de baas* (WRR 2015) examines the effects of robotization on the labour market, advocates an inclusive robot agenda to advance complementary collaboration between man and machine and opposes the scenario of technological unemployment. In 2016, at the request of the ministries of Security and Justice and Internal Affairs, WWR issued advice on big data in the domain of security. WRR concluded there was a mismatch between big data and the current legislation and regulations. The emphasis now is on gathering data. This needs to be

[115] Such as the Advisory Board Science and Technology (AWTI), Centraal Planbureau (CPB), Planbureau voor de Leefomgeving (PBL) or Sociaal Cultureel Planbureau (SCP).

[116] Institutions Act WRR, Art. 2.a 30 June 1976

supplemented with regulating and supervising the analysis and use of big data. WRR recommends introducing a duty of care for data-processing parties to clarify how they achieve certain outcomes. In addition, the capacities and technical expertise of the supervisors, such as the personal data authority and the Intelligence and Security Services Review Committee (CTIVD), need to be strengthened (WRR 2016).

Advisory Council on International Affairs

The Advisory Council on International Affairs (AIV) is an independent advisory body that advises the government and parliament on foreign policy pertaining to security, peace and human rights. At the government's request, AIV provided advice in 2014 on internet governance and in 2015, together with the Advisory Committee on Issues of Public International Law (CAVV), on autonomous weapons.

In the context of international internet governance, the AIV's advice *Het internet: een wereldwijde vrije ruimte met begrensde staatsmacht* (AIV 2014) examined Internet issues such as privacy, secure information and surveillance. The advice recommended that the Netherlands plays its part in protecting internet freedom, also in relation to the companies that have a defining role. To achieve this, a coherent vision of the Internet and stronger interdepartmental coordination are required. The Netherlands should serve as example for other countries by nationally promoting a high level of protection of human rights. The priority is to take a critical look at the guarantees with the intelligence and security services Act (Wiv), the supervision of the Personal Data Authority (AP) and strengthening the CTIVD.

The advice issued by AIV/CAVV on *Autonomous weapon systems* in 2015 highlighted the themes of security and controlling technology. Their view is that autonomous weapon systems must go hand in hand with 'meaningful human control'. This means people must be able to make an informed and deliberate decision on the use of weapons and applying (lethal) force. A moratorium or ban on (fully) autonomous weapons is not considered achievable and desirable. Autonomous weapon systems should comply with the international law of war. According to the AIV and CAVV, technically speaking, it is unlikely that there will be weapons that can function without 'meaningful human control' in the coming 20 years. If the future development of artificial intelligence makes weapons so self-sufficient that we can no longer speak of meaningful human control, such weapons should never be used.

Council for the environment and infrastructure (Rli)

The Rli advises the government on policy issues concerning the sustainable development of the environment and infrastructure. Although not automatically involved with digitization, the Council does have this topic on its agenda when there is an overlap with the living environment – such as the development of smart cities or the role of digital infrastructure in the Dutch business climate.[117]

With its study '*Verkenning technologische innovaties in de leefomgeving'* (2015b) the Rli identifies that the rapid development of technology is having a huge impact on our way of life and on moral values such as privacy and transparency, before we have been able to properly consider the

[117] See for example the Rli work programme (2015a; 2016)

implications. Data infrastructure is becoming increasingly important, socially and economically. The government must defend the public’s interests in access, transparency, security, privacy and robustness. Think of redundancy in the data infrastructure to compensate for local drop-out or of vulnerability due to reliance on one or a few large market parties. Regarding the use of data, the Council notes that autonomy and protecting freedom of choice are vitally important. According to Rli, the technological breakthroughs require a cabinet-wide vision. It sees the government’s role as organizing broad public debates about the impact of technological innoavtions on our values.

Rathenau Instituut

Rathenau Instituut plays a role in the process of identification and agenda setting. As a research institute of the Royal Netherlands Academy of Arts and Sciences, its remit is to stimulate the forming of public and political opinions on science and technology. In recent years the institute has highlighted the topic of digitization in a large number of varying reports. These address developments such as the Internet of Things, robotics, biometry, smart mobility, big data, digital platforms, and digitization in healthcare, insurance companies and farming.[118]

Privacy is a recurrent theme, especially where mobility, insurance, e-health, big data and the Internet of Things are concerned. New technology enables new forms of monitoring – for example of driving, health behaviour or lifestyle – and that raises issues about how the data obtained via monitoring is handled. The report ‘*Voorgeprogrammeerd’* (Van ’t Hof et al. 2012a) identifies that it is not just about regulating the collection of data, but also the analysis and application of that data, for example how social media and search engines filter information. Such developments are putting pressure on the freedom of choice online (Van ’t Hof et al. 2012b). Rathenau Instituut is calling for more transparency and awareness of profiling. The emergence of the Internet of Things allows consumers to manage and control their data flows, and therefore requires a new approach to privacy (Eskens et al. 2016); companies need to take more responsibility and there needs to be more focus on the right not to know and not to be measured, analysed or coached (Van Est 2014). In this way the discussion is shifting from informational privacy in the sense of protecting and controlling personal data, towards privacy as a fundamental right, aimed at protecting personal privacy. The big challenge is to continue safeguarding privacy in its original form of human right in a society that is becoming more and more digitized.

A recurring dynamic in the reports is the arrival of new parties – with their innovative new data-driven revenue models – that are shaking up existing markets like the medical domain, mobility, insurance practices, or agriculture. Consequently, these practices are now facing all kinds of ICT issues such as data security, privacy and the power of data collectors. A frequently asked question is who actually has ownership of the data, for example during discussions about whether car owners should also own the data generated by their vehicle (Timmer et al. 2014). Or: who owns the biological and physiological data that is collected by apps and wearables. In the agricultural sector, will the farmers of the future still own the data on their own land (Munnichs & Bos 2016)? In France

[118] Also reports such as: Beyond control: Consumer privacy in the Internet of Things (2016), Digitalisering van dieren (2016), De meetbare mens (2016), Verzekeren in de data-gedreven samenleving (2015), Dicht op de huid (2015), De data-gedreven samenleving (2015), De Kracht van platformen (2014), Tem de robotauto (2014), Intieme technologie (2014), Voorgeprogrammeerd (2012), Overal robots (2012).

this question led to an amendment of a Bill, thereby keeping the data collected by international technology providers accessible for French farmers.[119] Regarding digital platforms, Rathenau Instituut underlines the importance of data portability, so that consumers are able to transfer their accumulated data to another provider, thus counteracting the forming of market monopolies (Kreijveld et al. 2014).

Transparency is required to keep up to speed with data flows and analyses. Regarding health, the questions patients and consumers need to ask is what data are technology providers and underlying third parties collecting and why. And how are profiles being used to reach which conclusions about health and health risks (Geesink et al. 2016). For insurers, this transparency and explainability of automatic decisions are significant recommendations (Timmer et al. 2015).

Robotics and artificial intelligence raise numerous societal and ethical issues, for example concerning human dignity (Royakkers et al. 2012; Van Est & Kool 2015; Royakkers & Van Est 2016). In 2012, Rathenau Instituut called for the cabinet to form an integral vision in order to steer robotics developments in the right direction (Messer 2012). The Dutch government also had to strive for an international ban on autonomously weaponed robots, because life and death decisions should not be left to machines. To drastically improve traffic safety, the government needed to seriously consider introducing automatic speed limitation devices. In addition, politicians would have to focus quickly on the consequences of smart robot technologies in the living environment: what decisions do we want to have robots make or especially not make? Which new skills are required of carers and patients, and what does this mean for privacy and responsibility issues? In the area of labour, it is vital that new technology does not reduce human beings to merely a cog in the wheel instead of having enriching work. An inclusive robot society requires the complementary use of people and robotics.

The publication *Intieme technologie* (Van Est 2014) bundles insights from various studies on intimate technology. According to Rathenau Instituut, humans and technology are blending so rapidly that we can speak of an intimate technological revolution. The Institute pleas for a nationwide approach to consider how digitization is affecting fundamental values such as autonomy, human dignity and privacy (Van Est & Rerimassie 2014). It also calls for a state commission to consider the significance of the intimate technological revolution for fundamental rights. Finally, media literacy and technological citizenship should be encouraged, so that members of the public are aware and can discuss the impact of technology on their living environment and bodies.

To develop frameworks for socially imbedding the rapid ICT revolution, it would be useful to build on the experience with ethical issues surrounding biomedical engineering. That experience is relevant because ICT is becoming more and more interwoven with life sciences and behavioural sciences while all kinds of biomedical techniques are being applied in the public domain. As the 1997 Biomedical Ovideo Convention can provide an excellent basis to protect human dignity when applying (medical) technology in the public domain, Rathenau Instituut recommends that the government ratifies this convention. The traditional trend to discuss ethics within the biomedical sphere is now shifting, thanks to new technology, to technological practices in daily life, as

[119] Project de Loi République numérique. Amendment Article 40A. For more details see: republique-numerique.fr/pages/digital-republic-bill-rationale

highlighted in the report *From Bio to NBIC Convergence* (Van Est et al. 2014), commissioned by the Council of Europe's Committee on Bioethics.

Other advisory bodies and institutes

Alongside the above mentioned institutes, we see the topic of digitization and ethics being taken up by other advisory organizations. For example the Netherlands Bureau for Economic Policy Analysis (CPB) published its study *Kiezen voor privacy* on the personal data market. An effective personal data market stimulates innovative uses of data and gives people the opportunity to determine where and when they are prepared to relinquish their privacy (CPB 2014). The Education Council's multi-annual agenda indicates that it intends to study the impact of digitization on education, also focussing on the consequences for students' privacy and identity development and the balance of powers between educational institutes and the companies who control the online learning platforms (Onderwijsraad 2015: 30).

International developments

European Group on Ethics in Science and New Technologies

At European level, the European Group on Ethics in Science and New Technologies (EGE) plays an important signalling role in discussions about the ethical aspects of new technology. The EGE is the President of the European Commission's independent advisory body and also the epicentre of the network of national ethics boards in various EU countries.[120] Since it was established in 1991, the EGE has published various reports, the majority being in the biomedical domain. In recent years the EGE has been focussing more on digitization in its opinions on information technology (Salvi 2012), security and surveillance (Dratwa 2014).

The opinion paper *Ethics of Information and Communication Technologies* (Salvi 2012) was requested by EU chairman Barroso to serve as reference point for the responsible implementation of the European Digital Agenda (Salvi 2012: 59). A significant aspect is the inclusive accessibility of ICT, in particular for vulnerable groups such as minorities, seniors and people with limitations. The EGE pleas for the right to access the Internet and education to ensure that people are able to develop the digital skills they need nowadays. In addition, freedom of expression on the Internet and net neutrality need to be protected. Another important topic is the free development of identity in the digital era. Thereby social skills are crucial so that people for example learn how to deal with social media and the Internet in a responsible way. Finally, the EGE wants people to be able to embrace ICT innovations without having to sacrifice personal privacy or autonomy.

In *Ethics of Security and Surveillance Technologies* (Dratwa 2014), the EGE underlines that the state's responsibility to guarantee security should extend further than protecting physical integrity. It is also about social and human security that enables people and society to develop themselves based on freedom, dignity, autonomy and justice. Fundamental values such as human dignity cannot simply be exchanged for security. Proportionality is the key word when applying security technology along with looking at proven effectiveness. The EGE warns that profiling can lead to discrimination, and proposes that (ethical) assumptions underpinning algorithms must be made

[120] ec.europa.eu/research/ege/index.cfm

explicitly mandatory to prevent *stigmatization by design*. This requires an independent supervisor with adequate technical know-how at member state level, who can also be the point of contact for citizens who feel they have been wronged, and who can also drive the public discussion on the pros and cons of surveillance.

Table 3 Activities within the political-administrative domain to put issues on the agenda

Who/what	**Technology**	**Issue**	**Advice/action**
Scientific Council for Government Policy			
iOverheid	Digitizing government	privacy, transparency, autonomy, control	Realise transformative impact of ICT on government. Initiate iAutoriteit and iPlatform for citizens' resilience
Public core of the Internet	Internet infrastructure	Security, censorship, free access	Determine public core of the Internet in international treaties
Robot de Baas	Robotics	Work, inclusion, equality, autonomy	Work on complementing humans and robotics
Big data in free and secure society	Big data and algorithms	privacy, security, autonomy, discrimination, right to fair trial	Stronger focus on the use of data, supervising algorithms, new tasks for supervisors
Advisory Council on International Affairs			
The Internet	Internet infrastructure	Internet freedom, privacy, surveillance, information security	Protect internet freedom. Interdepartmental coordination and vision on internet policy
Autonomous weapon systems	Autonomous weapon systems	Control of technology, accountability	Meaningful human control when using autonomous weapon systems
Council for the Environment and Infrastructure			
Technological innovations in the living environment	Digitizing (AI, data infrastructure, drones, robotics, IoT, VR)	privacy, transparency, security, access, control of algorithms, autonomy	Data development requires cabinet-wide vision and public debates about the impact on fundamental values
Rathenau Instituut (selected publications)			
Just Ordinary Robots	Robotics, AI	privacy, autonomy, human dignity, control of technology	Policy vision on tasks that can be given to robots, not automate life or death decisions
Work on Robot society	Robotics, AI, platforms	Unemployment, human dignity, inclusivity	Training, inclusive innovation, guarantee against monopolization and exploiting digital platforms
Data-driven society	Big data, algorithms	privacy, transparency, control algorithms, autonomy, discrimination, balance of powers	Control algorithms, protect autonomy and equality. Data is not neutral: stimulate date literacy
Honest advicet	Health apps, wearables,	privacy, autonomy, reliability of technology,	Protect privacy and autonomy, hallmark for reliable e-coaches, obligatory burden of proof for

	persuasive technology	transparency, balance of powers	government contribution to influencing behaviour
Intimate technology	Digitization broad	privacy, autonomy, human dignity	Nationwide approach to impact of digitization on constitution, advance technological citizenship
European Group on Ethics in Science and New Technologies			
Ethics of Information and Communication Technologies	Digitization broad	privacy, human dignity, autonomy, freedom of expression, access to technology	Access to ICT. Stimulate digital skills, free online identity development and responsible personal use of ICT
Ethics of Security and Surveillance Technologies	Big data, surveillance security technology	security, privacy, human dignity, autonomy, discrimination	Make assumptions of algorithms explicitly mandatory. Do not exchange human dignity for other values like security

Rathenau Instituut

Policy and decision making

At the policy and decision making stage, preparatory reports and advice are translated into visions, policies, regulations and laws. Here we look at the actors whose institutional task is to determine policy and shape laws and regulations: the cabinet, ministries and parliament that constitute the Senate and the House of Representatives. We describe the actions undertaken to deal with the ethical and societal issues concerning digitization. As stated, we describe the actors based on their role in the institutional landscape, but their actions may also be more in the domain of policy agenda setting, for example if a ministry sets out research or establishes an expert group to support policy making.

Ministry of Economic Affairs

Ministry of Economic Affairs policy has focussed several times on the ethical aspects of digitization. Its vision of telecommunications, media and the Internet (Parliamentary Papers II 2013-2014, 26643 No. 300), emphasizes the importance of a free and open internet and digital freedom of choice, both for the protection of civil liberties as well as for the (free) market. In line with this, the focus is on digital platforms (Papers II 2013-2014, 26643 No. 345) and their (power) role as gateway to information and services. It considers whether measures are needed to encourage free choice and competition. The letter on future-proof regulation expands on this; new generic legislation is not yet desirable and the aim is to create more space for innovations such as platforms and the share economy. It is important, however, to keep an eye on protecting public values (Papers II, 2014-2015 33009, no. 10 & 12).

Privacy has a place in the *telecommunication vision*.[121] The letter on big data and profiling expands on this theme (Papers II 2014-2015, 32761, no. 76). It explains that big data and profiling can

[121] The *telecommunication vision* discusses expanding companies' duty of care set out in the Telecommunications Act, to take appropriate measures for integrity, continuity and the protection of personal privacy. The progress report (Papers II 2013-2014, 26643 no. 345), however concludes that this duty of care has not been amended, because the generic duty of care in the Wbp Act was deemed to be sufficient.

violate the right to privacy and equal treatment. The legal framework consisting of the Protection of Personal Data Act (Wbp), the Telecommunications Act and Equal Treatment Act (Awgb), provides protection. The supervision of compliance with these three Acts takes place by respectively the Personal Data Authority, the Consumer and Market Authority and the Netherlands Institute for Human Rights. At the same time, the letter indicates that a purely legal approach will not be sufficient; transparency and trust are also needed. It announces that a high level expert group will be formed to provide advice in 2016 on the relationship between big data and the protection of constitutional rights like privacy and equal treatment.

On the subject of ethics discussed following the Ester motion (Parliamentary Papers I, 2013-2014, 33750 XIII), the government was asked to 'create structural space in its technology and innovation policies for reflection on ethical issues'. In June 2016 Minister Kamp responded to the motion by writing *Ethical aspects of innovation policy* (Parliamentary Papers I, 2015-2016, 33009, no. 16). He states that rapid technological developments raise ethical issues such as the fusion between man, technology and nature, as well as the impact on fundamental values such as privacy and autonomy. He goes on to describe the current initiatives undertaken by the Ministry in the field of ethics and agrees to make this reporting part of the annual progress report on enterprise policy. Ethics is dealt with in innovation policy under the NWO research programme 'Socially Responsible Innovation' (MVI) and the social innovation program Top Sector Energy (STEM). The high level expert group is dealing with big data as indicated in the brief on big data and profiling. Finally, the brief also mentions that the ministry departments dealing with agriculture, food and cattle farming[122] have a set of guidelines on Ethics in Policy. This handbook helps policymakers deal with the ethical aspects of policy development.[123]

Despite some departments' ongoing initiatives on ethics and (digital) innovation, there is no overarching vision or coordination on this topic. There are guidelines on how to handle ethical issues in food, agro and cattle farming, but not in other policy areas. The expert group on big data – whose results have not yet been published – shows that attention is being paid to the ethical aspects of big data, but that this is still in a preliminary, advisory stage. Other technological developments that are part of digitization have not yet been addressed. The request to structurally monitor ethical aspects of innovation policy and an additional request by the Standing Committee for Economic Affairs (Parliamentary Papers I, 2015-2016, 33009, no. D) to link the consequences of policies to monitoring, imply that the focus may be extended in the coming years.

Ministry of Security and Justice

The topics of security and protection of personal privacy are important matters for the Ministry of Security and Justice. In 2007, the Brouwer-Korf Advisory Committee for 'Security and personal privacy' was asked to provide advice about the impact of technological developments on protecting safety and personal privacy. Based on this committee's advice and the evaluation of the personal data protection Act, it was agreed to introduce notification duty of data breaches and expand the power of the supervisor (currently the Personal Data Authority) to impose fines (Parliamentary Papers II 2009-2010 31051 no. 5).

[122] Departments of the former Ministry of Agriculture, Nature and Food Quality

[123] At the request of the Standing Committee on Economic Affairs, these guidelines are also sent to parliament (Papers II, 2015-2016, 33009 no. D)

The discussion on security and privacy appears in the memorandum *Privacy policy* (Parliamentary Papers II, 2010-2011, 32761, no. 1) and later in *Security and freedom in a digital society* (Papers II, 2013-2014, 26643, no. 298). They announce measures such as awareness-raising campaigns aimed at digital resilience, encouraging privacy and security by design in procurement processes, and the mandatory privacy impact assessment (PIA) for developing new legislation and policy. However, the theme is so complex that some aspects still need to be well considered. This is expressed in the request for WRR advice (published in April 2016) on the role of big data in the security domain. One of the questions raised is whether it is necessary to distinguish between access to data and the use of this data.

In the field of cyber security, a National Cyber Security Strategy (NCSS) has been drawn up. This aims at an integrated approach to cyber security through public-private partnerships (Parliamentary Papers II 2013-2014, 26643, no. 291). Part of the strategy is setting up the National Cyber Security Centre (NCSC) which responds to incidents and threats and is attempting to strengthen digital resilience and security. At the Senate's request, the cabinet is establishing its position on encryption (Parliamentary Papers II, 2015-2016, 26643, no. 383). The cabinet states that it does not find it appropriate to impose legal restrictions on encryption in order to provide intelligence and security services access to data – such as the FBI wanting access to a suspect's encrypted iPhone.

At the same time, the cabinet is looking into the potential for digital technology in the security domain. The bill on computer crime III and draft bill for the Intelligence and Security Services Act (Wiv) – with the Ministry of Internal Affairs playing a leading role – would give the government new powers. Both bills were severely criticized:[124] the government would get too far-reaching powers over untargeted data collection, which would be a violation of personal privacy. The Wiv proposal is being discussed by the Council of State.

During the discussion on policies for privacy and security, efforts were made not to treat these as opposing values, but in alignment (Parliamentary Papers II 2013-2014, 32761, no. 83). At different times, the Minister of Security and Justice responded to the parliament's requests to form a vision on privacy and the protection of personal privacy. The question is one of the reasons for the Privacy policy memorandum, later highlighted again by MPs Thieme and Oosenburg.[125] In response to Oosenburg's question, Minister Van der Steur stated that different components of the vision are reflected in the briefs *Freedom and security in the digital society*, *E-privacy* and *big data and profiling.*[126] One comprehensive vision, according to the Minister, would be so abstract that it would not do justice to the varying perspectives and angles of approach to the diverse areas. Each minister is therefore responsible for the privacy aspects linked with their policy area. Privacy is mainly approached from the perspective of data collection and data protection.

[124] For critique of the computer crime Bill, see: tweedekamer.nl/vergaderingen/commissievergaderingen/details?id=2016A00399). The draft Wiv Act came under criticism from the Netherlands Institute for Human Rights, Bits of Freedom and VNO-NCW, see: internetconsultatie.nl/wiv/reacties

[125] Respectively Parliamentary Papers II, 2010-2011, 32761, no.1; 2013-2014, 32761, no. 83; 2013-2014, 32761, no. 89

[126] Papers II 2013-2014, 26643, no.298; 2014-2015, 32761, no. 49; 2014-2015, 32761, no. 76.

Ministry of Education, Culture and Science

The actions taken by the Ministry of Education, Culture and Science to deal with the social impact of digitization are mainly in the area of digital skills. The platform ‘Onderwijs 2032’ is looking at the future of education. Digitization and robotization will alter jobs in the future, and education must prepare pupils for this rapidly changing digital world.[127]

Ministry of Social Affairs and Employment

In September 2014, Minister Asscher of Social Affairs and Employment (SZW) mentioned in his speech at the annual SZW conference, that rising robotization was a potential threat to employment. In response to MP Van Ojik’s motion (Parliamentary Papers II 2013-2014, 27406, no. 212), the minister’s letter discussed the effects of automation on the labour market. Because the subject is surrounded by uncertainty, and to anticipate various developments, policymakers must focus on this issue. The CPB and SER (Social and Economic Council) were asked to investigate the relationship between technology and employment, and also Rathenau Instituut (at the request of the House of Representatives) and WRR (2015) to publish studies on this topic.

Robotization has the potential to support human dignity by taking over heavy work and making work ‘safer, less demanding and more fun' (WRR 2015:3), at the same time, it can cause unemployment (for certain groups of people) and growing social inequality. In response to the Rathenau report *Working on the robot society* (Van Est & Kool 2015), the Ministry indicated that it is addressing good training and smooth transition to new jobs. This is also reflected in the Ministry of Education’s lifelong learning policy (Parliamentary Papers II 215-2016, 30012, no. 55). The SER advice about the effects of robotization, automation and digitization on the labour market and relations, draws attention to the flexibility of labour, and how the position of digital platform employees can be safeguarded from the viewpoint of healthy and safe working. The cabinet is acting on SER’s advice by working on a broad inclusive agenda for robotization and labour (Parliamentary Papers II 2015-2016, 29544, no. 725).

Ministry of Foreign Affairs

As described, the WRR and AIV have called for an integrated international internet policy. As a result of the AIV and WRR reports, the cabinet has responded to this call on behalf of the Ministers of Foreign Affairs, Economic Affairs, Defence, Internal Affairs, Security and Justice (Parliamentary Papers II, 2015-2016, 26643, no. 411). The cabinet underlines the importance of a coordinated inter-ministerial vision and agreed to develop this, bearing in mind the need for a free, open and secure Internet. According to the cabinet, fundamental rights apply online well as offline, a perspective emphasized in the 2015 human rights report (Parliamentary Papers II, 2015-2016, 32735 no. 154). The Netherlands drew attention to ‘digital rights’ by making this the main theme of the Global Conference on Cyberspace it organized in April 2016, also focussing on the ethics of algorithms. These actions home in on the advice given by the WRR and AIV to put the spotlight on human rights in international internet policy.

[127] The minister was referring here to WRR advice ‘De robot de baas’

Regarding the protection of human rights, the minister concludes in the letter about companies' duty of care for conducting socially responsible international business (IMVO),[128] that there are procedural thresholds for holding companies accountable, such as high costs and limited opportunities for collective actions (Parliamentary Papers II, 2015-2016, 26485, no. 219). The cabinet is therefore investigating the desirability of amending the law so that under certain circumstances, collective actions could claim compensation. These collective actions could be relevant in legal procedures appealing for the right to personal privacy.

Finally, the Ministries of Foreign Affairs and Defence produced a letter on autonomous weapon systems, in response to AIV advice in 2015, that autonomous weapon systems can only be used provided there is meaningful human control (Parliamentary Papers II, 2015-2016, 34300 X, no. 88). Therefore thought must be given to the allocation of responsibility and liability already at the design stage of weapon systems; also when procuring systems, the Advisory Committee on International Law and Conventional Weapon Use must supervize the meaningful control. The letter states that the ethical issues about human dignity with regard to autonomous weapon systems are no different to conventional weapon systems that feature meaningful control. The potential development and deployment of fully autonomous weapons – where human control is no longer possible – was rejected in advance by the cabinet. Like the AIV, the cabinet considers a moratorium is not feasible, although NGOs and scientists are calling for this, for example in the previously mentioned letter opposing autonomous weapons, signed by Stephen Hawking, Elon Musk and 1000 other experts (Future of Life Institute 2015).

Ministry of Internal Affairs

The Ministry of Internal Affairs is involved in various ways with digitization. It not only looks at digitizing government services, but is also the ministry responsible for examining the impact of digitization on constitutional rights. As a result of advice from State Commission Thomassen, Article 13 of the Constitution will be amended, as discussed above (Parliamentary Papers II 2010-2011, 31570, no. 20).

In response to the WRR's 2011 iOverheid report on digitizing the government, the Minister of Internal Affairs underlines that digitization does not only mean an instrumental change; the government's own organization and tasks will change fundamentally. That realization must be anchored in the government's work (Parliamentary Papers II, 2011–2012, 26 643, no. 211). The WRR's recommendation to establish an iAutoriteit for assisting citizens who have problems with e-government was not adopted, because these responsibilities are part of the government's entire service provision. Due to recurring problems with government ICT projects, in 2012 the House of Representatives initiated a parliamentary investigation, organized by the temporary ICT Committee, also called the Elias Commission. Its final report strongly criticized government policy (Parliamentary Papers II, 2014-2015, 33326, no. 5). Consequently, the review and monitoring of ICT projects have been improved, also by setting up an ICT Review Office (Parliamentary Papers II, 33326, no. 13). However, the monitoring and reviews focus mainly on technical and managerial dimensions, rather than the societal and ethical impact of government ICT.

[128] As set out in the OECD guidelines for multinational enterprises and the UN Guiding Principles on Business and Human Rights (UNGPs).

Finally, the 2002 intelligence and security services Act (Wiv) is currently undergoing review. An important driver is the technique-dependent formulation of the Act's interception provisions. The distinction between cable or air communication is no longer compatible with the developments in communication methods and data traffic (Parliamentary Papers II 2014-2015, 33820 No. 4). The Bill was proposed via internet consultation with experts and civil society organizations, and the Privacy & Identity Lab did a privacy impact assessment (Parliamentary Papers II 2015-2016, 33820, No. 8). The proposal was sharply criticized in parliament because of the disproportionate impact on privacy that would mean new powers and a lack of adequate safeguards. The Council of State is now considering an amended proposal.

Parliament

As representatives of the people, the Senate and the House of Representatives have an important role to play in creating awareness of societal and ethical issues with regard to digitization. And their task as controller is to keep a critical eye on government policy. Government questions play an important role in the cabinet's visions and letters which address policies on technological developments. The Ministry of Economic Affairs ePrivacy letter is a response to the motions by Verhoeven and Gesthuizen (Parliamentary Papers II, 2011-2012, 24095, no. 294) and Recourt (2011-2012, 32761, No. 10 and 11). This ePrivacy letter requested more information on big data and profiling, which resulted in another letter and a *high level expert group* being set up to investigate the impact of big data on fundamental rights (Parliamentary Papers II 2014-2015, 32761, no. 76). As indicated above, the Minister of Security and Justice was asked several times to develop a vision on digital privacy and security. We have seen that social actors, advisory councils and research institutes also play a role in putting issues on the agenda. The Big Brother Award by Bits of Freedom is the catalyst for Verhoeven and Schow's questions in parliament, and the response was the memorandum *Security and freedom in the digital society* (Parliamentary Papers II, 2013-2014, 26643, no. 298).

Parliament has repeatedly asked the government for its vision on privacy and security. Other issues concerning digitization are more often driven by current events. Reports in the media give rise to government questions about the desirability of certain technological developments, for example vehicle manufacturers collecting data from cars, initiatives by banks wanting to make use of big data, Uber evading regulations, the control and transparency of self-learning algorithms on the stock market, or seniors who think the government is going digital too quickly.[129]

The Gerkens and Ester motions explicitly draw attention to the ethical aspects associated with digitization and NBIC convergence. As described in Chapter 4, they pose the historically recurrent question whether the political-administrative system is adequately equipped to deal with ethical issues arising from technological innovations. The questions confirm a need for structural reflection and discussion on the impact of technological developments. Ester's request for annual reporting on the role of ethics in innovation policy should thus be seen as an initiative to enable a structurally recurring political-ethical discussion on this topic in the Senate.[130]

[129] Respectively Appendices Parliamentary Papers II 2015–2016, 1488; 2013–2014, 1658; 2013–2014, 1869; 2014–2015, 1818; 2015-2016, 2421

[130] Conversation with Peter Ester, 14 June 2016

In addition to MPs' questions, the political parties also consider technology. On behalf of the VVD party, Lucas presented a robot agenda *Robotisering zonder achterblijvers* [*Robotization without stragglers]* (Lucas 2016), urging to make room for innovation and at the same time work on education so that people can keep up with their changing environment; in the area of ethics, there are calls for investigating the value of a National Ethics Commission, to maintain a good balance between man and technology. The party D66 presents its views on technological developments in its publication*Techvisie* (Verhoeven et al. 2016). It states that the current political discussions are still too often triggered by incidents. A rapidly changing society requires a clear vision for the future. According to D66, technology and the Internet should be the cabinet's priority along with a Minister of Economics, Technology and Privacy. D66 promotes inclusive digital skills, digital freedom of choice, good encryption and protection of personal data, and transparency about data collection and algorithmic decisions. A key recommendation is to strengthen the position of supervisors – such as ACM (digital freedom of choice), the personal data Authority (privacy), NCSC (cyber security) and CTIVD (security services). Internet giants should have a duty of care, such as the banks, because of their utility function in the field of information. And it should be easier to hold liable those companies that produce poor software. The recommendations in 'Techvisie' are reflected in D66's electoral programme. It also proposes an iPlatform for critical reflection on the digital society and a special commission to facilitate annual discussions in the government on the relationship between technology and fundamental rights (D66 2016).

International developments

EU policy

The main pillar of European policy in the field of digitization is the strategic agenda for a *Digital Single Market.*[131] This agenda, despite its economic perspective, also argues for an inclusive and secure digital society. One working group that does pay explicit attention to ethical issues is the *Onlife Initiative,* consisting of 12 international experts who were invited to think about how digital technology is changing humanity. The result is the *Onlife Manifesto* (EC 2013), an incentive to develop new concepts in order to understand the fundamental impact of digitization on humans and their social environment. We need these new concepts to think about the fading boundaries between people and technology, protecting our private space, our attention, self-determination and autonomy. The manifesto forms an important input for questions about the societal and ethical impact of technological developments in the research programme Horizon 2020.

Also in legislation there are important developments at European level. Dutch legislation is to a great extent in line with European directives and regulations when it comes to digitization. The most significant change in this area is the replacement of the data protection Directive 95/46/EC with the General Data Protection regulation EU 2016/679. Major changes include increasing the supervisor's powers to impose fines; strengthening the rights of the individual (for example in the field of data portability and deleting their data), and intensifying the obligations for the data-processing party (for example, to apply *privacy by design* and *privacy by default*).[132]

[131] COM (2015) 192 final

[132] By fixing the standard privacy setting on a social network at limited visibility, instead of accessible to everyone

Yet another important development was the *Safe-Harbor A*greement on data exchange between Europe and the US. For this Agreement, the European Commission proposed that data belonging to European citizens in the US should be just as well protected as in the European Union, a legal requirement for the smooth international exchange of data. Following Snowden's revelations, the Austrian Schrems brought an action before the European Court of Justice. Because Snowden's statements revealed that European citizens' data was not adequately protected in the US, the Safe-Harbor Agreement was declared invalid. A new agreement on exchanging data between Europe and the US – the EU-US Privacy Shield – should provide better protection of personal data.[133]

European Parliament

The European Parliament's Committee on Legal Affairs (JURI) published a draft report on robotics and artificial intelligence on 31 May 2016 (2015/2103 INL). To deal with the ethical challenges of these developments, a set of fundamental core values needs to be drawn up – principles that can be applied at every stage in the contact between robots, artificial intelligence and people. The points that the JURI Committee identifies are: security, privacy, integrity, human dignity and autonomy. Other aspects that deserve attention include: standardization, intellectual property, ownership of data, employment and accountability. The JURI Committee has set out the ethics principles in a proposal for a *Charter on Robotics*. This Charter contains a code of ethics for robot builders,[134] a code for research ethics committees,[135] and a model for users about operations permitted with robots. [136] The JURI Committee advises setting up a European Agency for robotics and artificial intelligence so that this entity can advise public bodies at European and national levels on technology, ethics and regulations.[137]

The draft report aims to bring about a resolution that can be adopted by the European Parliament, which can consequently ask the European Commission to submit suitable topics to parliament for determining new (or amending existing) proposals.[138]

Pleas for digital rights

At the end of 2014, the Labour Party in the UK had a study carried out on a digital agenda for the United Kingdom. Based on the research, the recommendations were to work on digital skills to ensure that everyone can benefit from the digital society. It also called for an ethical framework to help policymakers deal with ethical issues to do with digital developments (*Digital Government Review 2014*). Several initiatives in the UK call for reflection and protection of fundamental values in a *Digital Bill of Rights.* In 2014, Berners-Lee, one of the founders of the world wide web, advocated a Magna Carta for the web (Kiss 2014). The Liberal Democrats published a call in 2015 to gather input for a Bill protecting fundamental rights on the web.[139] The *Digital Liberties* initiative is leading a campaign with support from various political parties to persuade the UK Parliament to adopt a

[133] See: justitia.nl/privacy/privacy-shield.html; en justitia.nl/privacy/safe-harbor.html

[134] Code of Ethical Conduct for Robotics Engineers

[135] Code of Ethical Conduct for Robotics Engineers

[136] License for Users

[137] Point 8 of the draft report

[138] Article 46 j.o. 52 European Parliament Regulation

[139] libdems.org.uk/protecting-your-data-online-with-a-digital-rights-bill

Digital Bill of Rights. Its key principles are: the ownership of personal data as right; equal access to the internet for all; preventing monopolization; and stopping mass-surveillance.[140]

Several other countries are also working on laws that define internet rights. The French Government is working on the Bill *Republique Numerique*. In 2014 and 2015, a large internet consultancy was set up so that everyone could respond and contribute to the proposal. The Bill has since been adopted by the French National Assembly and is now being discussed and awaiting approval by the French Senate. The Bill contains the following key elements: making open data more freely available; strengthening the rights of internet users; and an inclusive digital society. This can be seen as strengthening the right to data portability,[141] protecting net neutrality, better opportunities for young people to have information about their childhood removed, a right to indicate what happens to personal information after death and mandatory transparency of platforms on how they are paid for ranking products on their site.[142]

The call for transparency in online platforms – directed more at ranking algorithms – can also be seen in the German government's position paper.[143] It states that platforms should inform their users about how they preselect and present content, such as in a news feed on a social media site (Beuth 2016). In 2015, the Italian government adopted a declaration of internet rights; although not legally binding, the declaration serves mainly to spur the government and parliament to respect the established principles (Pollicino & Bassini 2015). Finally, certain ethical effects have been considered in relation to specific technological developments. Germany's Minister of transport has set up an ethics commission for self-driving cars (Ramthun & Schlesiger 2016). The US federal government has established rules for (highly) automated vehicles, drawing attention to ethical issues (USDoT 2016).

Table 4 Activities within the political-administrative domain regarding policymaking

Who/what	Technology	Issue	Action
Ministry of Economic Affairs			
Vision Telecommunication	Internet, digital communication	Free, open internet, freedom of choice	Stimulate security, neutrality and continuity
Letter big data and profiling	Big data, profiling, algorithms	Privacy and equal treatment	High level expert group
Letter future-proof regulation	Digital platforms	Public values such as consumer security, fair competition	Room to experiment in regulation, keeping an eye on public values

[140] cybersalon.org/digital-bill-of-rights-uk/

[141] The right to data portability does not only involve personal data, but also data associated with the account: "all files posted online by the consumer"; "all data resulting from the use of the consumer's account . . ."; and "other data associated with the consumer's account, the recovery of which is relevant to change supplier within a given industry"

[142] republique-numerique.fr/pages/digital-republic-bill-rationale

[143] bmwi.de/DE/Presse/pressemitteilungen,did=764540.html

Letter ethical aspects of innovation policy	Digitization	Fusion man & tech; privacy and autonomy	Focus on ethics in research; annual reporting business policy
Ministry of Security and Justice			
Brouwer-Korf Commission	Digitization, digital communication	Security and privacy	Mandatory reporting data breaches; expand power to impose fines AP
Memorandum freedom & security in the digital society	Digitization, digital communication	Security and privacy	Encourage privacy by design, mandatory PIA for new legislation. Campaign digital resilience. Request WRR advice big data
Bill computer crime III	Digitization	Security	New powers security services
Cabinet position encryption	Encryption	Confidential communication, privacy	Legal restriction encryption not desirable
Ministry of Education, Culture and Science			
Letter Onderwijs 2032	Digitization, robotization	Digital skills, privacy, security, online behaviour	Digital literacy in core curriculum. Continuous training
Ministry of Social Affairs and Employment			
Letter Technological deveopments and labour market	Robotization, automation	Human dignity, technological unemployment	Request research Rathenau, SER, CPB
Letter Working on robot society	Robotization, automation	Human dignity, technological unemployment	Work on good education, life-long learning, retraining and transitions
Ministry of Foreign Affairs			
Letter International Internet policy	Internet	Fundamental rights: freedom, privacy, equality	Interdepartmental vision of Internet policy, fundamental rights also apply online
Human rights reporting 2015	Internet, algorithms	Fundamental rights: freedom, privacy, equality	Focus on digital rights, ethics & algorithms at GCCS Conference
Letter Autonomous weapon systems	Autonomous weapon systems	Human dignity, control of technology	Allocate responsibility part of design phase. AIRCW assess meaningful control
Ministry of Internal Affairs			
Letter iOverheid	Digitization government	Citizens' resilience, control of technology	Realise impact digitization embed in government
Bill Wiv	Digitization communication	Security	New powers security services
Parliament			

Questions and motions in parliament	Various aspects digitization	Various ethical issues, much focus on privacy	Request vision, position, policy, legislation, regulation
VVD Robot agenda	Robotization	Human dignity; unemployment	Engage in eduation. Research value of National Ethics Committee
D66 'Techvisie'	Digitization, Internet	Privacy, surveillance, net neutrality, security, confidential communication	Minister of Economy, Technology & Privacy, digital skills, strengthen supervisors, internet giants' duty of care
EU and international			
EU – Onlife initiative	Digitization broad	Wide number of ethical issues	Onlife Manifesto informs research agenda
EU – General Data Protection Regulation	Data collection and protection	Privacy, data protection, transparency	Strengthen supervisor. Strengthen internet user rights and data processor obligations
European Parliament – Draft Report Civil Law rules on robotics	Robotization and artificial intelligence	Security, privacy, integrity, human dignity and autonomy	Proposal for resolution Eur. Parliament to create ethics principles and European Agency for robotics & AI
UK – Campaign for Digital Bill of Rights	Digitization, Internet, digital communication	Privacy, surveillance, balance of powers	Proposal right to data ownership. Equal access Internet
France – Bill Republique Numerique	Digitization, Internet, digital communication platforms	Privacy, net neutrality, transparency, balance of powers	The right to be forgotten. Transparency revenue model platforms. Rights to data after death

Rathenau Instituut

Policy implementation

At the policy implementation stage, we look at how supervisors and review committees ensure that the rules, standards and Acts determined in the policymaking phase are implemented and observed. A supervisor is a government-appointed, independent and impartial institution that monitors organizations' compliance with legislation and regulations. Based on regulatory frameworks and protocols, review committees carry out reviews, usually case by case, on whether a particular action – such as the procurement of an autonomous weapon system – adheres to stipulated frameworks. Apart from administrative control, organizations can also be called to order through legal procedures, for example via collective actions. However, this section focuses on supervisors and review committees.

Personal Data Authority

The Personal Data Authority (AP), formerly the Institute for Protection of Personal Data (CBP), supervises the observance of privacy legislation[144] and gives legal advice. In recent years, the AP has been studying topics such as profiling, the use of sensitive data and data processing by the government. It has also provided critical advice on data processing for Bills such as the Social Support Act (Wmo), Youth Law, the telecom data retention obligation and the draft Computer Crime III Bill (CBP 2013; CBP 2014; AP 2015). The AP looks at the necessity and justification for data processing and whether the powers are weighed against the violations of personal privacy. In addition, the AP reprimands various organizations if their privacy policy is not up to scratch. For example when privacy conditions were reviewed in 2014, Google had to request unambiguous consent for combining data from various services. Producers of lifestyle-apps and wearables such as Nike+ are reminded by AP that users must be clearly informed about, and must consent to the use of their health data.

In its 2014 annual report, the AP focuses on big data, pointing out the dangers of 'digital predestination' because through profiling, people are only offered choices that match their profile (CBP 2014). The following year, the topic of big data featured more prominently on AP's agenda, and the Authority indicated that alongside the legislation principles, a broad social and political debate was required on big data (CBP 2015). It also reminded everyone that in this field, the world has seen radical changes over the past five years: because of smartphones, wearables and Internet of Things, people cannot avoid leaving countless digital traces every day. This raises the question of whether the protection of personal data has become like 'trying to dry out a flooded room without turning off the taps'. The supervisory boards, however, are confident that the new General Data Protection measures will strengthen users' control (AP 2015:5).

The Mandatory Data Breach Notification Law requires organizations as of 1 January 2016 to report any data leaks directly to the AP. This gives the AP an additional new task as service desk. The aim of the reporting obligation is to raise the security level and increase citizens' empowerment. At the same time, AP has stronger powers to levy fines, enabling it to impose heavier sanctions. The expectation is that this will have a strong preventive effect. The developments in big data, profiling, and the Internet of Things are also on the agenda for the coming years. The AP's measures focus on ensuring that users are properly informed and that their consent is requested. One concern in the area of profiling is that it often happens in an invisible way, whereby those involved cannot, or only with difficulty, exert any influence. One of AP's research topics in the coming period is the collection of data on children. The current generation of children is growing up in an era of 'life-logging' when large amounts of information on their life and development end up in public and private databases. For parents and children, it is important to know what choices they can make about this (AP 2016).

Consumer and Market Authority

The Consumer and Market Authority (ACM) oversees competition, telecommunications and consumer law. One of the components of ACM's agenda is protecting digital consumers, so that they can confidently surf the Web and make online purchases (ACM 2014; 2016a). In this context,

[144] AP supervizes these four major Acts: Personal Data Protection; Police Data; Key Register of Persons; Judicial Information and Criminal Records.

the ACM investigated how young people cope with their online privacy, and it has campaigned to raise awareness of online privacy. Research shows that young people often do not know that their personal data is used by apps to make money. To alert young consumers to this, ACM launched the campaign ‘Every app has its price’.[145] ACM also enforces the revised cookie rules to deliberately inform consumers about online tracking.

ACM has the topics of net neutrality and the dominance of large internet companies on its agenda for 2016. It keeps track of whether internet providers are respecting net neutrality, which is mandatory in Europe as of April 2016 (ACM 2016a). In a study on how to monitor online platforms effectively, ACM concludes that we need to know more about the functioning of the dynamic markets in which online platforms operate. In addition to building up knowledge, it is vital to strengthen the contact with market parties in order to gain more insight into their business models and strategies and thus be able to fine-tune these at an early stage (ACM 2016b).

Netherlands Institute for Human Rights

The Netherlands Institute for Human Rights (CRvdM) aims to protect human rights – including the right to equal treatment – as well as raise awareness and promote adherence to these rights.[146] Protecting the right to equal treatment is one of the CRvdM’s special tasks. The Institute has taken over this task from the Equal Treatment Commission and can assess individual discrimination cases. We have already seen the questions raised about technological developments affecting fundamental and human rights, such as the high level expert group studying the impact of big data on the right to equal treatment and protection of personal privacy. The CRvdM’s advice on the draft Bill for the Intelligence and Security Services Act questions the impact of extensive powers to collect data on the right to privacy. The Institute’s strategic plan does not refer to the effect of technological developments on human rights (CRvdM 2016). In an interview, the Institute indicated that the impact of technological developments has been discussed in the strategic agenda framework, but that it is focussing on other priorities.[147]

The Review Committee for Intelligence and Security Services

The Review Committee for Intelligence and Security Services (CTIVD) supervises the operations of the General Intelligence and Security Services (AIVD) and Military and Intelligence and Security Services (MIVD) in the Netherlands. The CTIVD thus guards ‘the balance between the interests of national security and that of the protecting the personal privacy of citizens’ (CTIVD 2016:2). The CTIVD examines the legality of operations and data collection by security services, and is called upon as independent advisory committee in cases of complaints about security services’ actions.

The impact of digitization on security service activities is a major topic for the CTIVD. For example, in 2014 the Committee investigated how the AIVD collected data online. Having concluded that the data collection and use of certain powers (such as hacking) were not always well motivated and justified, the Committee recommended better management control mechanisms. The CTIVD argued for strengthening surveillance to guarantee the extension of interception powers under the amended

[145] jaarverslag.acm.nl/jaarverslag-2015/campagne-elke-app-heeft-een-prijs

[146] Netherlands Institute for Human Rights Act (Staatsblad 2011, 573)

[147] Conversation with Jan Peter Loof, 11 May 2016

Intelligence and Security Services Act (Wiv). An independent body should have the mandate to intervene in order to prevent or put a halt to unlawful activities (CTIVD 2016).

Finally, the CTIVD also looks at ways to improve transparency in the security domain – where this can be done responsibly – and thus strengthen the trust in security services' data collection and avoid myths and misunderstandings. In 2016 the CTIVD began a study on notification and insight in security services. The Committee has a great deal of expertise, but states: 'In this age of big data and digitization, we need to do more with intelligence services' (2015:3 CTIVD). For that reason a group of external experts has been formed since 2014 to forge a stronger link – in terms of vision and research – with technical developments as well as social and scientific discussions.

Other supervisors and review committees

The National Cyber Security Centre (NCSC) responds to cyber threats and incidents and is working on strengthening a secure and resilient digital society. Its key focus is the protection and continuity of vital infrastructure (for example energy, water and telecom sectors), so that Dutch society can continue to thrive. It also works on strengthening the awareness and competencies in information security and privacy for citizens, companies and governments. The Cyber Security Council (CSR) is an independent advisory body that monitors the execution of the National Cyber Security Strategy and raises awareness of new topics. The development of the Internet of Things is one of those topics that the CSR will look into from a cyber security perspective in the coming years (CSR 2016).

The Advisory Committee on International Law and Conventional Weapon Use gives advice on the acquisition, possession and use of weapons and looks at the extent to which this is compatible with the international humanitarian laws of war. The Committee also plays a role in advising on the acquisition of autonomous weapon technology and thereby evaluates if there is meaningful human control.

The National Ombudsman assists citizens who are encountering problems with the government. One of the topics on the Ombudsman's agenda is digitization, which it says can be user-friendly for citizens, but also create situations where systems go wrong and data is incorrect or exploited by others. The Ombudsman is working hard to help people who do not have digital skills and therefore risk being exluded from the continually digitizing communation with the government.

International developments

EDPS advisory group on digital ethics

The EDPS supervises European data protection. It advises the European Commission and parliament on legislation and policies concerning privacy and data protection, and collaborates with national supervisors to achieve uniform European data protection.

The EDPS has played an active role in creating the General Data Protection Regulation (EU 2016/679), which contains new measures to strengthen the protection of personal data. At the end of 2015, EDPS published its opinion in *Towards a new digital ethics*, in which it drew attention to the role of technological developments such as algorithms, AI, big data and IoT (EDPS 2015). It is difficult for individuals to be able to avoid data collection as surveillance by governments seems to be expanding and profiling creates risks of stigmatization and exclusion. This raises the question of whether people still have the freedom to develop themselves without being classified and profiled. According to the EDPS, the current principles of data protection alone are no longer adequate to protect human dignity online. The EDPS would like to see more focus on the ethical dimension of data processing, including the impact of data on freedom, dignity and the functioning of democratic processes. It highlights four major topics: 1) future-proof regulations; 2) accountability of organizations that process data; 3) privacy awareness of engineers and programmers who develop software; and 4) empowerment for individuals to be able to make their own decisions about their data. In addition, the EDPS will set up an ethics advisory group to explore the relationship between human rights, digital technology and business models in the twenty-first century. The step towards digital ethics requires reflection on the role of the supervisor and the principles that shape its work. In the coming years the EDPS wants to concentrate more on responsible activities rather than 'mechanically following the letter of the law' (EDPS 2015a: 11). So not just the substantive issue of ethical challenges is on the agenda, but also the governance requirement to organize monitoring and the supervisor's mandate.

Table 5 Activities in the political administrative domain to implement policy

Who/what	Technology	Issue	Action
AP	Digitization (services that process personal data)	Privacy, data protection	Supervize government & industry data processing
ACM	Internet, apps	Privacy, balance of powers	Awareness campaign privacy, power of Internet providers
CRvdM	-	Human rights (specific focus on discrimination)	-
CTIVD	Security technology	Privacy, data protection, security	Supervize security services
NCSC / CSR	Digitization	Security	Encourage secure and resilient digital society
AIRCW	Weapon technology	Autonomy, control of technology, human dignity	Advise meaningful control of weapon systems
National ombudsman	Digital goverment services	Autonomy, human dignity	Complain when digital government systems go wrong
EU and international			
EDPS	Digitization (services that process personal data)	Expand privacy to autonomy, human dignity, discrimination	Advisory group digital ethics, acknowledge impact of digitization on human rights

Bibliography

ACM (2014) ACM Agenda 2014-2015. Den Haag: ACM. acm.nl/nl/organisatie/missie-visie-strategie/onze-agenda/acm-agenda-2014-2015/

ACM (2016a) ACM Agenda 2016-2017.Den Haag: ACM. acm.nl/nl/organisatie/missie-visie-strategie/onze-agenda/acm-agenda-2014-2015/

ACM (2016b) Grote platforms, grote problemen? Een beschouwing van online platforms vanuit Mededingingsperspectief. Den Haag: ACM

AIV (2012) Digitale oorlogsvoering. No 77, AIV/No 22, CAVV December 2011. Den Haag: Adviesraad Internationale Vraagstukken.

AIV (2014) Het Internet. Een wereldwijde vrije ruimte met begrensde staatsmacht. No. 92. Den Haag: Adviesraad Internationale Vraagstukken.

AIV (2015) Autonome Wapensystemen. De noodzaak van betekenisvolle menselijke controle. No. 97 AIV / No. 26 CAVV. Den Haag: Adviesraad Internationale Vraagstukken.

AP (2015) *Jaarverslag 2015.* Den Haag: Autoriteit Persoonsgegevens.

AP (2016) *AP Agenda 2016.* Den Haag: Autoriteit Persoonsgegevens.

Article 29 Data Protection Working Party and the Working Party on Police and Justice (2011) The Future of Privacy. WP 168

Bennet, C.J. & C. Raab (2006) *The governance of privacy: Policy instruments in global perspective.* Massachusetts: MIT Press.

Beuth, P (2016) Bundesregierung will mehr über Googles Algorithmus wissen. In: *Die Zeit*, 13-05-2016. http://www.zeit.de/digital/internet/2016-05/transparenz-algorithmen-bundesregierung-google-facebook/komplettansicht

Bits of Freedom (2015) *Jaarverslag 2015. Connected we stand.* Amsterdam: Bits of Freedom.

Boka (2016) Facebooks Research Ethics Board Needs to Stay far Away from Facebook. In: Wired, 23 June 2016. wired.com/2016/06/facebooks-research-ethics-board-needs-stay-far-away-facebook

CBP (2013) *Jaarverslag 2013: Het CBP in zich.,* Den Haag: College Bescherming Persoonsgegevens.

CBP (2014) *Jaarverslag 2014: Het CBP in zicht.* Den Haag: College Bescherming Persoonsgegevens.

CBP (2015) *CBP Agenda 2015.* Den Haag: College Bescherming Persoonsgegevens.

CPB (2014) *Kiezen voor Privacy: Hoe de markt voor persoonsgegevens beter kan*. CPB Policy Brief, Den Haag: CPB

College voor de Rechten van de Mens (2016) Strategisch Plan 2016-2019, Utrecht: College voor de Rechten van de Mens.

Commissie Franken (2000) *Commissie grondrechten in het digitale tijdperk*. Den Haag.

Consumentenbond (2015) *Jaarverslag 2015*. Den Haag: Consumentenbond.

CTIVD (2015) *Jaarverslag 2014-2015*. Den Haag: Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten.

CTIVD (2016) *Jaarverslag 2015.* Den Haag: Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten.

Cyber Security Raad (2016) Werkprogramma 2016. De toekomst is dichterbij dan je denkt. Den Haag: CSR.

D66 (2016) *Concept-verkiezingsprogramma. Samen sterker - kansen voor iedereen*. Den Haag: D66.

Digital Government Review (2014) *Making Digital Government Work for Everyone*. 25 November 2014.

Dommering, E.J. (2011) Een nieuw voorstel tot aanpassing van de Grondwet. *Computerrecht* 2, pp. 52-55.

Dratwa, J. (Ed.) (2014) *Ethics of Security and Surveillance Technologies. Opinion No. 28 of the European Group on Ethics in Science and New Technologies*. Brussels, 20 May 2014.

EC (2013) *The Onlife Manifesto*: Being Human in a Hyperconnected Era. ec.europa.eu/digital-single-market/sites/digital-agenda/files/Manifesto.pdf

ECP (2015) *De volwassen informatiesamenleving. Het nieuwe normaal.* Visiedocument ECP. December 2015.

EDPS (2015) Towards a new digital ethics: Data dignity and technology. *Opinion 4/2015*, Brussels : European Data Protection Supervisor.

EDPS (2015a) *Leading by Example: The EDPS strategy 2015-2019* Brussels: European Data Protection Supervisor.

EDPS (2016) *EDPS starts work on a New Digital Ethics*. EDPS/2016/05, Brussels, 28 January 2016 Press Release.

EDRi (2014) The Charter of Digital Rights. *The EDRi papers* 10, Brussels: European Digital Rights Initiative.

Eskens, S., J. Timmer, L. Kool & R. van Est (2016) Beyond Control: *Exploratory study on the discourse in Silicon Valley about consumer privacy in the Internet of Things,* The Hague: Rathenau Instituut.

Est, R van (2014) *Intieme technologie: De slag om ons lichaam en gedrag,* Den Haag: Rathenau Instituut.

Est, R. van, D. Stemerding, V. Rerimassie, M. Schuijff, J. Timmer & F. Brom (2014) *From Bio to NBIC convergence – From medical practice to daily life; Report written for the Council of Europe, Committee on Bioethics,* The Hague: Rathenau Instituut.

Est, R. van & L. Kool (red.) (2015) *Werken aan de robotsamenleving. Visies en inzichten uit de wetenschap over de relatie technologie en werkgelegenheid*, Den Haag: Rathenau Instituut.

Est, R. van & V. Rerimassie (2014) *Strijd om onze intimiteit. Het Bericht,* Den Haag: Rathenau Instituut.

Est, van R. & D. Stemerding (2012) *Making Perfect Life: Final Report. European Governance Challenges in 21st Century Bio-engineering,* Brussels: STOA

Forus, A. (2014) Preface Committee on Bioethics of the Council of Europe by Chair DH-BIO. In: R. van Est, D. Stemerding, V. Rerimassie, M. Schuijff, J. Timmer & F. Brom (2014) *From Bio to NBIC convergence – From medical practice to daily life; Report written for the Council of Europe, Committee on Bioethics*, The Hague: Rathenau Instituut.

GCIG (2016) *Our Internet. Global Commission on Internet Governance*, Ontario / London: Centre for International Governance Innovation / Chatham House.

Geesink, I., M. Heerings & S. van Egmond (red.) (2016) *De meetbare mens: Het digitaal meten van het zieke en gezonde lichaam*, Den Haag: Rathenau Instituut

Gezondheidsraad (2006) *Betekenis van nanotechnologieën voor de gezondheid*, Den Haag: Gezondheidsraad; publicatie nr. 2006/06. ISBN 90-5549-593-X

Hof, C. van 't, J. Timmer & R. van Est (red.) (2012a) *Voorgeprogrammeerd: Hoe internet ons leven leidt,* Boom Lemma.

Hof, C. van 't, J. Timmer & R. van Est (2012b) *Het Bericht: Voorgeprogrammeerd – Online keuzevrijheid onder druk*, Den Haag: Rathenau Instituut.

IEEE (2016) *The Global Initiative for Ethical Consideration in the Design of Autonomous Systems*. IEEE. standards.ieee.org/develop/indconn/ec/ec_about_us.pdf

Janssen, A., L. Kool & J. Timmer (2015) *Dicht op de huid. Gezichts- en emotieherkenning in Nederland*, Den Haag: Rathenau Instituut

Kiss, J. (2014) An online Magna Carta: Berners-Lee calls for bill of rights for web. In: *The Guardian*, 12 March 2014. theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web

Kool, L., J. Timmer & R. van Est (2013) *Keuzes voor de e-coach: Maatschappelijke vragen bij de automatisering van de coachingspraktijk*. Den Haag: Rathenau Instituut.

Kool, L., J. Timmer & R. van Est (2015) *De data-gedreven samenleving: een achtergrondstudie*. Den Haag: Rathenau Instituut

Kool, L., J. Timmer & R. van Est (red.) (2014) *Eerlijk advies: De opkomst van de e-coach*. Den Haag: Rathenau Instituut.

Koops, E.J. (2011) Digitale grondrechten en de Staatscommissie: op zoek naar de kern. In: *Tijdschrift voor Constitutioneel Recht,* 2 (2), p.168-185.

Kreijveld, M., J. Deuten & R. van Est (red.) (2014) *De kracht van platformen: Nieuwe strategieën voor innoveren in een digitale wereld.* Den Haag/Deventer: Rathenau Instituut/Vakmedianet.

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 u.a.: Springer Open 2015, pp. 1-8.

Lucas, A. (2016) *Robotisering zonder achterblijvers*. Den Haag: VDD

Martijn, M. (2016) Deze professor probeert privacy opnieuw uit te vinden en dat is broodnodig. In: *De Correspondent,* 8 augustus 2016. decorrespondent.nl/5043/Deze-professor-probeert-privacy-opnieuw-uit-te-vinden-en-dat-is-broodnodig/155102508-199b13c9

Messer, P. (red.) (2012) *Robotrevolutie vraagt om actie. Het Bericht.* Den Haag: Rathenau Instituut.

Mulgan (2016) *A machine intelligence commission for the UK: how to grow informed public trust and maximise the positive impact of smart machines*, London: Nesta.

Moerel, L. (2015) Zo behouden alleen de rijken hun privacy. In: *NRC Handelsblad*, 28 november 2015. nrc.nl/nieuws/2015/11/28/zo-behouden-alleen-de-rijken-hun-privacy-1561104-a579887

Munnichs, G. & J. Bos (2016) *Digitalisering van dieren: Verkenning Precision Livestock Farming.* Den Haag: Rathenau Instituut.

Nanopodium (2011) *Verantwoord verder met nanotechnologie. Bevindingen maart 2009 – januari 2011*, Eindrapport Commissie Maatschappelijke Dialoog Nanotechnologie. Amsterdam: Nanopodium

NJV (2016) Homo Digitalis. In: *Handelingen Nederlandse Juristen-Vereniging* 146, Alphen aan de Rijn: Wolters-Kluwer.

Noort, W. van (2016) We bouwen aan een dictatuur van data. In: *NRC Handelsblad*, 19 augustus 2016. nrc.nl/nieuws/2016/08/19/we-bouwen-aan-een-dictatuurvan-data-3869694-a1517117\

Nouwt, J., P.H. Blok, B.J. Koops, M.H.M. Schellekens, E. Schreuders & M. de Vries (2000) Grondrechten in het digitale tijdperk. In: *Nederlands Juristenblad* 75(27), pp. 1321-1327.

Onderwijsraad (2015) *Meerjarenagenda 2015–2020, werkprogramma 2016.* Den Haag: Onderwijsraad.

Pollicino, O. & M. Bassini (2015) A*n Internet Bill of Rights? Pros and cons of the Italian way. London School of Economics – Media Policy Project Blog*. blogs.lse.ac.uk/mediapolicyproject/2015/08/05/an-internet-bill-of-rights-pros-and-cons-of-the-italian-way

Prins, J.E.J. (2015) Grondrechten en digitalisering. In: *Nederlands Juristen Blad* 2015/403, afl. 8, p. 419.

Privacy First (2015) *Eigen keuzes in een vrije omgeving. Jaarverslag 2015.* Amsterdam: Privacy First.

Raad voor de Rechtspraak (2014) *Advies grondwetswijziging recht op eerlijk proces.* Den Haag: Raad voor de Rechtspraak.

Radboud Universiteit (2016) Bart Jacobs zet digitale beveiliging op de kaart. ru.nl/onderzoek/over/vm/onderzoeksthema'/informatica-digitale/vm/professor-bart

Rli (2015a) *Werkprogramma 2015-2016*. Den Haag: Raad voor de leefomgeving en infrastructuur.

Rli (2015b) *Verkenning technologische innovaties in de leefomgeving*. Den Haag: Raad voor de leefomgeving en infrastructuur.

Rli (2016) *Werkprogramma 2016-2017.* Den Haag: Raad voor de leefomgeving en infrastructuur.

Royakkers, L., F. Daemen & R. van Est (2012) *Overal robots. Automatisering van de liefde tot de dood.* Den Haag: Boom Lemma.

Royakkers, L. & R. van Est (2016) *Just ordinary robots: Automation from love to war*. Boca-Raton, FL: CRC Press.

Salvi, M. (red.) (2012) *Ethics of information and communication technologies. European Group on Ethics in Science and New Technologies to the European Commission. Opinion No 26*. Brussels, 22 February 2012.

Shead, S. (2016) The biggest mystery in AI right now is the ethics board that Google set up after buying DeepMind. *Business Insider*, 26 March 2016. uk.businessinsider.com/google-ai-ethics-board-remains-a-mystery-2016-3

Solove, D.J. (2002) Conceptualizing Privacy. In: *California Law Review* 2002(4), pp. 1087-1156.

Ten Oever, N. & C. Cath (2016) Research into Human Rights Protocol Considerations. Internet Draft. IETF. tools.ietf.org/pdf/draft-tenoever-hrpc-research-04.pdf

Timmer, J., I. Elias, L. Kool & R. van Est (2015) *Berekende risico's: Verzekeren in de data-gedreven samenleving*. Den Haag: Rathenau Instituut

Timmer, J. & L. Kool (red.) (2014) *Tem de Robotauto: De zelfsturende auto voor publieke doelen*. Den Haag: Rathenau Instituut.

Timmer, J., J. Smids, L. Kool, A. Spahn & R. van Est (2013) *Op advies van de auto: Persuasieve technologie en de toekomst van het verkeerssysteem*. Den Haag: Rathenau Instituut

Verhey, L.F.M. (2011) Grondrechten in het digitale tijdperk: driemaal is scheepsrecht? In: *Tijdschrift voor Constitutioneel Recht,* 2(2), pp.152-167.

Verbond van Verzekeraars (2016) *Grip op data.* Green Paper Big data. Den Haag: Verbond van Verzekeraars.

Verhoeven, K., M. van Vliet, N. Mastenbroek, M. van Dieijen, D. van Egmond & O. Arts (2016) *Techvisie D66*. Den Haag: D66.

Whittall, H., L. Palazzani, M. Fuchs & Gazsó, A. (Conference's rapporteurs to the Committee on Bioethics) (2015) *Report of the International conference on Emerging technologies and human rights. Strasbourg, 4-5 May 2015*. Strasbourg: Council of Europe, DH-BIO.

WRR (2011) *iOverheid*. Rapport 86. Amsterdam: Amsterdam University Press.

WRR (2015) *De publieke kern van het internet. Naar een buitenlands internetbeleid*. Rapport 94. Amsterdam: Amsterdam University Press

WRR (2015) *De robot de baas. De toekomst van werk in het tweede machinetijdperk*. Verkenning 31. Amsterdam: Amsterdam University Press.

WRR (2016) *Big Data in een vrije en veilige samenleving.* Rapport 95. Amsterdam: Amsterdam University Press.

Zoeteman, C. & I. Widdershoven-Heerding (2007) Bio-ethiek: uniformiteit of maatwerk? COGEM Jaarverslag 2006, pp. 30-33.

Appendix B: The meaning of public governance

> *Governance is about efforts to align or bring about concerted action across multiple, competing institutional modes of social coordination for public purpose (O'Toole 2000: 278).*

Governance as social control

Ethylmologically, 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 thus avoid risks and unwanted outcomes (Hoppe 2010, 10). Public governance is therefore essentially all about social control. Trying to define such a multifaceted concept as governance is not easy in the extensive literature. We introduce a number of insights and concepts from that literature that can help us to consider the governance of the social and ethical aspects of science and technology.

Governance of public issues

Governance aims 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 to seek potential solutions. The free exchange of arguments and exercising of 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: underpinning the problem, seeking political support and participation (summarized as *puzzling, powering, participation*). The first process is using for example scientific knowledge to assess the problem well and ascertain whether it is 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 put the problem on the political and policy agenda? The problem is namely 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 institutions' solutions and instruments? Which public interests or values are better articulated and represented?

From the perspective of a democratic state, governance should fulfil a number of condiitons. Realising that there are many 'failing' or 'fragile' states all over the world, in 1994 the World Bank developed the concept of *good governance*: 'Governance is epitomized by predictable, open, and enlightened policymaking (that is, 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 defnition is still valid. Central to this is how the government interacts with society.

Governance designing interaction 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 parties. The government is a network partner and controls in interaction with other parties, applying a very diverse and extensive combination of formal and informal practices. Alongside traditional forms of *command & control*, it is also about stimulating public debate, negotiations, collaboration, joint vision development and forming of alliancies (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 cooperated for a very long time with actors in society. However, in recent decades the desire for governance has grown because of digitization, privatization and internationalization (Hajer et al. 2004).

There are several governance concepts circulating that refer to certain types of interaction between the government and civil society actors. These include *multi-stakeholder governance* and *network governance*. With multi-stakeholder governance, actors in industry, society and government together develop a joint approach for issues that affect them all, but are too complex to tackle effectively without collaboration. We already mentioned internationalization. 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. The dynamics are captured under 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 civic society groups, the term *deliberative governance* is also 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 laborious political-administrative handling of sensitive social problems and in situations where there is mutual distrust and an exchange of arguments is lacking (Hajer et al. 2004). Deliberation can be a way to build up institutional trust and seek workable solutions.

Meta-governance of the governance ecosystem

Thus governance 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 view governance as how it is handled by the government. We must keep a watchful eye on the entire system of governance arrangements in society in order to recognise, to discuss, to investigate and to address public concerns and find solutions which we implement and evaluate. Importantly, to organize such procedures legitimately and effectively, the range of institutes, administrative and social processes involved must be diverse. Together these form what we call a governance ecosystem.

The issue with governance is therefore whether the current governance ecosystem, being the entire governance arrangements surrounding a particular public problem, is working well. According to Hoppe (2010), two search processes play a role in improving a governance ecosystem. The first concerns the institutes. Certainly where new problems arise, there is often a lack of institutes. Hajer & Wagenaar (2003) spreak of an 'institutional void', when shared normative frameworks and organizational competencies are lacking and it is not clear who is responsible for what. Sociologist Ulrich Beck refers to this as 'organized irresponsibility' (Beck 1988), which he sees as a key feature of our high-tech risk society (Beck 1992). Establishing institutes 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* because it is all about controlling the governance of problems, or rather the structuring of the goverance ecosystem in which collective problems can be identified and addressed. The second search process is organizing social involvement that resonates with the perceptions of ordinary citizens.

Relevant questions from a governance perspective

The above brief introduction raises numerous questions concerning the meaning of governance as well as meta-governance of problems (how the governance ecosystem is structured and how it works).

The questions regarding the governance of problems include:

- What public problems are 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 put on the political or other agenda?
- Which parties have been involved in the debate and shaping policy?
- What solutions have been proposed and institutionalized?

The questions regarding the meta-governance of problems include:

- What institutes are there to discuss public problems and raise them at a political level?
- In what ways does consultation take place between public and private actors, and between governments, ordinary citizens and civil society organizations?
- In what way are public values institutionally safeguarded?
- Which institutes have been established over the years to achieve this?
- What does the governance ecosystem for a particular issue look like?

Bibliography

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 (ed.) (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.

Appendix C: The experts consulted

Name	Organization
Herm van der Beek	Ministry of Economic Affairs
Arie van Bellen	ECP
Vincent Böhre	Privacy First
Frans Brom	Scientific Council for Government Policy (WRR)
Corinne Cath	Article 19 human rights organization
Peter Ester	Senate member Christenunie
Bas Filippini	Privacy First
Valerie Frissen	SIDN Fund
Arda Gerkens	Senate member SP
Hielke Hijmans	European Data Protection Supervisor
Mireille Hildebrandt	Free University of Brussels
Jan Peter Loof	Netherland Institute for Human Rights
Ben van Lier	Centric
Françoise Rost van Tonningen	Rabobank
Cristiane Woopen	University of Cologne; outgoing Chair of German Ethics Council

Rathenau Instituut

In addition, we would especially like to thank the guidance committee for this research, who provided us with valuable insights and advice.

Name	Organization
Dr. mr. Heleen Janssen	Ministry BZK, Constitutional Affairs & Legislation
Dr. mr. Meine Henk Klijnsma	Ministry BZK, Constitutional Affairs & Legislation
Prof. mr. Corien Prins	Tilburg University, Director Rathenau Instituut
Prof. dr. Jeroen van den Hoven	Delft University of Technology / 3TU
Prof. dr. Inez de Beaufort	Erasmus MC
Prof. dr. Victor Bekkers	Erasmus University

Rathenau Instituut

About the authors

Rinie van Est, whose background is in Applied Physics and Political Science, is research coordinator at Rathenau Instituut. He identifies new developments in science, technology, politics and society and is involved in emerging technologies such as nanotechnology, biotechnology, information technology and cognitive sciences as well as the complex issue of energy. In 1999, Rinie graduated with his dissertation *Winds of Change*, comparing the politics, technology and economy of wind energy innovation in California and Denmark. He is also a lecturer at Eindhoven University of Technology's School of Innovation Sciences. His recent publications include: *Rules for the digital human park* (2016), *Working on the robot society (2015), Intimate technology: the battle for our body and behaviour* (2014) and *Just ordinary robots: Automation from love to war,* published by Routledge in 2016.

Linda Kool is a senior researcher and project leader at Rathenau Instituut. She conducts research on social issues with digital innovations such as Big Data, Internet of Things, Artificial Intelligence, robotics and persuasive technology. Linda studied Social Science Informatics at the University of Amsterdam and has a Master's in European Studies of Society, Science and Technology from Maastricht University and the University of Oslo. She previously worked on privacy and ICT issues at the Netherlands Organisation for Applied Scientific Research (TNO). Linda is a columnist for the magazine 'InGovernment' and her publications include: *Rules for beyond the digital human park* (2016)*, Beyond Control* (2016) about privacy and the Internet of Things, *Working on the robot society* (2015), *Dicht op de huid* (2015) face and emotion recognition in the Netherlands, *Data driven society* (2015) and *Eerlijk Advies* (2014) on the emergence of e-coaches.

Lambèr Royakkers is Associate Professor in the ethics of technology at Eindhoven University of Technology. He studied Technical Mathematics, Philosophy and Social Sciences at Eindhoven, and then Law at the University of Tilburg, where he obtained his PhD with a thesis on normative rules with deontic logic. In recent years, Lambèr has been working on military ethics, robot ethics, deontic logic and moral responsibility in research networks. He is also co-founder of the National Institute of Ethics Training (LIvET) and author and co-author of more than ten scientific works, including *Just ordinary robots: Automation from love to war* (2016), *Moral Responsibility and the Problem of Many Hands* (2015), *Ethics, Engineering and Technology* (2011).

Jelte Timmer was a researcher at Rathenau Instituut until March 2017. He looked at the social and ethical impact of digital innovations such as social media, Internet of Things, face recognition technology, big data and persuasive technology. Jelte studied Social Psychology at Utrecht University, and has a Master's in Arts Policy and Management and in New Media and Digital Culture. He was involved in the start-up and is still on the Advisory Board of the Utrecht Centre for new media and digital culture SETUP. He has written many articles and worked on many publications about digital innovations, such as reports on the ethical aspects of digitization for the Council of Europe (*From Bio to NBIC convergence, 2014*), and for the Global Summit of National Ethics Committees (*Rules for the digital human park*, 2016). Other recent publications are *Eerlijk Advies* (2014) about digital behaviour, *Berekende risico's* (2015) and *Tem de robotauto* (2014).

Who was Rathenau?

The Rathenau Instituut is named after Professor G.W. Rathenau (1911-1989), who was successively professor of experimental physics at the University of Amsterdam, director of the Philips Physics Laboratory in Eindhoven, and a member of the Scientific Advisory Council on Government Policy. He achieved national fame as chairman of the commission formed in 1978 to investigate the societal implications of micro-electronics. One of the commission's recommendations was that there should be ongoing and systematic monitoring of the societal significance of all technological advances. Rathenau's activities led to the foundation of the Netherlands Organization for Technology Assessment (NOTA) in 1986. In 1994 this organization was renamed 'the Rathenau Instituut'.

Het **Rathenau instituut** stimuleert de publieke en politieke meningsvorming over de maatschappelijke aspecten van wetenschap en technologie. We doen onderzoek en organiseren het debat over wetenschap, innovatie en nieuwe technologieën.

Rathenau Instituut
Onderzoek & dialoog | Wetenschap, technologie en innovatie