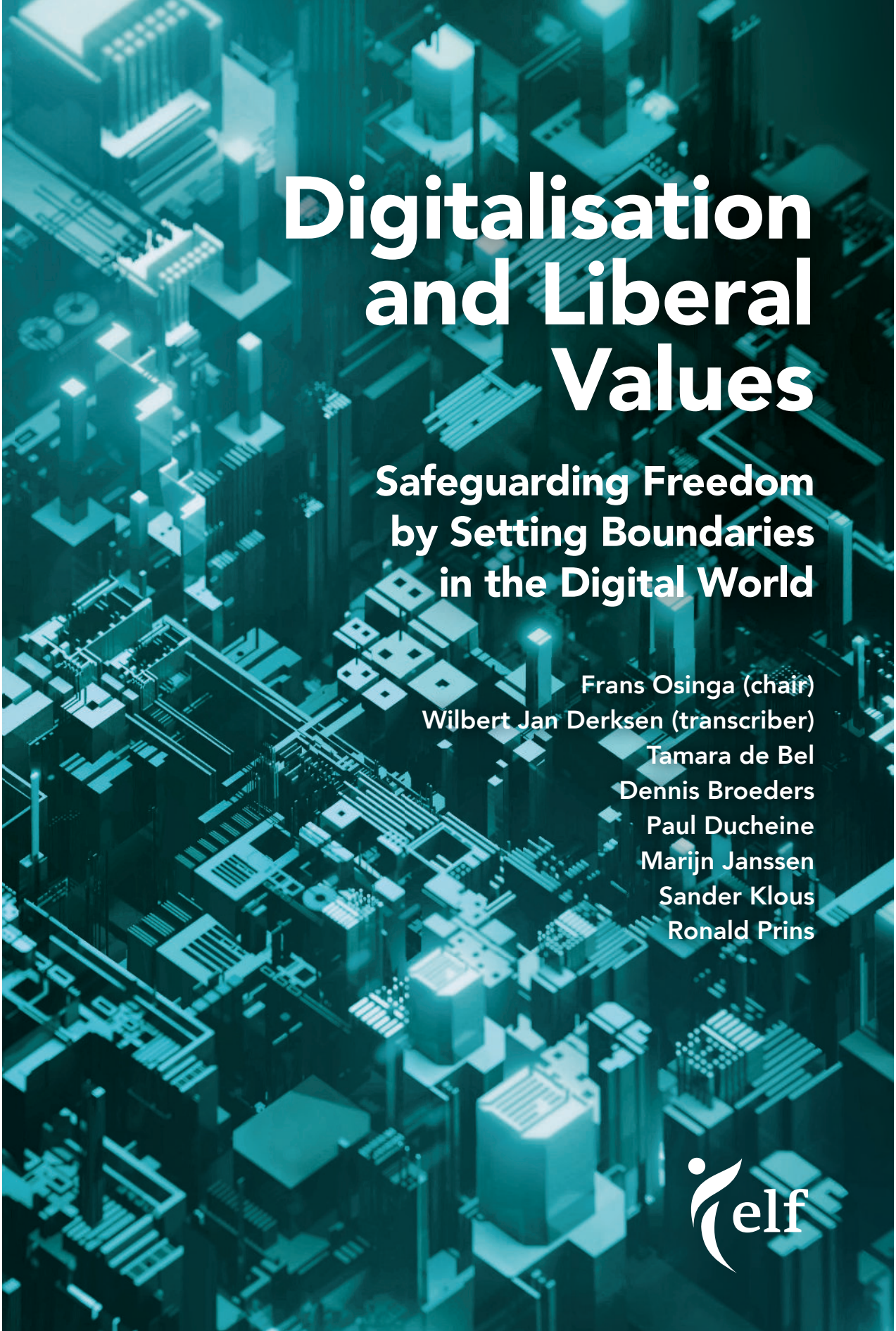

Digitalisation and Liberal Values

Safeguarding Freedom by Setting Boundaries in the Digital World

Frans Osinga (chair)
Wilbert Jan Derksen (transcriber)
Tamara de Bel
Dennis Broeders
Paul Ducheine
Marijn Janssen
Sander Klous
Ronald Prins

elf

Digitalisation and Liberal Values

Frans Osinga (chair), Wilbert Jan Derksen (transcriber),
Tamara de Bel, Dennis Broeders,
Paul Ducheine, Marijn Janssen, Sander Klous and
Ronald Prins

Digitalisation and Liberal Values

Safeguarding Freedom by Setting Boundaries in the Digital World

elf

The European Liberal Forum (ELF) is the official political foundation of the European Liberal Party, the ALDE Party. Together with 56 member organisations, we work all over Europe to bring new ideas into the political debate, to provide a platform for discussion, and to empower citizens to make their voices heard. ELF was founded in 2007 to strengthen the liberal and democrat movement in Europe. Our work is guided by liberal ideals and a belief in the principle of freedom. We stand for a future-oriented Europe that offers opportunities for every citizen. ELF is engaged on all political levels, from the local to the European. We bring together a diverse network of national foundations, think tanks and other experts. At the same time, we are also close to, but independent from, the ALDE Party and other Liberal actors in Europe. In this role, our forum serves as a space for an open and informed exchange of views between a wide range of different actors.

Frans Osinga (chair), Wilbert Jan Derksen (transcriber), Tamara de Bel, Dennis Broeders, Paul Ducheine, Marijn Janssen, Sander Klous and Ronald Prins
Digitalisation and Liberal Values
Safeguarding Freedom by Setting Boundaries in the Digital World

European Liberal Forum (ELF)
Brussels
2024
173 p. – 16 x 24 cm
ISBN 978-2-39067-071-1
NUR 740/980

Published by the European Liberal Forum in cooperation with the Prof. mr. B.M. TeldersStichting . The publication received financial support from the European Parliament. The views expressed herein are those of the author(s) alone. The European Parliament is not responsible for any use that may be made of the information contained therein.

Produced by Gompel&Svacina bv
Nationalestraat 111, B-2000 Antwerpen, info@gompel-svacina.eu

Table of Contents

Foreword

I only just got to experience the workplace of the pre-digital era. In 1982, when I started working, letters were still written by hand and typed up by secretaries, and we communicated with offices abroad via telephone and telex. *Spreadsheets* were still A3 graph paper sheets, filled in using a pencil. Data was collected by armies of analysts scouring libraries and archives, or issuing telephone requests for data to be sent by post. What you ended up receiving a few weeks later was usually exactly what you didn't need!

A few years later, the PC made its first inroads. The screen was the size of a cigarette packet and it was almost impossible to get the system to communicate with other devices. Over the next few years, all this changed with the roll-out of the internet. This invention not only transformed the workplace, but the entire world. Since then, digitalisation has radically altered society.

It offers countless benefits. We always have information at our fingertips and any number of *apps* have improved daily life and made things easier. Things like algorithms, artificial intelligence, *big data*, digital platforms and biometric technology have transformed society and the economy. We produce better, smarter and more economical products. Digital healthcare applications save both doctors and patients time and effort. As well as improving diagnoses, they provide new possibilities for medical interventions. Digitalisation also plays a major role in education nowadays, as the Covid-19 pandemic made abundantly clear. We increasingly shop online and manage our financial affairs through online banking. Furthermore, we are at the start of a new digital revolution centred around developments like the *internet of things*, artificial intelligence, neurotechnology and robotisation.

Behind all these digital technologies, there are a number of choices when it comes to certain values. These include efficiency, accessibility, quality, profit and sustainability. As such, digitalisation has become a tool for pursuing certain goals and values. However, this process also raises questions surrounding some of these values. For example, when it comes to privacy, autonomy, security, equal treatment and democracy. This text explores how key liberal values could form the basis for digitalisation policy. While acknowledging the opportunities that digitalisation offers, the authors also want to highlight certain risks it presents and the implications this can have society. If we identify, manage and mitigate these risks now, future generations will also be able to enjoy the full benefits of digitalisation and the possibilities it gives us.

Robert Reibestein
Chair of the Board of Governors of the TeldersStichting

1. Introduction

1.1 Why this book?

The future is digital. This motto sums up how digitalisation has become the key concept at the heart of many ambitious plans in both the private and public sectors. The European Union (EU) has named this decade 'Europe's Digital Decade', as it aims to secure a strong and sustainable digital future.[1] In 2019, total revenue in the European ICT market was estimated at some 1,085 billion euros.[2] Now, just a few years later, and given the sector's continued strong growth, we can only expect it to grow more in the years to come. Furthermore, ICT has a crucial role to play in the national and international value chains of other economic sectors. Digitalisation, thereby, increases prosperity in our society. It has also made our lives easier and more comfortable in countless ways. Think of smartphones now that allow us to make calls, transfer payments, find directions, exchange files, along with numerous other useful applications and functionalities. Digitalisation is fundamental to so much that matters to us as individuals and to society as a whole. We can no longer imagine life without all the possibilities that digitalisation offers. Nonetheless, digitalisation is not always reflected positively in the media, with countless news reports covering topics that range from data breaches to ransomware attacks, disinformation, and biased algorithms.

---

1. European Commission, 'Europe's Digital Decade: digital targets for 2023', URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en#the-path-to-the-digital-decade, accessed: 17 July 2023.
2. Statista, 'Revenu from the digital ICT market in Europe from 2012 to 2019', URL: https://www.statista.com/statistics/268648/revenue-in-the-digital-ict-market-in-europe-since-2005/, accessed: 17 July 2023.

Digital technological innovations are changing society at a rapid pace and politics often struggles to keep up. The lack of knowledge among policy makers surrounding the effects of digitalisation on society, is a frequent cause for concern, and there are doubts as to whether politicians give it enough importance. Often, a long-term vision that adequately identifies risks is lacking. All the same, change is underway. Until recently, digitalisation was generally always considered the domain of technical experts, but politicians are becoming increasingly aware that it raises important questions about a number of underlying societal issues. As a result, digitalisation is a subject that we increasingly see on the political agenda.

The implications of digitalisation go beyond mere policy issues. They force us to think about people and society at a far more fundamental level. Digitalisation raises interesting new political-philosophical issues for liberalism as a whole. It has altered the dynamics of our society in a host of new ways that require close evaluation. Liberalism offers a value system that can serve as a platform for these evaluations to be made. To that end, The TeldersStichting sees the urgency of conducting a study into the meaning of liberal values in a digital society. As we saw earlier, there are many positive aspects to digitalisation. In this book however, the focus is predominantly on the risks involved, as this is where the major political challenges lie. The main aim of this publication is to formulate a liberal vision on issues surrounding digitalisation. How can liberal principles guide policy makers in this complex social transition, in both the short and the long term? In answering this question, we re-explore the relevance of liberalism, including in the digital future.

1.2 Major trends in digital society

Throughout history, technology has had far-reaching consequences on people and society. Think of inventions like the wheel, irrigation, gunpowder, printing technology, steam engines, cars, radio, television and household appliances. This has shown, time and again, that while people may shape technology, technology also shapes people. Time and again, new technologies have led us to reshape our lives. However, technological developments have not only brought about progress, but also major

social disruption, in both positive and negative ways. Since the advent of the computer, and later the Internet, a process of digitalisation has been taking place throughout society. The digital (virtual) world has become a major realm of our daily lives, alongside our cognitive (mental) and physical (material) worlds.[3] Digitalisation has also shown that, while it can provide great societal opportunities, it can also be highly disruptive. This is why the United Nations has stated that digitalisation can make the world fairer, more peaceful and more just, while it can also threaten privacy, erode security and fuel inequality in the world.[4]

The World Economic Forum also sees opportunities for economic growth, emancipation, healthcare and sustainability through digitalisation, while simultaneously warning for risks of cyber attacks, misuse of personal data and manipulation of democratic processes.[5] The World Economic Forum has called this the 'fourth industrial revolution'. The first three industrial revolutions were based respectively on steam, electricity and information technology. The current, fourth industrial revolution is building upon its predecessor, but stands out through the unprecedented scale, speed and impact with which this information technology is applied. This transformation affects nearly every sector and impacts society as a whole. The boundaries between the physical, digital and biological worlds are becoming increasingly blurred.[6]

Europe has ambitious plans in the arena of digitalisation. Both the EU and all its member states strive to make optimal use of all the possibilities that digital technologies provide. The societal impact of digitalisation is already clear. This is only going to increase in the near future with

3. P. Ducheine, 'Het bevorderen en beschermen van nationale belangen in een democratische rechtsstaat in het informatietijdperk', in: M. Assies et al. editors, *Ordening in de dreiging. Beschouwingen over internationale veiligheid en de toekomst van de liberale democratie*, Hans van Mierlo Stichting report, The Hague, 2018, pp. 26-33.
4. United Nations, 'The impact of digital technologies', URL: https://www.un.org/en/un75/impact-digital-technologies#:~:text=Digital%20technologies%20have%20advanced%20more,can%20be%20a%20great%20equaliser, accessed: 17 March 2021.
5. World Economic Forum, *Our shared digital future. Building an inclusive, trustworthy and sustainable digital society*, Genève, 2018, p. 7.
6. K. Schwab, 'The Fourth Industrial Revolution: What it means, how to respond', *World Economic Forum,* 14 January 2016, URL: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/, accessed: 17 March 2021.

the emergence of new technologies. Various major trends are apparent. Three of these of particular relevance to this book are discussed below.

The first trend shows us how digitalisation leads to 'datafication'. This means that increasing amounts of 'data' are produced, in both the digital and physical worlds. This data can be organised and analysed, which makes it highly valuable. The advent of the 'Internet of Things' means that increasing numbers of everyday objects – from the 'smart city' to the 'smart house' – are connected to the digital world. We also increasingly use data-generating '*wearable*' technologies, such as 'smart watches'. The boundary between the public space and the private sphere is becoming blurred as the option of disconnecting becomes increasingly illusory.[7] Meanwhile, the networks which allow this data to be transferred from one device to another are also gaining in efficiency and speed. The 5G network will enable all sorts of new data-intensive technology applications, such as 'augmented and virtual reality' (AR/VR). The possibilities that data provides seem to have no limits. It has been said that, ultimately, everything in life consists of data and can therefore be quantified.[8] At the same time, there are risks associated with the protection and reliability of this data. And the data greed among companies and governments to which it gives rise poses real threats, not least to the privacy and autonomy of citizens.

A second noteworthy trend arising from digitalisation is the increase in the use of automated and autonomous technologies. 'Algorithms' allow computer systems to take automated decisions, so that humans barely have a role to play, if at all. There can be advantages to doing away with the need for human intervention. Computing power enables operations based on way more variables than a human could ever process, in a fraction of a second.[9] This facilitates the detailed analysis of complex issues, to arrive at better and more consistently substantiated solutions. The digitalisation of society has rendered the use of algorithms ubiquitous. For example, online search engines employ algorithms to decide which search results a user does or does not see, and banks use

7. K. Gabriels, *Onlife. Hoe de digitale wereld je leven bepaalt,* Tielt, 2016, p. 19.
8. Tegenlicht, 'Technologie als religie' (documentary, *VPRO*, 24 January 2021.
9. S. Blauw, 'Wat is een algoritme?', *De Correspondent*, 2 July 2019, URL: https://decorrespondent.nl/10306/wat-is-een-algoritme/149980270484-745de161, accessed: 19 March 2021.

algorithms to determine whether or not to grant someone a loan. The government also uses algorithms to support or automate particular tasks and decision-making processes. '*Machine learning*', a form of 'artificial intelligence' (AI), takes this even further. Algorithms learn from data to adapt and self-improve in order to reach conclusions that humans could never arrive at unaided.[10] Nowadays, many smartphones have machine learning-based virtual assistants to provide support during use. These include Apple's Siri and the Google Assistant. Also, research is being carried out at the moment into the role that advanced forms of AI might play in military operations.[11] Automated and autonomous technologies can make processes more efficient and also take work off human hands. At the same time, there is a risk that these technologies could influence our lives in undesirable ways, and there are concerns about the lack of transparency among companies and governments regarding their use.[12] These technologies also have the capacity to exhibit unintended bias.

A third trend that takes place in the arena of digitalisation is the emergence of digital vulnerability. We have become increasingly dependent on all these inventive technological applications. The Internet may only be a few decades old, but life without it is almost unimaginable to us now. The Covid-19 pandemic served to highlight how essential these sorts of technologies have become in keeping our economy and society running.[13] This also means that disruptions to them can have far-reaching consequences. All the more so because of the growing interconnectivity between different devices and systems. Extensive digital ecosystems of this sort may be efficient, but they're also vulnerable. This creates dependency chains where damage in one area can radiate out to others.[14] This is a cause for concern, particularly when it comes to critical processes within the telecommunications network, the financial

10. R. van Est, R. de Jong, L. Kool, 'Data doorzien. Ethiek van de digitale transitie in de Nederlandse provincies', Rathenau Instituut report, The Hague, 2019, p. 14.
11. Ministerie van Defensie, *Defensievisie 2035. Vechten voor een veilige toekomst*, The Hague, 2020, p. 22.
12. Tweede Kamer der Staten-Generaal, *Initiatiefnota van het lid Middendorp: Menselijke grip op algoritmen*, The Hague, 2019, pp. 1-2.
13. C. Prins, H. Sheikh, 'Coronacrisis vraagt om debat over digitalisering', *Wetenschappelijke Raad voor het Regeringsbeleid*, URL: https://www.wrr.nl/wrr-en-corona/artikel-coronacrisis-vraagt-om-debat-over-digitalisering, accessed: 29 April 2021.
14. Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Cybersecuritybeeld Nederland (CSBN 2020)*, The Hague, 2020, p. 21.

sector and energy supply. On a smaller scale, cyber incidents can also cause private individuals great distress. For example, in recent times, there has been a significant increase in the number of digital scams.[15] In the last few years, cybercrime has become a serious problem which is all the harder to detect for being carried out in the digital world. '*Cyber security*' has become essential for protecting our devices and networks against such attacks. This requires measures in both the digital and physical world. In a game of cat and mouse, the outcome of which can have major social consequences, we always need to stay a step ahead of any malicious parties.

1.3 Structure of the book

The combination of datafication, the growing use of automated technologies and the emergence of new digital vulnerabilities raises important questions. Many of these issues have previously been addressed in detail in various articles, reports and books. This is true of both the technological and social aspects. This book draws extensively upon all these sources. The added value of this book comes from reflecting upon these themes from a liberal perspective, identifying where liberals foresee dilemmas, and formulating answers that draw on liberal values. The book is structured as follows.

It begins with a deep dive into the five liberal values that can form the starting point in establishing digitalisation policy. This is followed by a discussion about the consequences of digitalisation upon the free market. It then turns to the effects of digitalisation on democracy. This is followed by an examination of the repercussions of the government's digital plans on its relationship with citizens. Subsequently, it looks at how digitalisation affects security within society. Finally, it demonstrates how digitalisation policy can be embedded within general *governance*-strategy. The book ends with a conclusion and a summary of its principal recommendations.

15. 'Grote toename phishing via hulpvraag op WhatsApp', *RTL Nieuws*, 25 January 2021, URL: https://www.rtlnieuws.nl/tech/artikel/5210684/fraude-oplichting-online-aankoop-webwinkel-hulpvraag-whatsapp, accessed: 19 March 2021.

Last but not least, please note that this book is a translation of the original 2022 Dutch edition. Several changes were made in the translation to adapt it to its international readership. However, it still draws extensively upon Dutch examples, both to maintain the readability of the book, and because these examples are illustrative of the situation in other European countries too.

2. Liberal values in a digital society

2.1 A digitalisation policy guided by liberal values

Liberalism was born out of the Enlightenment, in which reason and science took a leading role. One liberal attribute has always been a belief in progress, with great value placed on science and technology as the means to achieve this aim. Technologies are invented by people free to strive to create greater prosperity, freedom and comfort.[1] Liberals want a society that promotes maximum innovation. They believe in a market free of government interference, allowing space for technological developments through a process that the Austrian economist Joseph Schumpeter dubbed: 'creative destruction'. This allows old-fashioned and outdated technologies to be continually replaced by newer, better ones.[2] However, liberals accept that technology not only solves problems, but also creates them. The options available to us are largely determined through technology, and this can both promote and restrict freedom.

This book examines both the pressure being put on liberal values by digital society, and how these values can help determine the right political choices in the digital world. We decided to explore the following five liberal values: privacy, autonomy, security, equal treatment and democracy. All five are deemed essential to liberal thought and we believe that these core values have particular merit as driving forces in digital society. Although we have not explicitly listed freedom as a separate value here, all five of these liberal values influence the freedom of the individual, something liberals attach great importance to. A free society as envisioned by liberals cannot be realised if these core values are not safeguarded. These

1. D.J.D. Dees, G.A. van der List, E.G. Terpstra, *Gentechnologie, een liberale visie*, book by Prof.mr. B.M. TeldersStichting, The Hague, 1994, p. 5.
2. D. Acemoglu, J.A. Robinson, *Why Nations Fail*, London, 2012, p. 84.

five core values are briefly explored below, emphasising their relevance to liberalism. In later chapters, it becomes clear how these liberal values can be taken as the point of departure for a responsible liberal answer to particular developments within digital society.

2.2 Privacy

The legal scholar, Alan Westin, outlined four states of privacy. The first is 'solitude', which is when an individual is physically secluded from a group. The second is 'intimacy', when several individuals are secluded in a small group setting in order to engage in social interactions. The third is 'anonymity', which is about being able to take part in public life without being identified. And the fourth is 'reserve', which is consciously withholding information about oneself.[3] Lawyer Richard Posner asserted that secrecy and concealment are also important aspects of privacy.[4] In his view, a negative side of privacy is that it allows malicious activities to remain hidden. This includes domestic violence, crime and planning terror attacks. The 'right to privacy' in the legal sense is a relatively modern phenomenon. In 1890, lawyers Louis Brandeis and Samuel D. Warren were among the first to speak of a certain right to privacy. They claimed that it was the 'right to be left alone'.[5]

Violations of privacy are sometimes expressed in concrete terms. For example, Dutch law clearly states that you may not listen in on someone's telephone conversations without good cause. In reality, however, privacy is a somewhat more subjective term. Whether someone's privacy is infringed upon is situation-specific. For example, when it comes to someone asking you for your home address, the situation is not the same if they are a close friend or someone you barely know. This also means that the significance of the concept of privacy varies greatly from person to person. Cultural background has an important role to play too. Privacy is also often viewed as a western value. This is because western culture has a strongly individualistic focus. Western tradition is strongly

3. A. Westin, *Privacy and Freedom*, New York, 1967, pp. 31-32.
4. R.A. Posner, 'The right of privacy', *Georgia Law Review*, 1978, no. 3, p. 393.
5. Louis D. Brandeis, Samuel D. Warren, 'The right to privacy', *Harvard Law Review*, 1890, no. 5, p. 193.

focused on individual freedom, particularly since the Enlightenment. Over the years, it has come to form the fundamental basis for liberalism, and it is now deeply embedded in western thinking. But while the West has a strongly individualistic focus, elsewhere in the world this is not always the case.[6] Other places have a more collective ways of thinking, and consequently, privacy is regarded in a different light.[7]

Another major aspect of privacy worth mentioning is its close relationship to technological developments. Beginning with the Industrial Revolution (± 1760-1840), a range of technologies have been introduced with drastic consequences for the privacy of citizens. These include the photo camera and the industrial printing press which allowed newspapers – and thus gossip – to be circulated on a mass scale. The totalitarian regimes of the first half of the 20th century were the first to use these technologies on a wide scale to monitor and control their populations. In the 1980s, computers increasingly made their appearance in offices and private homes. This was followed by the Internet in the 1990s. The digital world provided new possibilities for anonymity, but this was not without risk. The growing role of these technologies in our daily lives impacted our privacy.[8]

Liberals make an important distinction between the public space and the private sphere. The Greek philosopher Aristotle (348-322 B.C.) was the first to make an explicit distinction between the two. He outlined the dichotomy between the private sphere (*oikos*) – the domain of family life – and the public space (*polis*), the arena of public life in which politics are conducted. He believed that both spheres were of equal importance, because it was in the private sphere that the virtues subsequently employed in public life were cultivated.[9] As such, he argued the private sphere is the foundation of a virtuous public life.

---

6. This does not alter the fact that there are differences between countries in this area, even within the West. There are also differences within these countries between, for example, urban and rural areas.
7. D. Robinson, 'How East and West think in profoundly different ways', *BBC Future*, 19 January 2017, URL: https://www.bbc.com/future/article/20170118-how-east-and-west-think-in-profoundly-different-ways, accessed: 16 December 2021.
8. G. Ferenstein, 'The birth and death of privacy: 3,000 years of history told through 46 images', *Medium*, 25 November 2015, URL: https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e, accessed: 28 May 2021.
9. Aristoteles, *Politics* (English translation), vol. 1, 1999, pp. 3-22.

Liberals support this public-private distinction and also believe in the importance of privacy. For liberals, privacy is instrumental as a condition for the personal freedom and autonomy of the individual (see paragraph below). Furthermore, privacy is a condition for all sorts of other needs. It provides opportunities for contemplation and self-evaluation. Experiences can be processed and reflected upon in a private setting. Moments like this are particularly beneficial to self-awareness and the creative process. Privacy also allows us to occasionally step away from our everyday social roles (colleague, parent, etc.).[10]

Liberals also believe that privacy has its own intrinsic value for which people have a natural need. The liberal French-Swiss politician and writer Benjamin Constant (1767-1830) spoke of two different definitions of freedom. The 'Liberty of the Ancients', in which private life was limited and participation in political life was the priority. Here, freedom meant being able to participate in collective life and having a say in public affairs. Constant argued that this direct form of public participation might have been desirable in the small city republics of old, but that citizens approached life differently in the large modern nation state. The 'Freedom of Moderns' assumes an independent private sphere in which citizens can escape the collective.[11] According to Constant, the need for privacy is a distinguishing characteristic of modern versus ancient society. Be aware that his plea for an independent private sphere is not an argument for total seclusion. On the contrary, he believed that political indifference opens the door to violations of individual freedoms by the state.[12] Privacy is therefore considered a natural need that has formed over time and one to which individuals should always be entitled, providing it is not used to the detriment of others.[13, 14] In a nutshell, we can say that privacy is important to liberals in both an instrumental and an intrinsic sense.

---

10. Westin, *Privacy and Freedom*, p. 34-37.
11. P. de Hert, 'Benjamin Constant, surveillance en de strijd voor vrijheid en privacy', in: M. Colette, P. De Hert, A. Kinneging, *Benjamin Constant. Ontdekker van de moderne vrijheid*, Kalmthout, 2015, p. 163.
12. B.R. Ruiz, *Privacy in telecommunications: a European and American approach*, The Hague, 1997, p. 14.
13. R. Benedictus et al., *Gen-ethische grensverkenningen. Een liberale benadering van ethische kwesties in de medische biotechnologie*, book by Prof.mr. B.M. TeldersStichting, The Hague, 2010, p. 17.
14. For example, domestic violence, as previously mentioned.

2.3 Autonomy

There are various philosophical interpretations of the concept of autonomy. Autonomy is understood here to be the ability to make choices free from external influences. It is about the capacity for self-determination. External influence can occur both directly and indirectly. In matters of direct external influence, the person in question is aware of the influence. Punishing certain behaviours is a way in which individual autonomy can be threatened. Someone can still make a particular choice, but they know they will then be subjected to a punishment designed to act as a deterrent. This might be corporal punishment through physically violent means, or might be a social punishment like exclusion. This might also be the condemnation of a group member whose behaviour deviates from group standards. Liberals recognise that people are social beings with a tendency to conform, susceptible to peer pressure.

A second way of threatening individual autonomy is through indirect external influence. The person in question is then entirely unaware of this influence. They believe they are making an autonomous decision, when they are actually being manipulated by others. This might involve telling lies or deliberately withholding information. The intentions behind this are not always bad. For example, parents might tell a 'white lie' by saying to their children that watching too much television will give them square eyes. Nonetheless, this remains a form of paternalism detrimental to the autonomy of the person being manipulated. Moreover, manipulation often seeks to get people to make decisions that run counter to their interests. Later in this book, we will look at several examples of this in the digital world.

According to liberals, autonomy is essential to the self-actualisation of the individual. The English liberal philosopher John Stuart Mill (1806-1873) posited that human nature was like a tree 'which requires to grow and develop itself on all sides'.[15] This individual freedom is also in the collective interest, because the intellectual and moral development of gifted individuals is the engine of social progress.[16] Mill argued that citizens should not be morally accountable to society for individual choices that

15. F. de Beaufort, P. van Schie, *Het liberalen boek*, Zwolle, 2011, p. 48.
16. M.J. Trappenburg, 'John Stuart Mill (1806-1873)', in: P.B. Cliteur, A.A.M. Kinneging, G.A. van der List, *Filosofen van het klassieke liberalisme*, Kampen, 1993, p. 263.

do no harm to others. Individuality should be cultivated and celebrated instead of condemned or suppressed. Such moral autonomy is essential in preventing dogmatic ideas from taking hold and individuals from making choices out of fear of public condemnation.

Freedom from external influences also plays a major role in what liberals value as 'negative freedom'. The British liberal philosopher Isaiah Berlin (1909-1997) drew a distinction between negative freedom – the absence of external influence – and positive freedom – the individual's freedom to be their own master. While socialists tend to emphasise the importance of positive freedom, which uses external influence to increase the individual's ability to be their own master, liberals prefer negative freedom, where the individual is not compelled to make choices imposed upon them by external actors.[17] Liberals see the danger of excess positive freedom, because it allows external actors, like the state, to impose far-reaching ideas about what is in the interest of the individual.[18] The American libertarian philosopher Robert Nozick (1938-2002), who should be situated in the most radical corner of the liberal spectrum, has a similar stance. He argued that the justice of a choice is determined by the means and not the end. Choices need therefore to be voluntary and fair.[19] But individuals do not need to be protected from their own foolishness, as this would be paternalistic and detrimental to their autonomy.

Privacy can be seen as a condition for autonomy because it implies the absence of direct or indirect external influence. People should not be held accountable for the choices they make in a private setting, and others should not have the opportunity to manipulate, or influence in any other way, the information upon which these choices are made. Liberals believe in the importance of autonomy on the grounds that individuals have the right to determine what is in their best interests, providing they do not harm others in the process. This is the only means of achieving optimal individual self-actualisation.

---

17. M. Doorman, 'Twee opvattingen over vrijheid', *de Volkskrant*, 1 May 2010, URL: https://www.volkskrant.nl/cultuur-media/twee-opvattingen-over-vrijheid~bdcf1059/, accessed: 17 February 2021.
18. Nonetheless, there are also liberals on the left side of the spectrum who want the government to have a limited role in promoting the positive freedom of individuals (see section 2.5).
19. J. Oversloot, 'Robert Nozick', in: P.B. Cliteur, G.A. van der List, *Filosofen van het hedendaags liberalisme*, Kampen, 1990, p. 108.

2.4 Security

Just as in the case of privacy, the meaning of security has evolved over the years. Although there has been a reduction in war casualties since the Second World War, threats to security have become increasingly complex. Traditionally, security was primarily concerned with limiting physical violence, that mostly arose through war and crime. In recent times, security has come to be understood in much broader terms. Security policy has started to cover more than just threats of physical violence. The government of the Netherlands' *National Security Strategy* (2019) lists six national security interests: territorial security, physical security, economic security, ecological security, social and political stability and the international rule of law. It also states that digital security is closely intertwined with all these interests.[20]

Security is often seen as the second-most important liberal value after freedom.[21] It is simply not possible to construct and maintain a liberal society without adequate security. Liberals believe that providing security is the primary task of the government. This is what liberals call the 'social contract'. This concept is owed to the English philosopher Thomas Hobbes (1588-1679) and argues that individuals consent to surrender some of their freedoms to a central authority, who in return ensures peace and security through the enforcement of laws and regulations. According to Hobbes, this requires an absolute sovereign state with a monopoly on power, which he referred to as the 'Leviathan'.[22] Without this social contract, mankind would live in a violent state of nature as it did prior to the emergence of civilised society.[23] The English philosopher John Locke (1632-1704, often called the father of liberalism) also believed in the necessity for a social contract to be put in place

20. Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Nationale Veiligheid Strategie*, The Hague, 2019, p. 5.
21. Technically speaking, safety is more of a principle than a value, given that its importance is less subjective than that of other classical values. However, for the sake of readability, this concept will be included among the liberal values.
22. Hobbes wrote *Leviathan* in the context of the English Civil War (1642-1651). At the time, he was watching his homeland plunged into anarchy. As a result, he believed that order and stability were the highest good and that civil freedom was subordinate to this. Therefore, Hobbes is often viewed as an apologist for absolutism and not considered as a liberal *per se*, but rather as a pioneer for later liberal thinkers.
23. T. Hobbes, *Leviathan*, London, 1651, p. 78.

in which the government protects the security of its citizens, but he rejected Hobbes' claim that an absolutist regime was essential to this. He conceptualised a number of inalienable natural rights that apply not only to the citizens themselves, but also to the relationship between citizens and central government. Locke believed it was necessary to overthrow a monarch whose behaviour was tyrannical and did not respect fundamental human rights.

Liberals believe that security, freedom and prosperity are closely interlinked and that a good balance between the three is essential. As such, it may sometimes be necessary to impose stringent security measures at the expense of certain freedoms. The ideas of the English philosopher Jeremy Bentham (1748-1832) provide an interesting perspective on this. He came up with something he called the 'panopticon' which was a design for a dome-shaped prison building monitored from a central watch tower by a single prison guard, the inmates unaware as to whether they were being observed at any given time. Bentham believed that the continual possibility that they might be being watched would motivate prisoners to behave.[24] The French philosopher Michel Foucault (1926-1984, who incidentally was not a liberal) argued that this design was also applicable to other institutions, such as schools, hospitals and factories, where standards are enforced through supervision.[25] It could even be projected on to society as a whole. Digital society increases our visibility like never before, and this has a disciplinary effect on people. Asymmetrical surveillance – where the person conducting the surveillance can see the persons observed, but not the other way round – is used, for example, by investigation, inspection and security services. This provides the state with a powerful instrument for social control. Freedoms can be curtailed under the guise of security. Liberals are only too aware that this can lead to abuses of power.

Liberals need to acknowledge that it is unrealistic to live in a free society entirely without security risks. Were that the aim, the cure would be worse than the disease. This involves an ongoing balancing act for

24. A.M. Hol, 'Jeremy Bentham (1748-1832)', in: Cliteur, *Filosofen van het klassieke liberalisme*, p. 162.
25. M. Foucault, *Discipline and Punish: The Birth of the Prison*, New York, 1995, pp. 298-299.

liberals. A third component that plays an important role in this is our prosperity. Prosperity thrives when freedom and security are in balance. This allows freedoms to be enjoyed in a secure context, and sustainable economic investments to be made. A lack of either security or freedom cause our prosperity and wellbeing to suffer.[26]

This balance means that in a free society some risks to security are inescapable. Liberals find it unacceptable for a government to turn into an authoritarian regime under the guise of increased security, not least because a government can become a security problem for its citizens, as is apparent in unfree countries across the world. Furthermore, dictatorial regimes often use violence to oppress their citizens and given the lack of democratic means, conflicts can only be settled with violence.[27] As such, freedom is a means of safeguarding security by preventing governments from becoming too powerful, and thus becoming a threat to their citizens.

2.5 Equal treatment

Every citizen deserves to be treated equally by the government. Governments must not judge the value of individuals. For liberals, equal treatment is not about the relationship between citizens, but about the relationship between citizens and the government. This means governments should not discriminate on the grounds of skin colour, age, gender or sexual orientation. Society should be organised to give everyone the opportunity to reach their full potential. However, please note that equality of opportunity does not mean equality of outcome. Everyone is unique. It is up to the individual to take responsibility for developing their own talents and qualities and to reap the rewards for their efforts.

German-British liberal thinker Ralf Dahrendorf (1929-2009) believed that equality was essential to ensuring freedom. In particular, he emphasised the importance of civil rights, such as the right to equality before the

26. P. Ducheine, 'Veiligheid en cyberspace. Veiligheid tegen (w)elke prijs', *Blind*, 2018, no. 49, p. 2.
27. W.J. Derksen, 'Veiligheid en vrijheid', in: *Koester de vrijheid*, ledenblad van de VVD, The Hague, 2020, p. 15.

law, universal suffrage and freedom of expression.[28] He argued that the pursuit of equality for its own sake (equality of outcome), leads to undesirable restrictions on freedom.[29] An example of this is the far-reaching economic redistribution policy of Soviet Union, where private property was collectivised.

An interesting addition to this is the 'veil of ignorance' concept, coined by American philosopher John Rawls (1921-2002). He argued that we should strive to create the society we would choose to live in if we did not know in what circumstances or with what abilities we would be born.[30] In relation to this, he discussed two different principles of justice. Firstly, each person should have an equal right to the most extensive basic liberty compatible with a similar liberty for others. Secondly, he claimed that social and economic inequalities were justifiable as long as everyone had equal opportunities and that inequality also benefitted the least advantaged.[31] Rawls did not rule out welfare redistribution policies.[32] He emphasised that the order of his two principles was deliberate on the grounds that the material prosperity motive of the second principle should never come at the expense of the fundamental right to freedom of the first principle.[33]

We can draw a parallel here with the distinction between classic and social fundamental rights found in the constitution of many countries. On the one hand, classic fundamental rights provide citizens with protection from the government. These include the right to privacy and freedom of religion. They impose limits on the government. On the other hand, fundamental social rights give the government the means to safeguard resources for society. They include things like the right to housing or work (although not all countries have fundamental social rights and instead regulate these types of provisions outside the constitution).

---

28. C.J. Loonstra, 'Ralf Dahrendorf', in: Cliteur, *Filosofen van het hedendaags liberalisme*, p. 128.
29. F. de Beaufort, 'Ralf Dahrendorf', *TeldersStichting*, URL: https://www.teldersstichting.nl/liberalen/ralf-dahrendorf, accessed: 18 February 2021.
30. M.J. Trappenburg, 'John Rawls', in: Cliteur, *Filosofen van het hedendaags liberalisme*, p. 92.
31. L. Wenar, 'John Rawls', *Standford Encyclopedia of Philosophy*, 12 April 2021, URL: https://plato.stanford.edu/entries/rawls/#TwoPriJusFai, accessed: 20 April 2021.
32. J. Rawls, *A Theory of Justice*, Cambridge, 1971, pp. 246-247.
33. M.J. Trappenburg, 'John Rawls', in: Cliteur, *Filosofen van het hedendaags liberalisme*, p. 94.

All liberals agree on the importance of the first principle. The second principle is somewhat more controversial, and opinions within liberalism differ towards it. Those who side with Rawls tend to be on the left-side of the liberal spectrum. These liberals envision a more active government role in promoting opportunities for individual self-actualisation. The liberals on the right-side of the spectrum consider even this limited form of government intervention too great a threat to individual freedom. They prefer to limit rights to classic fundamental rights and pay little to no importance to fundamental social rights.

In matters of equality, liberals across the spectrum agree that in the relationship between the government and its citizens, the government must be accessible to everyone. The government must take into account particular groups that are struggling. The value liberals place on active citizenship and self-reliance means that they find it unacceptable for any citizens who wish to participate in society to have difficulty in so doing, whatever the reason. This could be people who are partially sighted but also, for example, anyone who struggles with digitalisation. Liberals think that the government should facilitate equal access to its services at all times. What is more, citizens must also be able to hold the government to account if they believe that their right to equal treatment has been compromised.

2.6 Democracy

Although democracy has not traditionally been seen as a core value, it remains a key part of liberal thinking. It is with good reason that it is often called 'liberal democracy'. Democracy aligns with the liberal desire to put the individual front and centre, and to place power in the hands of the citizens, instead of a sovereign state. Liberals contend that democracy allows individuals to exercise maximum and equal influence and have a say in making collective decisions. Democracy, in this instance, does not just refer to the process of holding democratic elections. In a liberal democracy, citizens not only have a say in public affairs, but they also have certain fundamental rights. According to liberals, democracy must be embedded in the rule of law, allowing citizens to defend these fundamental rights. This protects citizens first and foremost from

government overreach.[34] Other aspects of this countervailing power within democracy that are of importance to liberals include the *separation of powers*, the freedom of the press and the creation of a vibrant civil society.[35]

Another essential part of liberal democracy is public debate. The liberal Austrian-British philosopher Karl Popper (1902-1994) took a stand for what he called an 'open society'. He argued that social progress should be the result of '*trial and error*' and that reform should occur in small steps, by measuring and assessing the results, and making adjustments when necessary.[36] Democracy is the most suitable framework for this system because it allows citizens to employ the critical exchange of ideas to amend policy. This critical-rational discussion also contributes to the population's acquisition of knowledge and promotes democracy's problem-solving capacity.[37] Popper also highlighted the 'paradox of tolerance'. Unchecked tolerance leaves space for the intolerant to undermine tolerance. This allows the system to undermine itself. Therefore, to create a tolerant society, it is necessary to impose limits on tolerance.[38] For example, freedom of expression should not be used to silence others. In an open society people must be able to tolerate each other at all times. This means that even when you strongly disagree with someone, you still have to tolerate them, however unpleasant it may be.

As previously stated, liberals see democracy as more than 'whoever gets the most votes'. It is essential to prevent the 'tyranny of the majority' as outlined by the French liberal Alexis de Tocqueville (1805-1859). Dissenters should not be oppressed by the popular will of the majority. This means that there are several classic fundamental rights that liberals consider so essential to democracy as to be inviolable. These fundamental rights should never be denied. Within their broad understanding of

34. This book uses 'democracy' in a wider sense than simply 'constitutional democracy'.
35. F. de Beaufort, 'Democratie', *Liberaal Journaal*, publication by Prof.mr. B.M. TeldersStichting, The Hague, 2020, p. 1.
36. G.A. van der List, 'Karl Popper', in: Cliteur, *Filosofen van het hedendaags liberalisme*, p. 66.
37. Ibidem, p. 65.
38. F. Bosch, 'Moeten we tolerant zijn tegenover intoleranten?', *Het Parool*, 31 October 2018, URL: https://www.parool.nl/nieuws/moeten-we-tolerant-zijn-tegenover-intoleranten~bc68ff72/?referrer=https%3A%2F%2Fwww.google.com%2F, accessed: 19 February 2021.

democracy, liberals want to prevent a democratic decision to abolish democracy itself.

The liberal Spanish philosopher José Ortega y Gasset (1883-1955) also feared a sort of tyranny of the majority.[39] He warned against what he called the 'mass man'. Ortega y Gasset believed that modern prosperity had created people who were self-righteous and passive; people reluctant to hear other people's opinions or think critically for themselves.[40] The mass man always believes he is right and only cares about himself and like-minded people. Therefore, the mass man oppresses anyone who is different. Political debate in modern 'hyper-democracy' suffers intellectually because increasingly few people are prepared to engage in genuine rational-critical argument.[41] French sociologist and psychologist Gustave Le Bon (1841-1931) supports this stance. He described how the individual can lose their ability to think critically in the crowd. Crowds render the behaviour of individuals anonymous, and emotionally and intellectually weak. He believed that not even the most highly developed individuals are immune to group dynamics of this sort.[42]

The digital world similarly swallows individuals into the crowd with negative societal consequences. Just think about the emergence of 'information tunnels' on social media, where users only see their own opinions confirmed by algorithms. This translates into a flattening of political debate and growing polarisation in society. In recent times some of these digital platforms have been approached and asked for information shared on their online stage. As a result, several of these companies now actively moderate content and no longer offer space to certain views. Liberals believe that space should be allowed for open debate in which all opinions can be expressed (providing that these do not incite harm to others, such as physical violence). Democracy can only safeguard a dynamic and pluralistic society through rational-critical argument. This requires continuous efforts with no room for intolerance or censorship. In a nutshell, liberals believe that democracy needs to be resilient.

---

39. W.J. Derksen, 'José Ortega y Gasset', *TeldersStichting*, URL, https://www.teldersstichting.nl/liberalen/jose-ortega-y-gasset, accessed: 19 February 2021.
40. P. Scotton, 'Intellectuals, public opinion and democracy. On Ortega y Gasset's social education', *Social and Education History*, 2019, no. 3, p. 290.
41. J. Ortega y Gasset, *The Revolt of the Masses*, New York, 1994 [1930], p. 8.
42. G. Le Bon, *The Crowd: A Study of the Popular Mind*, New York, 2002, [1895] pp. 2-9.

2.7 Safeguarding freedom by setting boundaries in the digital world

The following chapters explore how these five liberal values can guide certain developments in digital society. The ideas about these values expressed historically by liberal thinkers have been expressed in different technological contexts, but remain relevant in modern times. Liberals typically have a strong belief in the principle of non-intervention. This means that the government should limit itself to its core tasks and not meddle in society and citizens' lives. But when liberal values are at stake, there is a real need for the government to intervene.

But the advent of certain developments in digital society means that the principle of non-intervention needs to be abandoned, because we have reached a point where making no choice has actually become a choice. As this book makes clear, a *laissez-faire* approach has already enabled certain developments in the digital world that have created unacceptable risks in our society. A passive attitude to these developments is a real threat to liberal values. Society needs a more proactive attitude in order to take greater control in the digitalisation arena through awareness, legislation and establishing a broader strategy. This shift in mindset is needed first and foremost from the government, but also in civil society and among individual citizens. There is a need to set clear boundaries and liberal values are a good starting point for this. As stated earlier, these core values are the condition for a free society. We need to safeguard freedom by setting boundaries.

3. Digitalisation & the Free Market

3.1 The data-driven economy

The economy is changing at a fast pace as a result of digitalisation. The estimated economic value placed on new digital technologies, and the application thereof, often tends to be through the roof. For example, in the late 1990s, the dotcom bubble drove unrealistically high valuations and stock market predictions for internet-based businesses.[1] More recently, there have been similar astronomical rises in Bitcoin valuations.[2] Tech *start-ups* are sprouting up everywhere at a rapid pace, and anyone who wants to remain competitive in the current market is forced to stay on top of digital developments. In 2021, European online retail had a turnover of 718 billion euros. An increase of 13 percent compared to the year before.[3, 4] We also saw the rise of the 'platform economy', where supply and demand are connected on digital platforms in new and innovative ways[5] and often at the expense of traditional market players. The digital and real economies are increasingly intertwined as a result. This is creating shifts in the free market that liberals value so highly, that affect not only market players, but also the market itself.

Data has a major role to play in this new digital economy. Digitalisation has created enormous new data flows which businesses can

1. Corporate Finance Institute, 'What is the Dotcom Bubble', URL: https://corporatefinanceinstitute.com/resources/knowledge/trading-investing/dotcom-bubble/, accessed: 29 April 2021.
2. 'Cryptovaluta: goudmijn of bubbel?', *BNR*, 14 June 2017, URL: https://www.bnr.nl/nieuws/beurs/10324692/cryptovaluta-goudmijn-of-bubbel, accessed: 29 April 2021.
3. Amsterdam University of Applied Sciences and Ecommerce Europe, *European E-Commerce Report 2022*, 2022, p. 2.
4. In which the Covid-19 pandemic undoubtedly had a role to play.
5. Sociaal-Economische Raad, *Hoe werkt de platformeconomie?,* The Hague, 2020, p. 22.

draw upon. Data-driven working means that data is collected, stored, organised and analysed by businesses in order to subsequently make better-informed market choices. AI has a major role to play in this. This can be used to automate business processes by way of algorithms, so businesses can personalise the services they provide to consumers, for example. These algorithms use *machine learning* to continue to improve as they are fed more data.[6] Data and algorithms thereby determine the market mechanism. This means that data now has a strong economic value, as a result. Nowadays, data is sometimes qualified as the fourth factor of production, alongside nature, labour and capital.[7] Also noteworthy are the huge economies of scale that can be achieved with data. The more data, the better the algorithms and the better the product. And the better the product, the more users and therefore the more data generated by the users.[8] Data creates a positive feedback loop. Furthermore, network effects create similar feedback effects in the platform economy, thus contributing strongly to the profitability of certain digital products and services.

Such is the potential for growth that innovative companies can grow at unprecedented speed, so the emergence of several very large and powerful tech companies should come as no surprise. Tech titans like Google[9], Facebook[10], Apple, Amazon and Microsoft, as well as Asian giants like Alibaba and Tencent dominate the global market, most of which have only emerged relatively recently. They operate in a new and dynamic market which is currently relatively unregulated. For a long time, this has allowed these companies to often act in their own interest. Market parties of other types are also thinking about how datafication can add value to their business operations. For example, healthcare insurers are

6. United Nations, 'Data Economy: Radical transformation or dystopia', *Frontier Technology Quarterly*, 2019, no. 1, pp. 1-2.
7. 'Capgemini: Big Data als productiefactor voor bedrijven', *Consultancy.nl*, 2 July 2012, URL: https://www.consultancy.nl/nieuws/4300/capgemini-big-data-wordt-vierde-productiefactor-van-bedrijven, accessed: 6 April.
8. B. Baarsma et al., *De datagedreven toekomst.nl. Hoe we vormgeven aan onze toekomst in de datagedreven wereld*, rapport van DenkWerk, 2021, p. 14.
9. Since 2015, Google LLC has been a subsidiary of the parent holding company Alphabet Inc. As the former is probably more familiar to the reader, it will be referred to in this book the name of 'Google'.
10. In 2021, Facebook Inc. changed its name to Meta. This text also simply refers to the company name 'Facebook', given the greater familiarity of this name among readers.

currently looking into how they can promote healthy lifestyles by using client-data to offer discounts on supplementary insurance policies, thus reducing healthcare costs.[11]

Liberalism advocates a free market in which the market is left predominantly to its own devices, so that it can be shaped from the bottom up by individual choices, creating a spontaneous order, naturally regulated by supply and demand.[12] This creates prices which reflect the economic value of products and services. The government only acts as a market regulator enforcing rules to ensure a level playing field for all. Throughout history, free markets have created prosperity and proved complementary to guaranteeing free societies revolving around the freedom of the individual. The TeldersStichting recently published *A Free Market for All* (2022), which explores this in depth.[13]

Yet this book also acknowledges that at the current time, the free market is encountering a range of issues that require new solutions. When it comes to the data-driven economy, there are particular concerns around how businesses collect and use data. This market in which the individual is the product, is fundamentally different to anything we have previously known. Economic gain seems to come at the expense of liberal values like privacy and autonomy. Moreover, market competition appears to have been distorted and we see multiple examples of tech companies abusing their power. This chapter examines how we can protect liberal values and maintain a level playing field in the free market without hindering competition and innovation.

3.2 Data Revenue-Models

It's clear we are through times in which the rush for data in the market is huge. Data is often referred to as the 'new oil'. The impact fossil fuels had on society in the industrial age, now appears to apply to data in the

11. 'Gezond gedrag belonen met korting of wearable?', *ICT&health*, 6 January 2020, URL: https://www.icthealth.nl/nieuws/gezond-gedrag-belonen-met-korting-of-wearable/, accessed: 7 April 2021.
12. F. de Beaufort, P. van Schie, *Het liberalen boek*, Zwolle, 2011, p. 57.
13. M. Schulz et al., *A Free Market for All*, book by Prof.mr. B.M. TeldersStichting, Antwerp, 2022.

information age.[14] Data is of huge value to market players. Frequent use is made of *'big data'*: i.e. the collection of enormous data sets. Large data sets are linked and analysed with the aim of discovering connections, with the help of AI. In this process 'raw data' (unprocessed data) is processed into 'information' (interpretation), 'knowledge' (conclusion) and ultimately 'wisdom' (application).[15]

Personal data can also be found among all the data collected and analysed. 'Metadata' can also contain personal data. Metadata is data that describes the other data (basically, data about data).[16] This might be the date on which and the language in which an email was sent. The *General Data Protection Regulation* (GDPR) defines personal data as (meta) data that can be directly or indirectly traced back to a specific person. Therefore, it is data that contains information about individual identity.[17] Examples of directly identifiable personal data include social security and bank account numbers. Indirectly identifiable personal data includes, for example, dates of birth and post codes. In isolation, this data cannot be traced back to a particular person, but in combination with other data it may be. The GDPR also refers to 'special category data'. This is personal data that can be classified as sensitive because it contains information about a person's religion, health status or political preferences.[18] This might be biometric data or membership of a political party or union. The requirements for the processing special category data are especially strict. It is in principle prohibited, unless there are legal grounds to do so. An important caveat is that in practice it is difficult to draw a line between what is and what is not personal data, because personal data is often not obtained directly, but derived from other types of data. (See below for more information).

---

14. J. van Haaster, *On Cyber: the Utility of Military Cyber Operations during Armed Conflict*, University of Amsterdam thesis, Amsterdam, 2019, p. 78.
15. J. Rowley, 'The wisdom hierarchy: representations of the DIKW hierarchy', *Journal of Information Science*, 2007, no. 3, p. 164.
16. J. Hare, 'What is metadata and why is it as important as the data itself', *OpenDataSoft*, 25 August 2016, URL: https://www.opendatasoft.com/blog/2016/08/25/what-is-metadata-and-why-is-it-important-data, accessed: 31 May 2021.
17. European Parliament and Council, *Regulation (EU) 2016/679 (General Data Protection Regulation)*, Article 4.1, Brussels, 2016.
18. Ibidem, Article 9.1.

A lot of personal data is created in the digital domain. Data is generated that can be traced back to users of digital products and services. For example, on the internet users often have to agree to the use of '*cookies*', which enables webmasters to identify visitors. This data may have something to say about the identity, preferences and user behaviour.[19] GPS functionality can also be enabled on mobile phones when using apps. While this information may be necessary to the service that the app provides, it also allows the app supplier to collect user location data.

There are several reasons why gathering all this personal data is interesting to companies. Service provision can be optimised by offering functionalities based on the data collected (for example, navigation apps detect road closures on this basis). Generally speaking, there is something in this for both the consumer (better user experience) and the company (better judgement). For example, Google's privacy policy states that user data is collected to provide certain features, detect issues and malfunctions, and to develop new services.[20]

Another way in which collecting user data adds value is by making personalisation possible. When companies receive data about users' identity, preferences and behaviour, they can use it to build personal profiles. For example, Facebook uses personalisation to deliver unique content to individual users. Facebook's algorithms select specific content to show them based on previously collected user data. Personalisation is also interesting for marketing purposes by enabling targeted advertising. Whereas in the past, advertisers could only target groups, for example, by advertising a sports brand during football matches, it is now possible to approach individuals individually.

A third reason why personal data is of economic value for companies is that it can be sold on. The sociologist Amitai Etzioni has called these market players who sell data of this sort to the highest bidder '*privacy merchants*.[21] There are even companies that trade exclusively in data of this type. These data merchants collect and merge data, before

19. Kaspersky, 'What are cookies?', URL: https://www.kaspersky.com/resource-center/definitions/cookies, accessed: 21 April 2021.
20. Google, 'Privacybeleid van Google', URL: https://policies.google.com/privacy?hl=nl, accessed: 23 April 2021.
21. A. Etzioni, 'The privacy merchants: what is to be done?', *University of Pennsylvania Journal of Constitutional Law*, 2012, no. 4, p. 930.

selling it on to third parties.[22] The GDPR restricts the resale of personal data and has strict requirements with regard to lawfulness, fairness and transparency.[23] A caveat here is that in many cases enforcement is complicated, due to the fact that many market players are located outside the EU.

The monetary value of this personal data is clear from the revenue models of many tech companies. The services provided to users are often 'free', while at the same time, these tech companies offer services to business customers who want to advertise specifically through their platform. By offering their services to users free of charge, these tech companies are able to collect more data. They then use this user data for their advertising services to business customers.

Google's revenue model

The internet search engine Google Search (www.google.com) is currently the world's most visited website with some 3.5 billion search requests a day. Google also provides other digital services such as Gmail (email), YouTube (videos), Google Maps (navigation and maps) and Google Drive (file storage). All of these services can be used free of charge (although some have paid *premium features*). Anyone who wants to use these services needs to agree to the terms and conditions. Google generates its income by using their data. The other side of Google's business operations is its advertising services. On Google Ads, business customers bid against each other to show adds to specific users. The advertisers relevant to specific users are identified on the basis of data collected by Google. A combination of this quality rating and the bid price determines which businesses get to advertise. The advertiser then has to pay Google for every click on an ad (*pay-per-click*). In 2020, Google's turnover for advertising services was approximately 146 billion dollars. That accounts for the lion's share of the company's total turnover. Google's revenue model demonstrates that its real clients are its advertisers and not the users of its services.

22. C. Burdova, 'Data brokers: who they are and how they work', *AVG*, 26 August 2020, URL: https://www.avg.com/en/signal/data-brokers, accessed: 23 April 2021.
23. European Parliament and Council, *Regulation (EU) 2016/*679, Article 5.1.

The example above is just one of many similar data-driven revenue models that exist today. For example, social media businesses like Facebook and Twitter have their own variations, as do mediation platforms like Booking, Airbnb and Uber, and transaction processing businesses like PayPal and VISA, etc. Earning money through processing personal data is in no way prohibited and, as we saw above, users also have an interest in sharing it to ensure well-functioning digital services.

Yet we need to recognise that this is a market of a fundamentally different kind to anything we have ever seen before. Traditionally, individuals are consumers in the marketplace. On the supply side there are market parties which offer products and services for a fee to the individuals (consumers) on the demand side. By way of illustration, for a traditional market party like a shoe manufacturer, individuals are potential customers to whom to sell shoes. However, individuals have an entirely different role within data-revenue models. There, individuals are not consumers but products. Tech companies sell the attention of the individuals on their platforms to advertisers, like a product. Based on their data, individuals are selected in advance as being of potential interest to these advertisers. By way of illustration, Google determines how interesting a particular brand of shoes will be to someone, on the basis of their personal data. Then, for a fee, this shoe brand can place a Google ad specifically for this person. The platform is free for users, encouraging more individuals to engage and thus allowing more personal data to be collected for advertising purposes.[24] What this means for individuals is: 'if you're not paying for the product, you are the product'.

3.3 A liberal perspective on GDPR

As companies make money from processing users' personal data, it is easy to see that this is an economic transaction. Users 'pay' to use digital services with their personal data. However, to simply categorise this as

24. As previously stated, this market has similarities with the traditional advertising market, in which newspapers, for example, receive advertising revenue by offering advertisers space in which to target their readership. The critical difference is that in this market, advertisements are tailored at an individual level according to a person's personal data, with major consequences for that person's privacy and autonomy.

an economic transaction is incorrect, because it would also imply ownership of personal data. Ownership of personal data is a legally tricky matter. According to the law, ownership is about the control of material things.[25] Intellectual property is an exception to this, but this should not in principle be the case for personal data, because works must be of original character, the result of creative choices and bear the personal stamp of the creator. This does not include primary data amounting to simple facts, which is usually the case with personal data.

Although it is understandable that you might intuitively see the data about yourself as something you own, such ownership would also imply unlimited control. That is problematic because there is also a general need for freely available, accurate information. For example, you cannot simply transfer your surname to someone as property and thus give up control of it. The most important argument against the ownership of personal data is that it would actually weaken the position of individuals. Market parties would then be able to take full control of someone's personal data, were they to relinquish it as property through an economic transaction.[26] After which the individual would no longer have any say over their personal data. Therefore, we do not talk of ownership, but of 'control' over personal data, which is something individuals always retain. GDPR was drawn up with this vision of personal data, and it establishes the rights of the persons to whom the data relates (data subjects) and the obligations of the data controllers (processors).

This section will examine the individual's rights established by the GDPR from a liberal perspective. According to the GDPR, data subjects have the right to access, the right to erasure, the right to rectification and supplementation, the right to data portability, the right to limit processing, the right to object, the right not to be subject to a decision based solely on automated decision-making, and the right to clear information about what data is processed and why and with whom it is shared.[27] Under the GDPR, data processors have an 'accountability

25. Netwerk Auteursrechten Informatiepunten, 'Data protection', 2019, p. 1.
26. In addition, the economic value of data at the individual level is limited. It only becomes relevant after this data has been collected and combined in large quantities. The individual would not gain much from an economic transaction.
27. Autoriteit Persoonsgegevens, 'Rechten van betrokkenen', URL: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen, accessed: 10 May 2021.

obligation' with regard to these rights, giving rise to several compulsory measures. For example, data processors have to maintain processing registers, identify privacy risks in high-risk data processing, keep track of data breaches, be able to demonstrate that data subjects have given consent for data processing and appoint a data protection officer (DPO), or be able to substantiate why they have chosen not to do so.[28]

Somewhat remarkably, there is not a single instance of the word privacy in the GDPR text, although the rights and obligations it lays down are clearly aimed at protecting the privacy of citizens. Liberals consider privacy an inalienable natural right. As mentioned earlier, the English philosopher John Locke (1632-1704) claimed that the protection of these inalienable natural rights served not only to guarantee safety, but was also the reason why citizens entered into a social contract with one another.[29] The right to privacy is therefore rooted within the legal systems of many countries. Deeming privacy a fundamental right, that individuals must always retain, is a reflection of liberal thinking when it comes to the importance of privacy. As previously stated, our understanding of privacy is strongly related to technological developments. From a liberal perspective, the GDPR is justifiable on the grounds that it offers individuals more legal tools, in order to continue to exercise this fundamental right in a digital society. The rights under the GDPR imply an inalienable control over personal data, which individuals can never lose.

Liberals argue that it is undesirable to have an unregulated situation in which individuals (can) relinquish their fundamental rights. After all, privacy also has an intrinsic – independent and not just instrumental – value for liberals. Furthermore, individuals often don't have sufficient insight into the situation to enable them to make responsible choices. For a long time there was a complete lack of transparency around the processing of personal data, with data subjects left in the dark as to what data was being processed, for what purpose, and with whom it was

28. Autoriteit Persoonsgegevens, 'Verantwoordingsplicht', URL: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht#hoe-voldoe-ik-aan-de-verantwoordingsplicht-6099, accessed: 10 May 2021.
29. P.C. Westerman, 'John Locke (1632-1704)', in: P.B. Cliteur, A.A.M. Kinneging, G.A. van der List, *Filosofen van het klassieke liberalisme*, Kampen, 1993, pp. 62-63.

being shared.[30] Even when viewed from the non-interventionist perspective of American libertarian Robert Nozick, improving transparency is necessary to ensure that individuals are able to make fair choices (see section 2.3). The GDPR helps fix this information asymmetry, for example, through the right of access for data subjects and the duty of care required of processors. In this sense, the GDPR scarcely restricts the freedom of data subjects as they are neither obliged to make particular choices, nor are they obliged to make active use of their rights.

Some people consider this to be possibly the greatest weakness of the current legislation. In theory, the GDPR allows individuals (data subjects) to exercise greater control over their personal data, but this does not necessarily happen in practice. After all, people often claim to find privacy important, but then fail to act accordingly. This is partly due to the fact that any negative effects are often only visible over the longer term and occur at a societal rather than an individual level. Consider, for example, the emergence of a surveillance economy and unwanted political influence (more about this in the sections below).

Nonetheless liberals remain wary of additional legislation restricting the individual's freedom of action with regard to their personal data. The English liberal John Stuart Mill articulated the 'harm principle', in which he proposed that individuals should be completely free to act as they wish, providing it causes no harm to others.[31] For liberals, the harm principle serves as a means to determine the extent to which restrictions on freedom through government intervention are justified. The concept of harm can be interpreted in multiple ways and needs clarification before it can be used to formulate concrete policy. This can be difficult at an individual level, when it comes to abstract concepts like privacy and autonomy. Furthermore, the harm doesn't occur as a direct result of individuals sharing personal data, it's what data processors subsequently do with this personal data. Added to which, a lot of data is not acquired directly from individuals but is derived indirectly from other data. This is why the processors, rather than the individuals, should bear full responsibility for any harm caused. Therefore, liberals

30. General Terms and Conditions are often a form of false transparency. It is unrealistic to expect users to go through such long, complicated legal texts time and again.
31. J.S. Mill, *On Liberty*, Kitchener, 2001 [1859], p. 13.

consider it undesirable to use legislation to restrict individual freedom of action.[32]

The GDPR's lack of constraints on individuals aligns nicely with liberal values. However, there are some major practical objections. Currently the tools are not in place for individuals to make active and effective use of their rights under the GDPR. Thought must be given to how to create an infrastructure within the digital domain that would allow individuals to exercise control over their data in a convenient, accessible and standardised way. Inspiration for this may be drawn from a money transfer system like the upcoming European Payments Initiative, to which all major European banks will be connected and which will enable money to be transferred between parties with ease. An equivalent standardised system could potentially be set up to allow individuals to easily manage their data. However, if that were the case there would be no financial incentive for market parties to set up such a system. For this data infrastructure to be implemented, it probably needs to be enforced through legislation.

Another complaint about the GDPR is the heavy administrative burden it places on smaller processors who have to comply with accountability obligations. For example, the owner of several cheese shops claimed to have spent 80 hours making her company GDPR-proof.[33] Partly, because the GDPR still leaves a lot of room for interpretation. On the one hand, there is a need for open standards to ensure legal flexibility and to prevent new technological developments from rendering the GDPR immediately obsolete. However, on the other hand many data processors struggle to interpret these hazy concepts and translate them into concrete measures.[34] Large corporations with extensive *compliance*

32. Individuals qualified as legally incompetent, such as minors, are an exception to this. The GDPR, classifies them under the category 'vulnerable natural persons'. When sharing personal data, children under the age of 16 must obtain permission from whoever has parental responsibility over them (see Article 8 of the GDPR).

33. S. Yoo, '1 jaar later: waarom de AVG ondernemers tot wanhoop drijft', *MKB-Nederland*, 24 May 2019, URL: https://www.mkb.nl/forum/1-jaar-later-waarom-de-avg-ondernemers-tot-wanhoop-drijft, accessed: 10 May 2021.

34. C. Hendriks, 'Hoogleraar Gerrit-Jan Zwenne: 'Veel onduidelijk over de AVG'', *University of Leiden*, 10 May 2021, URL: https://www.medewerkers.universiteitleiden.nl/nieuws/2018/06/nog-veel-onduidelijk-in-de-avg, accessed: 10 May 2021.

departments have the capacity to research the topic in depth, but it presents a huge problem to the owners of SMEs.[35] According to liberals, free markets should be regulated using the minimum amount of rules, with maximum effectiveness. Clarity when it comes to regulations is therefore absolutely essential. A lot of progress is therefore yet to be made in terms of 'explainability', by formulating more explicit guidelines.

Furthermore, the biggest problem with GDPR to date is that it appears to be making less of an impact than had been hoped, because many large tech firms still fall short when it comes to compliance.[36] Despite the fact that this is exactly where the greatest threat to the privacy and autonomy of citizens lies. This is because these regulations clash directly with the data revenue model of these tech companies. Legislation needs to afford more rights to the individual to increase their scope for action. However, the unique characteristics of this market require that the freedom of action among market parties be limited in some areas. This will become more apparent in the text below.

3.4 The surveillance economy

As previously mentioned, data has economic value in this chapter, in part because it tells us about individual behaviour to which market parties can then respond. The possibilities for mapping individual behaviour are growing, as the trend towards datafication expands and increasing numbers of objects are connected to the digital world. Smart thermostats know how many hours we spend at home each day, supermarket discount cards know which products we like to buy, *fitnesstrackers* know how much we exercise. The more this data is collected, the better our

35. Although it is only the market that is under discussion here, this criticism also applies to other actors in society. These include, for example, schools and sports associations whose administrative burdens are heavy as a result of the GDPR, while these are often not the sources of the problem that the GDPR is aiming to address. There is a need here for more concrete guidelines to adhere to.

36. N. Vinocur, ''We have a huge problem': European tech regulator despairs over lack of enforcement', *Politico*, 27 December 2019, URL: https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605, accessed: 2 May 2022; Kavya, 'Big Tech vs GDPR', *Cookie Law Info*, 30 September 2021, URL: https://www.cookielawinfo.com/big-tech-vs-gdpr/, accessed: 2 May 2022.

behaviour can be analysed. This makes it possible to profile individuals. Algorithms find patterns in our past behaviour.[37] Individuals are then labelled and subdivided into different groups. These groups are based on categories of interest for market parties. This allows certain characteristics to be attributed to individuals and market parties try to make predictions based on this.

The writer Shoshana Zuboff explores this in his book *The Age of Surveillance Capitalism* (2019). She argues that in the early days of the internet, businesses collected data with the sole aim of delivering products and services and improving them in the future. This data, which is created when individuals use digital services and products, also produces a by-product in the form of data about human behaviour. Zuboff calls this a 'behavioural surplus'.[38] These companies soon realised that this surplus of behavioural data could provide lucrative revenue models, as explained earlier in this chapter. Thus individual behaviour became commodified and human experience became the raw material for products using behavioural prediction techniques, Zuboff argues.

It is a widely used technique in the marketing world, with the aim of predicting consumer needs and then responding to those needs. Aside from demographic characteristics (age, gender, etc.), this also includes psychographic factors. Psychographics revolves around determining individuals' personalities, interests, opinions and others psychological criteria.[39] Algorithms then draw on this data to determine people's needs, what products are therefore worth advertising to them, and when this is most effective.

The extent to which companies have this predictive ability has already been demonstrated in various ways. One example (from years ago now) involves an American supermarket chain that was able to establish that a teenage girl who shopped there was pregnant. When she started receiving coupons for baby products, her angry father demanded to talk to the store manager. The girl subsequently turned out to be pregnant. The

37. K. Gabriels, *Onlife. Hoe de digitale wereld je leven bepaalt,* Tielt, 2016, p. 19.
38. S. Zuboff, *The Age of Surveillance Capitalism: the Fight for a Human Future at the New Frontier of* Power, London, 2019, p. 75.
39. A. Nix, 'Cambridge Analytica – The power of big data and psychographics', presentatie tijdens het Concordia Annual Summit, *YouTube*, 27 September 2016, URL: https://www.youtube.com/watch?v=n8Dd5aVXLCc&t=594s, accessed: 17 July 2021.

supermarket's algorithm had worked out that there was a strong chance this girl was pregnant because, among other things, she suddenly started buying unscented soap, which is indicative of the changes in smell perception that often occur in pregnant women.[40]

The issue here is that privacy-sensitive information is often derived from data that in itself does not appear to be particularly revealing. But, as the example above shows, seemingly innocent data about a change in soap preferences suddenly revealed highly confidential information. Likewise, preferences for particular music or films on streaming services indicates the statistical probability of a given sexual orientation.[41] The more data points that can be connected, the more information that can be extrapolated from them. As previously stated, special personal data such as sexual orientation, religion and medical data is subject to extra protection under the GDPR. But this becomes more difficult to enforce when it can be established indirectly through other 'innocent' data. This means that the privacy of citizens can be negatively affected by the behavioural prediction techniques used by market parties.

The rush for data that we see emerging in the surveillance economy is proof of the enormous confidence that is placed on this data. Yet it is important to take a nuanced approach to *big data*. Professor Mireille Hillebrandt argues that among all the mountains of data there is a lot that is incorrect or irrelevant.[42] Data analysis can also show correlations, without there being a causal relationship. The Rathenau Institute likes to highlight the work of statistician Tyler Vigen, who graphed what looks like a connection between the amount of cheese someone eats and how many people die from getting tangled up in the duvets.[43] The predictive power of algorithms is sometimes overestimated, because data and data analyses are found to be lacking. Nonetheless, the overvaluation of some

40. K. Hill, 'How Target figured out a teen girl was pregnant before her father did', *Forbes*, 16 February 2012, URL: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=702e69766686, accessed: 3 June 2021.
41. M., Kosinski, D. Stillwell, T. Graepel, 'Private traits and attributes are predictable from digital records of human behavior', *Proceedings of the National Academy of Sciences*, 2013, no. 15, p. 5805.
42. R. van Est, L. Kool, J. Timmer, *De datagedreven samenleving*, Rathenau Instituut report, The Hague, 2015, p. 43.
43. Van Est, *De datagedreven samenleving*, p. 46.

data in the surveillance economy stimulates all kinds of parties to collect as much personal data as possible, and this is harmful to the privacy of individuals.

3.5 Influencing behaviour in the digital market

The surveillance economy goes beyond merely predicting individual behaviour. It also attempts to influence and steer individual behaviour. This has major consequences on individual autonomy. Firstly, there may be direct external influences the individual is aware of. We currently see healthcare insurers that are looking at how customers can be encouraged to lead healthy lifestyles. This benefits both customers (better health) and healthcare insurers (lower healthcare costs).

Healthcare insurers reward healthy behaviour
Nowadays, several healthcare insurers offer rewards to their clients for moving around enough. Clients can track how much they move using a *fitness tracker* and their health insurance app. This then generates points that can be used to earn rewards, such as a discount code to an online store. Financial rewards are offered in return for healthy behaviour, and this can amount to significant sums per month. Customers are encouraged to move around more with weekly goals. An example of this is the Vitality programme, offered in Germany, France, Spain and the Netherlands, with some 10 million participants worldwide.

This seems to be a win-win situation, resulting in cost savings for both the customer and the health insurance provider. However, there are some objections to this arrangement. First of all, offering financial rewards to healthier people is a politically sensitive matter. There is a risk that this could potentially create a precedent for more far-reaching reward schemes, in which people with unhealthy lifestyles (who generally speaking are the less affluent people anyway) would increasingly pay relatively more. The way in which healthy behaviour is encouraged

could also become more drastic. For example, in South Africa, there is a variation of the Vitality programme which includes food choices.[44] Medical experts also question whether the most relevant target audiences are being reached. It appears that these measures mostly interest individuals with higher incomes who are already more likely to prioritise their health as it is. So the question is whether rewards of this sort can break years of unhealthy behaviour cycles.[45]

Something that makes these fitness tracking programmes a particularly sensitive issue is that users are obliged to share medical data with health insurance companies. For example, in the case of Dutch health insurer ASR's Vitality programme, the more medical personal data you share with them, the bigger the discount you get. This includes things like living and eating habits and whether you smoke or have smoked in the past. Its privacy statement says that such data is used, among other things, for targeted advertisements. Although insurer ASR stores this data in Frankfurt, it also states that the use of the apps and fitness tracker is the user's responsibility.[46] Many suppliers are also located outside the EU and store their data there. In this instance, the GDPR becomes more difficult to enforce, which means that medical data can be misused.

And with these health insurance discount programmes, individuals are at least still aware that external parties are trying to influence their behaviour, which is not always the case in the digital world. This involves indirect external influence, in which the individual has little to awareness of the behavioural influence. This can have negative effects when individuals are steered towards making choices that go against their own best interests. Above all, it violates their autonomy. This sort of manipulation often occurs in the digital world. We have previously mentioned the world of online marketing. This attempts to predict the needs of individuals and offer them particular services or products on that basis. This can target certain vulnerabilities of particular individuals

44. Discovery, 'HealthyFood', URL: https://www.discovery.co.za/vitality/healthyfood, accessed: 16 June 2021.
45. R. Bertens, K. Jongsma, 'Premie korting bij gezond gedrag: moeten we dat willen?', *Medisch Contact*, 2020, no. 23, pp. 35-36.
46. ASR, 'a.s.r. Vitality – Privacyverklaring', URL: https://www.asr.nl/vitality/privacy, accessed: 16 June 2021.

known to market parties. For example, McDonalds specifically targeted the children of low-income groups on the assumption that they were more likely to be tempted to consume fast food.[47] We can find similar algorithm-driven profiling and personalisation in web searches and suggested content on social media. The information asymmetry between individuals and market players means that individuals can never be sure about exactly what information of theirs is getting used, to determine the content that is being shown. This is detrimental to individual autonomy because users do not know to what extent and in what way their behaviour is being influenced.

A variety of influencing tactics are used for this. The concept of '*nudging*' is all about giving a 'gentle push in the right direction'. Psychological tricks are used to steer individuals towards making particular choices in their own supposed best interest.[48] This is a concept taken from behavioural economics, which claims that people often make different choices to the ones they want to make. Individuals often fail to make sensible choices – these could be things like healthy eating, but also financial matters – out of convenience or other temptations. This is where a *nudge* can be helpful. For example, a gym café that places fruit on the most accessible shelves. We see a similar sort of *nudging* taking place in the surveillance economy, but it is one that is absolutely not in the best interests of the individual. The clients are not the users (individuals), but the advertising market parties. Tactics are used to encourage individuals to spend as much money as possible by capitalising on their psychological weaknesses. These types of unconscious behavioural patterns are exploited at individual level, undermining the ability of individuals to make autonomous, rational decisions.

One variation of this is 'gamification', where game mechanics are introduced into an environment with the intention of manipulating the behaviour of individuals.[49] For example, there are various applications that provide language learning in game form, in which points can be

47. M. Gallagher, 'How McDonald's social ads impact health of global youth', *Medical News Today*, 6 January 2022, URL: https://www.medicalnewstoday.com/articles/how-mcdonalds-social-ads-impact-health-of-global-youth, accessed: 28 March 2022.
48. C.R. Sunstein, R.H. Thaler, *Nudge: Improving Decisions about Health, Wealth and Happiness*, London, 2009, p. 5.
49. D. Basten, 'Gamification', *IEEE Annals of the History of Computing*, 2017, no. 5, pp. 76-81.

earned. The game and the competitive elements can encourage individuals to continue and good behaviour is rewarded. A well known example of gamification is Pokémon Go that was launched in 2016 to enormous hype. In this game, the player uses augmented reality (AR) to capture Pokémon characters at locations in the real world. This encourages people to spend time exercising outdoors, promoting healthy behaviour. However, it turned out that restaurants and bars and other businesses were using the app to summon Pokémon characters to their premises, to draw customers to their establishments. McDonalds Japan even made a special deal with the makers of the app, so their branches became key game locations.[50] As a result, players were steered towards fast-food restaurants, encouraging unhealthy behaviour.

In the surveillance economy, extensive use is made of behavioural psychology. Social media companies (and other market players too) deliberately look to create addiction among their users. After all, the more their services are used, the more advertisements can be shown. This sort of slot machine design is sometimes referred to as '*addiction by design*'.[51] In order to grab their users' attention, algorithms endlessly vary the way they display content. Unpredictable rewards of this type of work like slot machines, where the ever-present but unpredictable chance of a reward has an addictive effect on players. As early as 2017, the Central Bureau of Statistics in the Netherlands established that one in ten users is addicted to social media.[52, 53]

The combination of tactics used to predict and influence behaviour imperil both the privacy and autonomy of the individual. Furthermore, these same surveillance economy tactics have now been adopted by all

50. D. Verlaan, 'McDonald's betaalt voor aantrekkelijke locaties in Pokémon Go', *RTL Nieuws*, 22 July 2016, URL: https://www.rtlnieuws.nl/tech/artikel/479101/mcdonalds-betaalt-voor-aantrekkelijke-locaties-pokemon-go, accessed: 17 June 2021.
51. Netflix, 'The social dilemma' (documentary), 26 January 2020.
52. J. van Beuningen, R. Kloosterman, *Opvattingen over sociale media*, Centraal Bureau voor de Statistiek report, The Hague, 2018, p. 3.
53. There is another interesting discussion around the extent to which the use of behavioural manipulation, and in particular creating addictions, can be justified when it involves underage users. Many social media platforms impose an age limit, but in practice this rarely seems to be enforced. Social media addiction appears to be major problem, especially among children and young people. Serious discussions are needed both about the policy of these platforms, and the role of parental responsibility in this regard.

sorts of other parties, for example in the field of political influence (see the next chapter for more about this). This is why it is so important to understand something as seemingly trivial as personalised advertising as part of an underlying system that is actually damaging to liberal values. Authors like Yuval Noah Harari employ sinister terms like '*brain-hacking*' to indicate how the surveillance economy collects our personal data and uses it to manipulate us.[54] From a liberal perspective, it is unacceptable to allow the surveillance economy to run its course. Therefore the question becomes: how can liberal values guide us in the creation of a better system?

Firstly, the predictive ability of market players is reduced when they have fewer data points from which to extrapolate behaviour patterns. Therefore it is necessary to strive for the greatest level of privacy possible for individuals in the market. Purpose limitation, as established under Article 5 of the GDPR, is an essential concept here. Companies should only collect personal data that is actually needed for a specific, explicitly described and legitimate purpose. This data should not be kept for longer than necessary.[55] Nor may these be shared with third parties without good cause. Anonymisation and pseudonymisation of personal data are also a means to help conceal individual identities, although it can be hard to prevent re-identification when several data points are connected. Therefore it is necessary to also think about how different strands of personal data can remain separated from each other, in as far as possible. This will be hard in practice because this is the basis for so many data revenue models. The role of regulators is important here, they must be able to take tough action in the event of unlawful collection, connecting and use of data. Rights under the GDPR can only be structurally guaranteed if enforcement is strengthened significantly. Therefore, regulators need be able to issue much higher fines.

It is important to realise that regulations and strict enforcement are the only way we can make a difference, and that individuals cannot be expected to take responsibility for these issues. Nonetheless, it is useful to raise awareness. Some change is underway with regard to that. For example, experts regularly bring out books and articles on

54. Wintergasten, 'Yuval Noah Harari' (documentary), *VPRO*, 27 December 2021.
55. European Parliament and Council, *Regulation (EU) 2016/*679, Article 5.

the surveillance economy and this is increasingly the subject of television programmes and documentaries.[56] Informed individuals can take measures to escape the surveillance economy as much as possible. This might be by setting up a 'virtual private network' (VPN), with which to encrypt an internet connection or by opting to use a privacy-friendly search engine like DuckDuckGo.[57] The European Parliament has highlighted things like the automatic rejection of third parties *cookies* in the browser.[58] There are also quality scores for privacy, for which companies are assigned a privacy score.[59] Initiatives of this sort make it easier for individuals to make informed choices between different market parties. Healthy market competition remains important, but digitalisation presents unique challenges in this area.

3.6 The economic power of *Big Tech*

In the last decades, a few companies have emerged in the digital domain that now completely dominate the market. This success has served these companies well. Four of the five richest people in the world are tech-entrepreneurs: Jeff Bezos (Amazon), Elon Musk (Tesla, previously PayPal), Bill Gates (Microsoft) and Mark Zuckerberg (Facebook).[60] 'Googling' and 'Tweeting' are established words in our vocabulary and the cinema shows Hollywood movies on the stories behind these Tech Giants such as *The Social Network* (2010) and *Steve Jobs* (2015). In Silicon Valley (USA), where many of these Tech Giants are headquartered, important decisions are taken that directly affect our lives. The extent of the power

56. Netflix, 'The social dilemma' (documentary), 26 January 2020.
57. DuckDuckGo, 'Over ons', URL: https://duckduckgo.com/about, accessed: 2 May 2022.
58. Europees Parlement, '10 tips om uw privacy op het internet te beschermen', URL: https://www.europarl.europa.eu/thenetherlands/nl/eerder-in-het-nieuws/10-tips-om-uw-privacy-op-het-internet-te-beschermen, accessed: 21 June 2021.
59. P. Kulche, 'De Privacymeter maakt privacy makkelijk', *Consumentenbond*, 29 April 2021, URL: https://www.consumentenbond.nl/internet-privacy/hoe-werkt-de-privacymeter, accessed: 21 June 2021.
60. K.A. Dolan, 'Forbes' 35th annual world's billionaires list: facts and figures 2021', *Forbes*, 6 April 2021, URL: https://www.forbes.com/sites/kerryadolan/2021/04/06/forbes-35th-annual-worlds-billionaires-list-facts-and-figures-2021/?sh=23ee37d25e58, accessed: 14 May 2021.

residing in this Californian tech hub is evidenced by the fact that Denmark recently sent an ambassador there.[61] [62] The Eurasia Group refers to it as a 'technopolar world', where nowadays not only nation states, but also large tech companies are major protagonists on the geopolitical playing field.[63]

There are a few reasons why only a small number of companies are currently calling the shots in the digital world. As already mentioned, data collection provides many economies of scale, creating a positive feedback loop. The more data you have at your disposal, the better your features, personalisation, marketing campaign, etc. This results in more customers, with even more data. This way, data can lead to exponential growth. Something that many Tech Giants have in common is that they were early providers of the services or product they offer and so have been able to collect a lot of data. Therefore, they now have a head start that is almost impossible to catch up.

A second reason we see in many tech businesses is a so-called 'network effect'. This is what happens when the value of a service or product increases the more people use it. The larger the user group, the more appealing it becomes for new users to join. Therefore, value creation occurs not only on the supply side, but also on the demand side.[64] [65] Take social media platforms like Facebook and (X, formerly Twitter) as an example. The more people use these platforms, the more interesting it becomes for others to do so. After all, there are more connections for you to make with other users, increasing your reach. The same effect can be seen on mediation platforms like Uber. The more drivers there are working on the platform, the easier it is for clients to find a ride. More clients attract more drivers. This creates a positive feedback loop here too.

---

61. P. Baugh, ''Techplomacy': Denmark's ambassador to Silicon Valley', *Politico*, 20 July 2017, URL: https://www.politico.eu/article/denmark-silicon-valley-tech-ambassador-casper-klynge/, accessed: 18 May 2021.
62. A pertinent detail is that Casper Klynge, the first person to occupy this position, now works for Microsoft.
63. I. Bremmer, C. Kupchan, *Top Risks 2022*, Eurasia Group report, New York, 2022, pp. 5-6.
64. M. Kreijveld et al., *De kracht van platformen. Nieuwe strategieën voor innoveren in een digitale wereld*, Rathenau Instituut report, The Hague, 2014, p. 265.
65. As we saw earlier, this is not because users are more willing to pay (they use the service free of charge), but because market parties (the real customers of these services) have a larger group of users to whom they can target advertisements.

A third reason why power is so concentrated in this market is the '*lock-in*-effect'. By this we mean when switching from a provider to a competitor is made more difficult because of additional inconveniences or extra costs. Many Tech Giants offer various services and products and integrate certain features between them.[66] This creates their own extensive digital ecosystems. This provides users with certain useful features. If a consumer moves to a competitor, they lose these functions and sometimes have to repurchase things they'd already bought previously. Apple, who provide phones, tablets and laptops within their own ecosystem, is a good example of this. These hardware products all run on Apple's own operating system and use various applications unique to Apple. It is very easy to shares files between them, but hard to share them with devices that run on other operating systems. Additionally, there are applications that only work on Apple products, and therefore become unavailable if you move to a competitor. Google has a similar sort of *lock-in*-effect with its operating system.

A fourth reason for the power of *Big Tech* is that several companies are not only active as market players, but also have a role as market regulators. They have created digital market places in which they are also active as retailers. And in this dual role they give their own products priority. This is the case, for example, for companies that manage platforms, online stores or app stores. For example Google and Apple, as well as Amazon. This tech conglomerate started out as an online store, but over the years it has also slowly started to enter into all sorts of different areas. The company now has its own *cloud-*, *streaming* and delivery service and also offers all kinds of private label products.[67] As the administrator of the Amazon online store, Amazon can display its own products to visitors first, giving it a competitive advantage. Competitors can also be denied access to the digital marketplace or required to pay a fee.

As a consequence of the above, market power has become entirely concentrated among today's Tech Giants. This seems to be a *winner-takes-all*-situation and there is little space for new players to enter the market. The Tech Giants have so much financial power that they can drive away new businesses entering the market, by temporarily setting a

66. Kreijveld, *De kracht van platformen*, p. 96.
67. Amazon, 'Amazon Basics', URL: https://www.amazon.com/stores/AmazonBasics/AmazonBasics/page/947C6949-CF8E-4BD3-914A-B411DD3E4433, accessed: 17 May 2021.

lower price (*predatory pricing*) or by simply acquiring them. Acquisitions worth billions regularly take place in this sector. For example, in 2016, Microsoft acquired LinkedIn, the world's largest professional network, for 26.2 billion dollars. In 2014, Facebook bought the chat application WhatsApp for 22 billion dollars.[68]

On the one hand, there is something to be said for the fact that these Tech Giants have become so rich and powerful. They often offer products and services which require investment costs so high that only those with vast amounts of capital can afford them. For example, the development and maintenance of high-quality software products. Furthermore, these Tech Giants also invest in new technologies in robotics, cyber security and the healthcare industry.[69] Breakthroughs in these areas are in everyone's interest and these Tech Giants have the capital and know-how to do a lot of good.

At the same time, too great a concentration of market power can also have significant drawbacks, including less consumer choice, higher prices, a less dynamic market and less innovation.[70] The price mechanism that naturally allows supply and demand to meet is hereby disrupted. A lack of competition in this market can also prove disadvantageous to consumers.

3.7 A level playing field

Liberals are not only critical of governments abusing power, but also by market players. An important question to ask with regard to Tech Giants is whether they are examples of monopolies. Both the Scottish liberal Adam Smith (1723-1790) and the liberal John Stuart Mill were critical of the monopolies of their time.[71] The liberal view is that governments should intervene in markets to ensure competition when the creation

68. CB Insights, 'Visualizing tech giants' billion-dollar acquisitions', 24 February 2021, URL: https://www.cbinsights.com/research/tech-giants-billion-dollar-acquisitions-infographic/, accessed: 17 May 2021.
69. Google Ventures, 'Portfolio', URL: https://www.gv.com/portfolio/, accessed: 17 May 2021.
70. Schulz, *Een markt voor ons allemaal*, p. 73.
71. E.A. Posner, E.G. Weyl, 'Liberty versus monopoly', *American Affairs,* 2018, no. 4, pp. 55-56.

of monopolies becomes detrimental to consumers. This happens when a monopoly abuses its power to prevent innovation.[72] As we saw earlier in section 2.1, liberals consider innovation to be essential to progress. Creative destruction ensures that market players are under continual pressure to innovate (or else rendered obsolete by the competition) and society as a whole continues to reinvent itself. The government fulfils the role of market regulator, guaranteeing a level playing field for all market players and preventing abuse of power.

The economic power *Big Tech* has is being put up for debate in the hearings initiated by the United States Government.[73] During these hearings, these corporations were accused of anti-competitive monopoly power and compared to 19th and early 20th-century oil barons and railroad tycoons.[74] TeldersStichting's 2007 book *Vertrouwen in de markt* discusses how monopolies are formed. Firstly, governments consciously can prevent new parties from entering the market, in order to maintain control over an industry guarantee the quality and independence (legal monopoly). Secondly, when a single, large market party is able to draw up economies of scale to produce something at a far lower cost compared to several small market parties doing the same (natural monopoly). Thirdly, when a manufacturer makes a product that offers so many more advantages or is cheaper than the alternatives available on the market, driving out all of the competition.[75]

Big Tech belongs within the second and third categories. At the same time, these enterprises are active in various different markets. For example, Google can be considered a monopoly in the internet search engine arena, but it is a competitor of Facebook when it comes to advertising

72. This is also a key idea in German 'ordoliberalism', considered a sub-movement within liberal philosophy, which explicitly states that the government must ensure the preconditions for free competition. This movement arose mainly in response to the monopoly and cartel formations of the late 19th century and sought to prevent powerful market players from using their position to manipulate the market.

73. K. Paul, D. Rushe, ''Too much power': Congress grills top tech CEOs in combative antitrust hearing', *The Guardian*, 29 July 2020, URL: https://www.theguardian.com/technology/2020/jul/29/tech-hearings-facebook-mark-zuckerberg-amazon-jeff-bezos-apple-tim-cook-google-sundar-pichai-congress, accessed: 18 May 2021.

74. 'US tech giants accused of 'monopoly power'', *BBC News*, 7 October 2020, URL: https://www.bbc.com/news/business-54443188, accessed: 18 May 2021.

75. F. de Graaf et al., *Vertrouwen in de markt. Naar een liberaal privatiseringsbeleid*, report by Prof.mr. B.M. TeldersStichting, The Hague, 2007, p. 41.

services for business customers (upon which the revenues of both corporations are based).[76] And while Amazon dominates several markets, the corporation experiences very stiff competition from Netflix and Disney when it comes to streaming services.[77] In that sense, these corporations function in many markets more like oligopolies, with a small number of large suppliers experiencing stiff competition from one other. However, oligopolies can still have a distorting effect on competition when market players form cartels and make price agreements with each other. And their strong financial position means that these market players can also use takeovers to hinder newcomers from entering the market.

One way to establish whether healthy competition exists is to look at the creative destruction mentioned above. Is there continuous technological innovation, in which outdated and obsolete technologies are continuously replaced by new and better technologies? The author Bryan Bourne lists several examples of corporations considered to be monopolies at their peak, but now play little to no role in the market. MySpace as a social media platform, Nokia as a phone seller and Apple as a music supplier with iTunes.[78] They were all overtaken quickly by better alternatives. In this sense, the market in which these Tech Giants operate is volatile and sensitive to hype. A misstep or slow reaction to a new development on the market can bring about the demise of positions of long-standing dominance.

Nevertheless, there are also plenty of examples where creative destruction seems to be in short supply. Buying up the competition has become the proven strategy of large tech corporations. Companies can be acquired with the aim of speeding up their innovation, thanks to the scaling options and large sales market of *Big Tech*. However, the intention of large tech companies is not always to promote innovation in the market, but to prevent their own technologies from becoming irrelevant. Then acquisitions become a means of preventing creative destruction and securing their own position in the market. This '*buy*

76. R. Bourne, *Is This Time Different? Schumpeter, the Tech Giants, and Monopoly Fatalism*, Cato Institute policy analysis no. 872, Washington D.C., 2019, p. 2.
77. J. Koetsier, 'Netflix beating Amazon, Hulu, Disney+ with 42% share as streaming doubles', *Forbes*, 7 April 2020, URL: https://www.forbes.com/sites/johnkoetsier/2020/04/07/netflix-beating-amazon-hulu-disney-with-42-share-as-streaming-doubles/?sh=83eabd06cecf, accessed 25 May 2021.
78. Bourne, *Is This Time Different?*, pp. 6-12.

and kill' strategy often provides the financial deal of a lifetime for startup entrepreneurs whose companies get bought out, but has a negative effect on the economy as a whole by preventing innovation.[79] This is clearly an example of building a monopoly and from the liberal perspective that is highly undesirable.

It is often said that tech companies should be broken up. That might well be effective in the short term, but nonetheless it is not an ideal solution. Not only would this be difficult from a legal standpoint, but there are no guarantees that when a corporation is split up, power does not end up once again concentrated in the hands of one of the split parties, given the inherent scaling and network effects outlined in the section above. It would merely mask the symptoms, leaving things open to misuse once a market party has regained all it power. The rules of the game are severely lacking and allow players to abuse the situation. Therefore, procompetitive regulation should not focus primarily on breaking up individual market players, but rather on how the market *itself* functions. Breaking up tech companies should only be a final option in combination with these measures.

The steps that need to be taken to safeguard the free market mechanism is something currently being looked into. The way in which some corporations currently fulfil a dual role of market player and market regulator in the digital marketplace is a prime example of the type of abuse of power that needs to be addressed. As mentioned above, the liberal opinion is that the market regulator role should be reserved for the government, which must guarantee a level playing field. Tech companies should therefore be able to set up digital marketplaces, but abandon the role of market regulator (determining the rules of this marketplace). Legislation must prohibit market parties from setting up digital marketplaces in which they are able to prioritise their own products. The separation of roles prevents a conflicts of interest. This would allow all market players to enjoy the reach that such digital marketplaces offer, while also ensuring fair competition.

---

79. R. Waters, 'Big Tech 'buy and kill' tactics come under scrutiny', *Financial Times*, 13 February 2020, URL: https://www.ft.com/content/39b5c3a8-4e1a-11ea-95a0-43d18ec715f5, accessed 22 July 2021.

It is also necessary to take a closer look at how consumers are inconvenienced when they look to switch from a provider to a competitor. All too often, tech corporations appear to put up unnecessary barriers, deliberately aimed at giving themselves the competitive advantage. There is a need to increase the interoperability between products and services, with greater scope for different hardware and software products to interact with each other. For example, it needs to be easier to transfer files. Therefore, it is important for government to promote standardisation. Interoperability can be increased by including certain requirements within regulatory standards, thus benefitting market competition. Consider, for example, the standardisation of chargers, so that these no longer have to be bought separately for every product.

In a similar vein, tech corporations must be made to improve the right to data portability (as established in the GDPR). It must be possible – and easy – to take your data with you from one market player to another. For example, a restaurant should be able to transfer its online reviews on Google to other platforms, in order to prevent dependency. Users should also be able to easily transfer emails and photos stored in the cloud from one provider to another. This feature must also be introduced when it comes to data portability, in exactly the same way that the right to retain phone numbers was established in the past.

Another form of abuse of power that we encounter regularly in this market is that tech companies engage in tie-in selling, in which different products and services are bundled and can only be purchased together. Tech corporations sometimes force extra costs on consumers because there are no alternatives. For example, Microsoft linked a media player to its Windows operating system, forcing consumers to purchase it.[80] In such cases, the government must enforce the detachment of these products and services, so that consumers can make their own choices on the market.

There must also always be checks in place that assess whether the various tech companies have made any illegal cartel agreements between

80. Autoriteit Consument & Markt, 'Misbruik van economische machtspositie: koppelverkoop', URL: https://www.acm.nl/nl/onderwerpen/concurrentie-en-marktwerking/concurrentie-en-afspraken-tussen-bedrijven/bedrijven-met-een-machtspositie/misbruik-van-machtspositie-voorbeelden/misbruik-van-machtspositie-koppelverkoop, accessed: 29 March 2022.

them. For example, Google and Facebook are currently accused of cutting a secret deal, in which Facebook is alleged to have made competitive commitments to Google's advertising services in exchange for preferential treatment.[81] Cartel agreements of this sort are illegal under current legislation, so it should be possible to impose sanctions under the current legal framework.

Furthermore, it is also necessary to examine the possible anticompetitive practices of takeovers more rigorously. Facebook acquired Instagram in 2012 and WhatsApp in 2014, clearly with the intention of preventing them from developing into fully fledged competitors. In the United States, the market regulator is currently looking at whether Facebook should be forced to divest itself of these parties.[82] This is likely to lead to a long and complex legal battle, even though it was actually clear all along that these takeovers would hinder competition. In future, in order to guarantee marketplace innovation, potential abuse of power will need to be monitored much more closely during takeovers of this sort. As well as large acquisitions like this, it will also be necessary to combat *buy and kill* policy when purchasing startups. Before acquisitions like this, large tech companies must be made to commit to a set of criteria in which they promise to further develop the innovation of these startups, rather than stopping them. If it later proves to have been a case of *killer* acquisition, the tech corporation must be fined or even forced to divest itself of the party.

All these measures require strong regulation. Regulators must therefore be provided with adequate resources with which to uncover and tackle abuses of power. This requires a suitable budget, as well as the authority to enforce certain measures, such as the ability to issue fines high enough to act as a deterrent. If the bottom line is that companies make

---

81. R. Tracy, J. Horwitz, 'Inside the Google-Facebook ad deal at the heart of the price-fixing lawsuit', *The Wall Street Journal*, 29 December 2020, URL: https://www.wsj.com/articles/inside-the-google-facebook-ad-deal-at-the-heart-of-a-price-fixing-lawsuit-11609254758, accessed: 25 May 2021.

82. 'Facebook aangeklaagd in de VS, moet mogelijk Instagram en WhatsApp afstoten', *RTL Nieuws*, 9 December 2020, URL: https://www.rtlnieuws.nl/economie/bedrijven/artikel/5202291/facebook-instagram-aangeklaagd-verenigde-staten-zuckerberg, accessed: 9 December 2015.

enough money from such practices despite being fined, these measures will be of little to no effect.

Moreover, the policy will have to be regulated predominantly at EU level. Liberals attach great value to the principle of subsidiarity, which means that decisions should be made at the lowest possible level of government.[83] This means that politics remains as close to citizens as possible, and that power can be monitored. In a case like this, the enormous economic – and political – power of Big Tech demands a Europe-wide approach. Individual member states have too little influence to make much of a difference on their own, whereas by banding together, European countries become a power to be reckoned with, given the size of the sales market they form as a whole for these tech companies. Moreover, the expertise available at national level may be inadequate, while they can gain strength by coming together at European level.

The European *Digital Markets Act* (2022) recently came into force. It lays down various concrete measures to firmly tackle abuses of power by tech companies. The law applies to the companies that the EU qualifies as 'gatekeepers'. These are platforms that have a significant impact on the internal market, operate one or more key gateways for access to customers, and have or are expected to have an entrenched and sustainable position through their operations.[84] This law makes explicit mentions of unlawful self-advantage on the gatekeepers' own platforms, lack of interoperability, unjustified linking of services and products and other types of abuse of power.[85] Thus the EU appears to be taking important steps towards ensuring a fairer playing field in the market. From a liberal perspective, such pro-competition legislation is only to be encouraged.

Tackling these companies in particular should therefore have an effect on the market as a whole, given the pivotal position they occupy. This distinction is also important to prevent unintentionally burdening

83. R. Kubben, 'Geloven in vrijheid. Een bijdrage aan een lopend debat', *Liberaal Reveil*, 2008, no. 3, p. 115.

84. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act))*, Brussels, 2020, p. 2.

85. European Commission, 'Wet inzake digitale markten: voor eerlijke en open digitale markten', URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_nl#wat-zijn-de-volgende-stappen, accessed: 25 May 2021.

SMEs and startups with excessively onerous regulations, which currently appears to be the case with the GDPR. These companies lack the resources that gatekeepers have at their disposal to comply quickly with new regulations. Therefore, it is always important before introducing new competition-promoting legislation to check carefully whether it does not unintentionally create a disproportionate administrative burden for smaller companies, which would actually worsen their position on the market.

3.8 Conclusion

In this chapter we looked at how digitalisation has changed the economy. We emphasised the crucial role data plays as a new factor of production. Entirely new revenue models have emerged that revolve around collecting this data. All sort of personal details are contained within it, which has consequences for the privacy of citizens. Personal data is collected for the delivery of certain features, as well as for the personalisation of products and services, and in order to sell this data on to other market parties. These revenue models are highly profitable, so many digital services are provided free-of-charge in order to attract large numbers of users. This is a fundamentally different sort of market to anything we have known previously, in which companies do not see individuals as consumers, but as products.

Sometimes this is incorrectly referred to as a financial transaction, in which personal data is used as the relevant currency and traded off in return for ownership over said personal data. Firstly, this has the potential to conflict with public interest and the provision of information, and secondly, it could facilitate abuse of power by market parties, because individuals sometimes then lose control over personal data. The idea of control of personal data established in the GDPR is more aligned with the liberal view of privacy, which considers it an inalienable natural right. The GDPR is further legitimised from a liberal perspective because it enhances individual freedom by increasing individual rights, while neither endorsing nor prohibiting particular actions. As such, the autonomy of the individual is taken as a starting point. There is a need for a practical infrastructure within the digital domain to make it easier for

individuals to make use of their GDPR rights. Regulations must be made clearer for anyone processing data because, currently, SMEs in particular are struggling to interpret them. However, the main issue seems to be that large tech companies do not comply adequately with this legislation, while they are the greatest threat to liberal values.

While individuals need to have their freedom of action increased, companies need theirs restricted in certain areas. To a growing extent, a surveillance economy is emerging. The collection of personal data, with the intention of predicting and subsequently influencing behaviour, is a fundamental threat to individual privacy and autonomy. It is therefore important that market parties adhere to the purpose limitation principle, anonymise and pseudonymise data in as far as possible, and definitely refrain from connecting various data points. This makes the role of regulators very important. They need to be prepared to take tough action and have the ability to impose significant fines. The height of the fines must be proportionate to the vast income of these large tech firms. This will ensure that fines are not just seen as a nuisance, but as a real deterrent. Without this increased regulation, tech companies will continue to flout the rules, as these conflict with their own data revenue models. In order to aid this process, it's also important to increase awareness among individuals about the surveillance economy, and what they can do to escape it in as far as possible.

There is also a clear concentration of power in this market, with a small number of players having emerged as true tech giants. This is due to the scalability of data, as well as the network and *lock-in* effects and the conflicting nature of the dual role some parties have as both market player and market regulator. It is not always easy to ascertain whether monopolies are being formed, as these companies often operate in multiple markets. However, we do see that their powerful position gets in the way of creative destruction. Breaking up tech companies does not seem to be a good solution. It is actually the lack of market 'rules' that enable these market players to abuse their position. In the first instance, regulation should not be targeted at specific market players but at the market itself. There is a need for pro-competitive legislation aimed at the separation of roles, interoperability, data portability, and a ban on both tie-in sales and *buy-and-kill* acquisitions. As previously mentioned, a violation of these rules should be met with significant fines. The final

option, in combination with these measures, is to break up the tech companies. Legislation of this type and the enforcement thereof will largely have to be implemented at European level, given the might of these tech businesses and the international nature of digitalisation.

Europe took a major first step with the GDPR towards setting up a legal framework in which liberal values such as privacy and autonomy were key. The EU has adopted a pioneering role and appears to want to expand this further with initiatives like the *Digital Markets Act.* Legislation of this kind is essential to creating a free market in which competition is guaranteed and the commercial interests of market parties are not allowed to come at the expense of liberal values.

4. Digitalisation & democracy

4.1 Democracy in the digital age

Democracy is an inherently dynamic political system. Every individual with a right to vote has a say in society, this ensures that the debate surrounding what is in the best interest of society continues to be held. For liberals, this is where the strength of democracy lies, in comparison to other political systems. Digitalisation has further reinforced this dynamic. Information flows have become faster and more accessible and citizens interact with each other in new ways, in the virtual world. The application of digitalisation can, in fact, serve to strengthen democracy.

For example, IT can be used to support democratic processes, sometimes referred to as *'e-democracy'*. An interesting example of this in Europe is Estonia. Since its independence in 1991, this former Soviet republic has increasingly embraced digitalisation as the cornerstone of its political system.[1] In doing so, the country is trying to make democracy more inclusive and direct. For example, it has declared internet access a human right. Furthermore, citizens are actively involved in democratic processes through digital channels, not only in electoral periods, but also in between, during other political decision-making processes.[2] This way, digitalisation is used to stimulate active citizenship among the population, which benefits democracy.

---

1. E-Estonia, 'This is the story of the world's most advanced digital society', URL: https://e-estonia.com/, accessed: 4 June 2021.
2. F. Plantera, 'Inclusive policies call citizens to act. Democracy in a digital society, at the e-Governance Academy', *e-Estonia*, URL: https://e-estonia.com/inclusive-policies-citizens-act-democracy-digital-society/, accessed: 4 June 2021.

There are also examples of authoritarian regimes that have been brought down – in part – through digitalisation. Tunisia, for example, suffered under a dictatorship for decades, which was overthrown in a popular uprising in 2011. People used social media platforms like Facebook to share information about political developments, and organise protests.[3] Recent demonstrations in Cuba and Belarus have also been facilitated by social media.[4] [5] As such, digitalisation can pose a threat to dictatorial power. While dictators can control and censor traditional media, this is has proved much harder to do on the internet.

Nevertheless, this seems to be slowly changing. Those in power are taking initiatives to stop the democratising effect of digitalisation, and to use it to strengthen their own dominant positions instead.[6] Large parts of the internet are restricted and information is distributed according to their own best interest. This is exactly what we saw happen after the protests in both Cuba and Belarus. China, in particular, has demonstrated how, by bringing the digital world under state control, digitalisation can be turned into the cornerstone of an authoritarian regime. In 2000, the US President at the time, Bill Clinton, quipped that China's attempts to control the internet would be like trying to 'nail Jello to a wall'.[7] Nevertheless, thanks in no small measure to what has been dubbed the '*Great Firewall of China*', the country seems to be having some success in regulating and censoring the internet within its own borders. China currently uses digital technologies to observe and control its citizens in various ways. In fact, its model of 'digital authoritarianism' seems to have been

3. E.A. Fox et al., 'The use and impact of social media during the 2011 Tunisian Revolution', paper for the 17th International Digital Government Research Conference, Shanghai, 2016, p. 5.
4. C. Barría, 'Protestas en Cuba: qué papel juegan "la directa" y las redes sociales en las históricas manifestaciones en la isla', *BBC Mundo*, 13 July 2021, URL: https://www.bbc.com/mundo/noticias-america-latina-57783099, accessed: 23 July 2021.
5. S. Walker, 'Belarus protesters use Telegram to keep pressure on Lukashenko', *The Guardian*, 1 November 2020, URL: https://www.theguardian.com/world/2020/nov/01/telegram-belarus-protesters-pressure-lukashenko, accessed: 28 September 2021.
6. M. Janssen, N. Karkin, 'Structural changes driven by e-petitioning technology: changing the relationship between the central government and local governments', *Information Technology for Development*, 2020, no. 4, pp. 837-855.
7. B. Allen-Ebrahimiam, 'The man who nailed jello to the wall', *Foreign Policy*, 29 June 2016, URL: https://foreignpolicy.com/2016/06/29/the-man-who-nailed-jello-to-the-wall-lu-wei-china-internet-czar-learns-how-to-tame-the-web/, accessed: 4 June 2021.

adopted by increasing numbers of undemocratic countries including Egypt, Venezuela and the Philippines.[8]

But we can also see in our society that digitalisation not only has positive effects, but also negative effects on democracy. For example, the free and accessible nature of the internet allows information to be disseminated with greater ease. However, this applies just as much to incorrect information as it does to factually correct information. Misinformation and disinformation have become serious problems. Furthermore, some citizens live increasingly within their own information bubbles, mostly due to social media. We are also seeing that social media platforms struggle in their roles as discussion and news platforms within the democratic landscape, as well as various foreign actors who are trying to interfere in our democratic processes.

As previously mentioned, liberals see democracy as something broader than merely the idea of holding elections. It is also about healthy rational-critical debate within society. This chapter looks at the various ways in which democracy is coming under increasing pressure from digitalisation and how it can be prevented from degenerating into the 'hyper-democracy' feared by liberals (see section 2.6), in which individuals stop listening to one another and treat others as enemies. Once again, liberal values can lead the way in providing answers to the dilemmas that digitalisation raises for democracy.

4.2 Disinformation and its consequences on society

In early 2017, Kellyanne Conway, the advisor to then-US President Donald Trump, coined the phrase 'alternative facts' when speaking about the attendance numbers at the new president's inauguration.[9] This term was typical of what has since come to be known as the 'post-truth era'. In this new 'reality', facts appear to be reduced to mere opinions,

8. A. Shabaz, 'The rise of digital authoritarianism', *Freedom House*, URL: https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism, accessed: 4 June 2021.

9. NBC News, 'Kellyanne Conway: Press Secretary Sean Spicer gave 'alternative facts', *YouTube*, URL: https://www.youtube.com/watch?v=VSrEEDQgFc8&ab_channel=NBCNews, accessed: 9 June 2021.

with everyone free to form their own 'truth'. In this context, traditional media is portrayed as biased and corrupt and some people have turned to online alternatives instead. This is has caused citizens to become increasingly suspicious and susceptible to conspiracy theories.[10] We are increasingly confronted with similar developments in Europe too, as became particularly clear during the Covid-19 crisis. Various conspiracy theories surrounding Covid-19 circulated throughout society. A survey demonstrated that more than 30 percent of respondents in France, Italy, Germany and England believed that their governments were colluding with pharmaceutical companies to cover up the risks of vaccination.[11] Some people went as far as to claim that the virus was caused by the construction of the 5G network or that Bill Gates was behind the outbreak.[12] The World Health Organisation called this a clear case of an 'infodemic', alongside the pandemic.[13]

Digitalisation enables the easy dissemination of incorrect or distorted information. The term for incorrect information, spread without any intention to mislead, is 'misinformation'. Sometimes, people share incorrect information with others by accident. But the term for incorrect or distorted information used to deliberately mislead is 'disinformation'. The term appears to originate from the Cold War, when the Russian KGB (secret service) claimed to use *dezinformatsia* as a strategy for misleading the enemy with information.[14] However, this is not a new phenomenon. Attempting to mislead people through disinformation is

10. From a liberal perspective, a sceptical and critical attitude towards the authorities should in principle be encouraged. After all, we have seen in the past that not every conspiracy theory is (total) nonsense by definition. The issue is that the critical eye with which many conspiracy theorists view the '*mainstream* narrative', is totally absent when they come to assess the veracity of alternative theories. What is understood by conspiracy thinking here is a way of thinking that does not use scientific methodological falsification methods to test conspiracy theories.

11. J. Henley, 'Pandemic leaves Europeans more likely to believe conspiracy theories – study', *The Guardian*, 22 February 2022, URL: https://www.theguardian.com/world/2021/feb/22/covid-pandemic-leaves-europeans-more-likely-to-believe-conspiracy-theories-study, accessed: 17 July 2023.

12. S. van Heck, *Complottheorieën over het coronavirus*, report by Ipsos in collaboration with Nieuwsuur, Amsterdam, 2020, p. 3.

13. World Health Organization, 'Infodemic', URL: https://www.who.int/health-topics/infodemic#tab=tab_2, accessed: 9 June 2021.

14. R. Godson, R. Shultz, *Desinformatsia. Active Measures in Soviet Strategy,* Washington D.C., 1984, p. 37.

a strategy that has been used since time immemorial. 'Fake news', for example, was already being spread by political opponents among the Ancient Roman population.[15]

However, what is new in the digital age is the speed and scale at which disinformation can be spread. For example, 'botnets' – networks of large numbers of infected computers under central control – are used to spread disinformation on a massive scale. Furthermore, digital technology provides new and evermore sophisticated ways of creating disinformation. The Rathenau Institute has drawn attention to techniques like 'text synthesis', in which AI is used to automatically generate easily readable texts, and '*voice cloning*', which allows a voice to be imitated. '*Deepfakes*' also offer huge potential for disinformation. This technology allows AI to stick one person's face on to another person's head, so to speak, making it look like someone did or said something when in reality they never did.[16] Many of these technologies are still under development and therefore remain relatively easy to spot. But in the longer term, they will undoubtedly become better and cheaper – thus more accessible, potentially resulting in more disinformation. This is giving rise to an arms race between technologies that spread disinformation and those that identify it.

Not only has digitalisation brought about new ways of creating disinformation, but new channels have also emerged that make it very easy to share. These include social media platforms like Facebook and X (formerly Twitter). While traditional media employs editorial teams, this is not the case for social media. Editorial teams can serve as journalistic gatekeepers, verifying the authenticity of certain information.[17] The power of social media is that it allows information to be shared easily and freely. This is important for citizens in countries where there is less

15. I. Kaminska, 'A lesson in fake news from the info-wars of ancient Rome', *Financial Times*, 17 January 2017, URL: https://www.ft.com/content/aaf2bb08-dca2-11e6-86acf253db7791c6, accessed: 9 June 2021.
16. P. van Boheemen, E. Dujso, G. Munnich, *Digitale dreigingen voor de democratie. Over nieuwe technologie en desinformatie*, Rathenau Instituut report, The Hague, 2020, pp. 34-37.
17. Of course, there is always the danger that these editors bend information according to a particular political-ideological view. This is a criticism often made today of the traditional media. Sensationalism is sometimes also used as a means to attract more readers.

freedom, where the government controls the media. But the flipside of this is the ease with which disinformation can be sent out into the world, precisely because it is not verified. This can be detrimental to public debate and thus to democracy.

An even more dangerous issue with social media, perhaps, is the design of algorithms that deliver content in increasingly extreme forms. Sensational, provocative and polarising news reporting seems to take precedence over less exciting content. As we saw in the previous chapter, the slot-machine design of these platforms is aimed at keeping users online for as long as possible (and even getting them addicted), so that they can be shown as many ads as possible. And when it comes to disinformation, the societal impact it has is further reinforced, as users are then continually exposed to different, increasingly radical, variations. This sucks people into 'information tunnels' or 'echo chambers'. It is also how individuals end up encountering conspiracy theories.

In the United States, these conspiracy theories have become a serious problem in the political landscape.[18] They further polarise society and encourage individuals to engage in dangerous and violent behaviour. At the beginning of 2021, different groups of President Trump supporters stormed the Capitol – the seat of the US Parliament – convinced by false claims of election fraud. Many of them also proved to believe in all sorts of other conspiracy theories, such as 'QAnon'.[19] [20] Similar conspiracy theories are emerging increasingly in Europe too and causing grave security threats. For example, during the Covid-19 pandemic, various political figures came under increasing pressure from conspiracy

18. W.J. Derksen, 'From UFOs to Conspiracy Entrepreneurialism. How Conspiracy Theories Have Infected Politics in the United States', in: M. Milosz red., *Beyond Flat Earth: Conspiracy Theories vs European Liberals*, Brussels, 2021, pp. 73-83.

19. M. Biesecker et al, 'Who were they? Records reveal Trump fans who stormed the Capitol', *Associated Press News*, 11 January 2021, URL: https://apnews.com/article/us-capitol-siege-trump-supporters-8edfd3bb994568b7cdcd2243ad769101, accessed: 10 June 2021.

20. The QAnon theory claims that during his presidency, Trump was fighting a secret war against the so-called '*deep state*' consisting of satanist paedophiles in high-ranking positions in the government, business world and media. This theory can be seen as the successor to the Pizzagate conspiracy theory that arose around the time of the 2016 US presidential election, in which it was claimed that presidential candidate Hillary Clinton was part of a paedophile network run from the basement of a pizzeria.

theorists.[21] The EU Counter-Terrorism Coordinator has even warned of potential terrorist attacks perpetrated by conspiracy theorists.[22] As such, disinformation can pose a genuine security threat to society.

An interesting phenomenon that we have seen emerge in recent years is a wave of the so-called *conspiracy entrepreneurs*).[23] These are individuals who have established revenue models based on spreading conspiracy theories. In the USA, Alex Jones manages to draw millions of monthly visitors to his InfoWars website. Not only does this website share conspiracy theories, but it also offers its visitors all sorts of products to buy. These products are heavily promoted within all of his channel's content. People can also make voluntary donations. Thus, while presenting itself as a news website, it is actually an online store in disguise, making millions of dollars in profit.[24] This successful revenue model – in which visitors can buy products and donate money – has now been copied by other conspiracy entrepreneurs across the world. In Europe, there are people who want to cash in on the spread of conspiracy theories too.[25]

Disinformation is also problematic because misleading people also undermines the credibility of fact-based news, as well as affecting science and other institutions. This can only be expected to get worse in the future. For example, once *deepfakes* become indistinguishable from genuine videos, all videos will potentially be viewed with scepticism. After all, it's always possible that they could have been manipulated.[26]

---

21. J. Jonker, 'Kamervoorzitter Arib wil acties tegen 'zeer intimiderende' demonstraties rond Binnenhof, *NOS*, 14 October 2020, URL: https://nos.nl/nieuwsuur/artikel/2352298-kamervoorzitter-arib-wil-actie-tegen-zeer-intimiderende-demonstraties-rond-binnenhof, accessed: 10 June 2021.
22. L. Dearden, 'New forms of terrorism inspired by conspiracy theories may emerge after pandemic, warns EU counter-terror chief', *The Independent*, 1 September 2020, URL: https://www.independent.co.uk/news/uk/home-news/coronavirus-conspiracy-theory-terrorism-5g-gilles-de-kerchove-a9699571.html, accessed: 17 June 2023.
23. Frontline, 'United States of conspiracy' (documentary), *PBS*, 28 July 2021.
24. E. Steel, E. Williamson, 'Conspiracy theories made Alex Jones very rich. They may bring him down', *The New York Times*, 7 September 2018, URL: https://www.nytimes.com/2018/09/07/us/politics/alex-jones-business-infowars-conspiracy.html, accessed: 10 June 2021.
25. A. Haijtema, 'Als bijbelse onheilsprofeten verkondigen talkshowhosts Jones en Jensen hun waarheid', *de Volkskrant*, 3 July 2020, URL: https://www.volkskrant.nl/foto/als-bijbelse-onheilsprofeten-verkondigen-talkshowhosts-jones-en-jensen-hun-waarheid~be450022/, accessed: 11 June 2021.
26. These technologies also cause major problems for the judicial system, because they challenge the credibility of video images and audio recordings as evidence.

This could cause citizens to distrust all news sources, including the most reliable ones.[27] Even more so when politicians attempt to use these forms of information pollution to their advantage (more on this later). This can only harm the functioning of journalism as democracy's informal fourth power. We can already see it suffering the consequences of this. For example, the sources behind disinformation regularly label the traditional media as fake news. This creates distrust within society and even aggressive behaviour towards traditional media channels.[28]

The misleading nature of disinformation means that liberals consider it a significant threat to individual autonomy. When facts are deliberately distorted and lies are spread, individuals no longer have an objective basis upon which to form opinions. This involves indirect external influence, because attempts are being made to manipulate these individuals. We can say here, in line with the freedom of expression, that the individual's 'freedom to hold opinions without interference' is at stake. In addition, disinformation also poses a legitimate security threat to the government, to journalism and to society as a whole. The inflammatory nature of disinformation can lead to acts of violence. Above all, disinformation is harmful to democracy because it undermines rational-critical debate in society. This debate needs be grounded in fact-based opinion. When facts themselves are considered mere opinions, the foundation of public debate is lost. Citizens can no longer enter into rational-critical debate with each other because they are no longer grounded in the same 'reality'. This leads to the erosion of democracy and growing polarisation within society. A sort of hyper-democracy is slowly emerging, in which citizens only want to have their own feelings of being in the right confirmed to them.

Therefore, it is extremely important for citizens to learn to arm themselves better against disinformation. Vulnerable groups in particular, including the less educated, as well as children and the elderly, need to increase their digital and media savviness. Citizens need to be made aware of issues such as disinformation and information tunnels, to improve their ability to identify misleading reports. Currently, various

27. Boheemen, *Digitale dreigingen voor de democratie*, p. 75.
28. Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Dreigingsbeeld Terrorisme Nederland 54*, p. 30.

measures are being taken both at European and national level regarding media literacy, including organising information campaigns.[29] We recommend continued investment in these types of initiatives. Liberals also want to ensure that pupils develop critical thinking skills as part of their education. It is important for media savviness to become part of the curriculum, to teach people how to apply this in the digital world. This allows individuals to behave more responsibly. Nonetheless, the effectiveness of this will always be limited because disinformation is going to become increasingly difficult to identify. There are limits to what can reasonably be expected of an average citizen in this regard. Therefore, awareness and training alone will not suffice. The principal measures against disinformation need to be taken by the channels through which it is disseminated, i.e. social media platforms.

4.3 The role of social media platforms in democracy

In early 2021, Twitter decided to suspend former US President Donald Trump from its platform. The suspension was initially temporary but then became a permanent ban. They found him guilty of inciting the mob that had stormed the American parliament building shortly before that. This was a hard blow for Trump, whose frequent use of the platform had led to his time in power being dubbed the 'Twitter Presidency'. Indeed, he lost his most important mouthpiece. That same year, Facebook also suspended him for a minimum of two years.[30] Even before his suspensions, these platforms had started to add *fact-checking* warnings on any of his posts containing disinformation. Not only in the United States but also in Europe, social media platforms can be seen to have taken on a more active role upon themselves in democracy. For example, they can label political '*tweets*' as misleading.[31]

---

29. European Commission, 'Media literacy', URL: https://digital-strategy.ec.europa.eu/en/policies/media-literacy, accessed: 17 July 2023.
30. 'Facebook suspends Trumps accounts for two years', *BBC News*, 5 June 2021, URL: https://www.bbc.com/news/world-us-canada-57365628, accessed: 12 July 2021.
31. B. Vroegop, 'Twitter noemt tweet van Baudet misleidend, dit zijn de gevolgen', *Algemeen Dagblad*, 9 March 2021, URL: https://www.ad.nl/tech/twitter-noemt-tweet-van-baudet-misleidend-dit-zijn-de-gevolgen~aa9bb784/, accessed: 12 July 2021.

Social media companies have gained huge political power as news and discussion platforms, in addition to their economic power. As such, they have started to play a key role in democracy and have become critical to public debate. With this power, comes responsibility. However, we have to ask ourselves whether these social media platforms are adequately fulfilling this responsibility. What measures have these companies taken and are they justifiable from a liberal point of view?

Most social media platforms have taken action on disinformation. For example, they try to detect misleading information, delete fake accounts, and work together with fact-checking-organisations. In doing so, these platforms are actually trying to make up for their lack of a verifying editorial team, the kind found in traditional media. Companies including Facebook and Twitter have signed up to a special EU code of conduct outlining these goals.[32] Sharing disinformation can result in suspensions. Besides Trump, conspiracy entrepreneur Alex Jones of the InfoWars channel was also removed for spreading disinformation and conspiracy theories.

Liberals maintain that democratic debate must be grounded in fact. If basic facts including hard figures are ignored, there is no point in having a discussion at all. The legitimacy of an argument is then immediately dismissed from the start, as people refuse to acknowledge the information and facts upon which it is based. However, facts cannot be dismissed as mere personal beliefs on an equal footing with other kinds of other unscientific 'alternative facts'. The scientific method must always prevail in debate. At the same time, liberals want to allow maximum space for free debate without censorship. The question then becomes how to strike a balance between countering disinformation on the one hand and guaranteeing freedom of expression on the other.

When it comes to fact-checking, social media platforms have three different policy options: i) no fact-checking at all: this ensures maximum freedom of expression, but results in the unimpeded dissemination of disinformation, ii) fact-checking and the labelling of disinformation as such: this is a compromise between freedom of expression on the one hand and countering disinformation on the other, iii) fact-checking and

32. European Commission, *EU-brede praktijkcode betreffende desinformatie*, Brussels, 2018, pp. 3-4.

the removal of disinformation and the channels behind it: this results in the maximum suppression of disinformation, but the likelihood of censorship is high when cases that are inconclusive are also removed and people no longer feel safe to express themselves on certain topics, out of fear that their channel or account will be removed. The second of these three options – fact-checking and labelling – seems to be the most balanced choice. In principle, anyone can continue to say anything, while also being aware that messages containing disinformation may be labelled with a disclaimer by a fact-checking organisation. Removal from the platform is then restricted to the most extreme cases only, such as bot accounts that consistently and deliberately spread disinformation.

An important follow-up question to ask then is: what should this fact-checking entail? There would be a clear conflict of interest were social media platforms to do this themselves, as these companies are driven by certain commercial interests that could compromise their position as a neutral party in the matter. A government organisation should not take on this responsibility either, because the state should not meddle in public debate. One potential solution is for independent third parties to act as legitimate fact-checkers. It would be advisable to involve a mix of different organisations to prevent a single organisation becoming the 'designated arbiter of truth'. This would enable individuals to choose between different fact-checkers when using social media platforms, for example. These types of solutions are already being experimented with.[33] Although fact-checking would probably not solve all disinformation issues, it could be a significant step in the right direction, enabling individuals to recognise disinformation more easily and make their own choices on that basis.

It should also be noted that, formulating a single, unequivocal liberal stance on the matter would be difficult, as there would be inevitable differences of opinion within the liberal spectrum. The question of where to draw the line changes depending on which liberal principles are prioritised. For example, some liberals will argue for maximum freedom of expression and categorise any form of fact-checking as unwanted censorship. This will clearly always involve compromise, and

33. Fact Check Tools, 'About', URL: https://toolbox.google.com/factcheck/about, accessed: 3 May 2022.

there's no ideal solution available that will be completely immune to scrutiny.

Besides disinformation, social media platforms are also looking to combat hate speech. To this end, Facebook, Twitter, Microsoft and YouTube signed up to an EU code of conduct, in 2016. The 2020 annual compliance report claimed that some 90 percent of all reports of illegal hate speech were addressed within 24 hours, and 71 percent of these messages were deleted.[34] Companies are therefore increasingly taking measures in this area, for example, by prohibiting offensive images.

The liberal view on these types of measures, however, is unequivocal. Liberals believe that it is important for opinions to be heard, unless, of course, they are to the obvious detriment of others. For example, in cases of incitement to violence, libel or slander. However, liberals don't have a problem with controversial opinions being expressed. This basic principle can be compromised when the concept of 'hate speech' is interpreted too broadly. Many incidences of hate speech are clearcut, but others fall into a grey area. Whether the situational context of something should be interpreted as hateful then becomes a matter of personal opinion. Someone who posts an offensive photo may not necessarily have bad intentions. For example, when showing historical footage. Liberals argue that caution is required in this area. After all, it's a slippery slope and it affects people's right to freedom of expression.

The difference between fact and opinion is therefore crucial. By way of illustration, the percentage of women on the boards of listed companies in the Netherlands is still many times lower than the percentage of men.[35] This is an indisputable fact. In the view of some liberals, social media platforms should have independent fact-checkers check whether the facts that are being presented are correct. The ideal policy (whether it be the preferred policy or not), therefore, becomes a matter for debate. This is a subjective matter in which everyone has the right to form and

34. European Commission, *Countering Illegal Hate Speech Online. 5th Evaluation of the Code of Conduct*, Brussels, 2020, p. 1.

35. OR Rendement, 'OR kan groei aantal vrouwen in bedrijfstop stimuleren', *Rendement Online*, 6 September 2021, URL: https://www.rendement.nl/discriminatie/nieuws/or-kan-groei-aantal-vrouwen-in-bedrijfstop-stimuleren.html#:~:text=Tussen%202018%20en%202020%20steeg,uit%200p%2013%2C6%25., accessed: 3 May 2022.

express an opinion, however controversial it may be. These platforms should be reluctant to intervene in cases like this because it would amount to censorship and restrictions on the freedom of expression.

The measures taken by these companies all stem from policies of self-regulation. The key issue here is whether it's ideal for these social media platforms to take the initiative in how they steer democratic debate. Given the pivotal role they have in politics, should they not be accountable to the government, which can then introduce legislation? After all, in many countries, the traditional media is regulated by media law. Before answering this question, we need first to determine what type of legal entity these tech companies are. Here, we see already that they try to find smart ways to use national legislation to their advantage in different countries. For example, in the United States they classify themselves as internet intermediaries according to Section 230 of the *Communications Decency Act*, under which they are not responsible for what users post on their platform.[36] This means they are able to avoid certain regulations that apply to newspapers, for example.

When we look at what exactly these companies do, it becomes clear that they are not just neutral distributors of information, in the way that telecom companies facilitate phone calls, for example. They play a very important and active role in the way information is shared and whom it is shared with. Under the *Digital Services Act* (2022), the EU classifies them as 'very large online platforms', to which specific rules apply regarding the distribution of illegal content and causing harm to society.[37] This ought to result in greater democratic control and regulation of these platforms and address the risks of manipulation and disinformation.[38] Government regulation is needed here, given that self-regulation

36. 'Advertiser boycott Facebook: The great responsibility of social media platforms', *University of Utrecht*, 3 July 2021, URL: https://www.uu.nl/en/news/advertiser-boycott-facebook-the-great-responsibility-of-social-media-platforms, accessed: 13 July 2021.
37. 'Very large online platforms' are platforms that reach more than ten percent of European citizens (45 million users).
38. European Commission, 'Wet inzake digitale diensten: Zorgen voor meer veiligheid en verantwoordingsplicht online', URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_nl#welke-providers-vallen-hieronder, accessed: 13 July 2021.

by these companies has proved inadequate to date. This public sentiment appeared evident, for example, during a 2020 Facebook boycott by more than 1,000 different advertisers under the slogan "*stop hate for profit*", including large corporations such as Adidas, Coca Cola and Volkswagen.

Where these tech companies mostly fall short is in the level of accountability that is required when it comes to their algorithms. As we saw earlier, the revenue model these companies operate under is aimed at retaining user attention for as long as possible, by showing increasingly extreme forms of content. These recommendation algorithms thus create information tunnels and cause political polarisation and radicalisation (see section 4.2). The importance of these recommendation algorithms to these corporations is illustrated in the fact that some 70 percent of all YouTube videos are viewed on this basis.[39] These algorithms are the reason for the economic success of these corporations, as they allow so many more targeted ads to be shown. At the same time, they have a negative effect on democracy. For example, one researcher showed how, after joining a Facebook group opposing Covid-19 measures, the algorithm recommended he also join a group focused on the QAnon conspiracy theory.[40]

These information tunnels not only reinforce the effects of disinformation, but also pose a threat to public debate in general. Citizens are less exposed to different opinions and their ideas are left unchallenged as a result. Instead, they always have their own prejudices confirmed and this reinforces social polarisation.[41] For liberals, citizenship involves interacting with people with differing opinions, because this exchange of ideas ensures that people do not get stuck in dogmatic thought. Algorithms disrupt this sort of public debate within a democracy. To avoid ending up in a hyper-democracy, in which citizens only engage with others who think like them, something needs to be done about these algorithms.

---

39. S. Lewandowsky et al., *Technology and Democracy. Understanding the Influence of Online Technologies on Political Behaviour and Decision-Making*, Joint Research Centre – European Commission report, Brussels, 2020, p. 27.
40. J. Carrie Wong, 'Down the rabbit hole: how QAnon conspiracies thrive on Facebook', *The Guardian*, 25 June 2020, URL: https://www.theguardian.com/technology/2020/jun/25/qanon-facebook-conspiracy-theories-algorithm, accessed: 13 July 2021.
41. Carnegie Council of Ethics in International Affairs, 'Cass R. Sunstein: #Republic: Divided democracy in the age of social media', *YouTube*, 8 May 2017, URL: https://www.youtube.com/watch?v=_Uv-IJXVm3c, accessed: 20 December 2021.

Self-regulation inevitably falls short here, because society's best interest of maintaining a healthy democratic process where this topic is concerned, conflicts with the financial interests of these companies. In 2020, Facebook introduced a 'news credibility'-update, in which the algorithm prioritises news from primary sources that are transparent about their authorship in users' newsfeeds.[42] While steps like these are to be encouraged, they still involve self-regulation which means that transparency is lacking. It is unclear how these algorithms work exactly, and regulators are not currently authorised to monitor them. Tech companies view their algorithms as trade secrets that they prefer not to disclose to other parties for no reason. When we look at social media platforms, we may legitimately question how desirable it is for our democracy and public discourse to be at the mercy of this sort of technology.

Regulation could provide more transparency. For example, regulators and independent researchers could be appointed to monitor algorithms. Simple access to the blueprints of these algorithms would provide important insight.[43] Were an algorithm to be shown to be detrimental to society, a decision could be made whether to possibly prohibit it. This could force social media platforms to come up with alternatives that are not harmful. From a liberal perspective, these sorts of regulations are justifiable because they protect democracy and promote individual autonomy. These platforms can thereby be held accountable and we would be able to ensure they kept a neutral stance in their role as facilitators in the online public debate.

4.4 Profiling and politics

In democracy, political parties need to get their message across to their desired target groups in the right way. People have been thinking about how best to do this for decades. For a long time in Europe, parties were

42. C. Brown, 'Prioritizing original news reporting on Facebook', *Facebook*, 30 June 2020, URL: https://about.fb.com/news/2020/06/prioritizing-original-news-reporting-on-facebook/, accessed: 21 June 2021.
43. U. Reisach, 'The responsibility of social media in times of societal and political manipulation', *European Journal of Operational Research*, 2020, no. 291, p. 914.

quite clear about their supporters and who their attention should be aimed at. The political landscape was mostly made up of large traditional parties like the Liberals, Christian Democrats and Social Democrats. Nowadays, politics is much more fragmented in many countries. Over the last 30 years in Europe, some 800 new political parties have emerged.[44] Party loyalty has diminished and many voters only decide who to vote for just before elections. Effective campaigning is therefore of immense importance to political parties, because election results are far from certain prior to the voting.

Digitalisation plays an increasingly crucial role here. In fact, during the Covid-19 pandemic, election campaigning could not easily take place in the traditional way, if at all. Large gatherings were forbidden and *lockdown-* measures also made it harder to hand out flyers in shopping streets. But politicians could use the digital route to get in touch with voters. Political parties became particularly active on social media as a result. But even before the Covid-19 crisis, it was clear that data-driven campaigns with effective social media strategies could prove decisive in determining election results.

Social media is a good way of reaching younger voters, although more and more older people are also on these platforms nowadays.[45] An advantage of social media for politicians is that they can engage with voters directly without needing the traditional media as an intermediary. This can include posting online, as well as *live streams* in which viewers can ask questions. Some parties have their own talk shows or newscasts.[46] As discussed in the previous section, journalism loses its gatekeeper function when it comes to verifying the truth behind certain statements, for example. Journalists do not always get the opportunity to ask critical questions either. The spread of disinformation by politicians is therefore

44. H.T. Hung, 'Fragmentation of the European party system: new dimensions of electoral competition', *European Student Think Tank*, 24 January 2023, URL: https://esthinktank.com/2023/01/24/fragmentation-of-the-european-party-system-new-dimensions-of-electoral-competition/, accessed: 17 July 2023.

45. Centraal Bureau voor de Statistiek, 'Steeds meer ouderen maken gebruik van sociale media', 20 January 2021, URL: https://www.cbs.nl/nl-nl/nieuws/2020/04/steeds-meer-ouderen-maken-gebruik-van-sociale-media, accessed: 23 June 2021.

46. Forum voor Democratie, 'FVD Journaal', *YouTube*, URL: https://www.youtube.com/playlist?list=PLi7orMmZGePv6uftti2QsIhpyYEdiFwtw, accessed: 23 June 2021.

a serious concern.[47] Political parties also try to influence public opinion in other questionable ways. These include, for example, fake Facebook and Twitter accounts used to attack opponents.[48]

In the previous chapter we saw how users are profiled though the analysis of their behavioural data. In the context of the surveillance economy, profiling is used to attribute certain characteristics to individuals to determine their particular product preference. But it is not only market parties who are interested in determining the characteristics of individuals. Behavioural predictions and influencing tactics are also proving extremely interesting for political actors. Individual political sentiments can be revealed in much the same way as preferences for particular products are established. Although this involves special personal data that cannot be requested directly under the GDPR, this can often be derived relatively easily nonetheless, as long as there are enough relevant data points available. For example, a simple '*like*' on a Facebook post about a book on the importance of the nation state, or another on the harmful effects of the bio-industry, indicates a statistical probability of a particular political leaning.[49]

The extent to which this can escalate has been demonstrated in various countries. For example, there are companies that get hired by political parties to collect and analyse voter data, which is then used to approach voters with personalised political messages. This was the case with the scandal involving political consultancy firm Cambridge Analytica, which came to light in the United States in 2018.

Political profiling by Cambridge Analytica

Cambridge Analytica was set up as a company in 2013, as a subsidiary of the SCL Group. The latter had been active since the 1990s and was specialised in psychological warfare. The company was active in this

47. R. Bouma, 'Politici plaatsen steeds vaker desinformatie op sociale media', *NOS*, 3 October 2019, URL: https://nos.nl/nieuwsuur/artikel/2304514-politici-plaatsen-steeds-vaker-desinformatie-op-sociale-media, accessed: 24 June 2021.

48. 'DENK gebruikt nepaccounts op social media', *Algemeen Dagblad*, 10 February 2017, URL: https://www.ad.nl/binnenland/denk-gebruikt-nepaccounts-op-social-media~a7d819e0/, accessed: 23 June 2021.

49. Of course, this is a generalisation but the more data points of this sort are available, the better the estimate of an individual's political preferences can be made.

area during the Afghan and Iraq wars. It was also involved in various elections campaigns, particularly in developing countries. Cambridge Analytica was founded as a subsidiary in the USA, first assisting Ted Cruz, a Republican candidate in the presidential primaries, and later the Republican presidential candidate, Donald Trump, during the 2016 US presidential elections. The company profiled American voters, looking in particular at their psychological characteristics, which were used when approaching them on social media with political advertisements and other politically charged messages. Particular attention was paid to floating voters, who were susceptible to this type of communications. Political advertisements were carefully tailored on the basis of voter profiles. These were drawn up based on the many data points collected by the company. For example, the company claimed to have more than 5,000 data points per person from more than 230 million Americans. Following a data breach, it would transpire that this data contained a lot of illegally obtained personal data, much of it from Facebook. After the scandal broke in 2018, Cambridge Analytica (and the SCL Group) filed for bankruptcy. Facebook also had to answer to the American Congress on this matter.

The Cambridge Analytica scandal made it very clear political profiling can go to extreme lengths with the current technology. In 2016, Alexander Nix, CEO of the company, gave a presentation in which he explained how they went about this. Voters were profiled according to five broad personality traits, among other things.[50] On this basis, a political advertisement – one, for example, promoting the right to own a gun – was personalised for these voters. People with a tendency to be anxious or fearful by nature were shown an advertisement featuring a burglar, emphasising the importance of weapons in self-defence. People who valued tradition were shown an advertisement applauding gun ownership, drawing on the sport of hunting, as an American tradition to be passed down from one generation to the next.[51] In doing so, the

50. I.e. emotional stability, extraversion openness, conscientiousness and friendliness.
51. Concordia, 'Cambridge Analytica – the power of big data and psychographics', *YouTube*, 27 September 2016, URL: https://www.youtube.com/watch?v=n8Dd5aVXLCc, accessed: 24 June 2021.

company sought to respond in a very deliberate way to the particular sensitivities of certain individuals, and these often included negative feelings like fear or anger. What was particularly concerning was that the company had collected data from more than 87 million Facebook users without their consent.[52]

There are concerns about political parties' use of profiling in Europe too. Although, European legislation is generally stricter than in the United States, political profiling is becoming increasingly common here too. There are clear distinctions between different countries. In France, for example, there are already very strict rules when it comes to political advertising, which makes it hard for political parties to profile their voters. At the other end of the spectrum, in a country like the Netherlands, there are hardly any restrictions on political advertising at the current time.[53] One example we saw was a political party that used political profiling during the Dutch 2018 local elections, in which voters with a Moroccan background were shown an advertisement featuring a council official wearing a headscarf, while this was not shown to members of, for example, the LGBTQ+ community.[54] These groups were defined by looking at things like their GPS data and the type of phone subscription they had (calling abroad is cheaper with certain providers). In the United Kingdom, political advertisements on television, radio and in newspapers are regulated, but online advertisements are not. This allowed political profiling to play a major role there during the 2016 Brexit referendum, especially in the '*Vote Leave*' camp. This was also widely used in the 2019 general election, where Brexit once again played a key role.[55]

A positive aspect of political profiling is that it allows people who are hard to reach in traditional ways to be reached digitally. A greater

52. H. Kozlowska, 'The Cambridge Analytica scandal affected nearly 40 million more people than we thought', *Quartz,* 4 April 2018, URL: https://qz.com/1245049/the-cambridge-analytica-scandal-affected-87-million-people-facebook-says/, accessed: 22 July 2021.

53. T. Dobber, R.Ó. Fathaigh, F.J. Zuiderveen Borgesius, 'The regulation of online political micro-targeting in Europe', *Internet Policy Review*, 2019, no. 8, p. 4.

54. D. Davidson, R. Delhaas, 'Als de politiek in iedere oor een andere boodschap fluistert', *Argos*, 22 April 2020, URL: https://www.vpro.nl/argos/lees/nieuws/2020/microtargeting-in-Nederland.html, accessed: 25 June 2021.

55. K. Ryabtsev, 'Political micro-targeting in Europe: a panacea for the citizen's political misinformation or the new evil for voting rights', *Groningen Journal of International Law*, 2020, no. 1, p. 76.

number of citizens become engaged in the democratic process as a result. Added to that, new, smaller parties that don't tend to get much attention from traditional media are able to get their message across. This benefits a pluralist democracy. Although these things can be seen as positive from a liberal perspective, the various elements mentioned above provide cause for concern with regard to several liberal values. They allow political parties to compromise both the privacy and the autonomy of the individual, in a similar way to what we saw with market parties in the surveillance economy. The data that interests political parties is often sensitive in nature, such as religion, ethnicity or political party membership. The situation with regard to data collection does not currently seem to be too bad in Europe, although there is undoubtedly an incentive to collect as much voter data as possible during election campaigns and to push at the boundaries of privacy legislation.

From the voter point of view, there is also the issue of whether it is desirable for parties to be able to personalise their political messages on the basis of people's individual personal characteristics. At its core, politics is about balancing the interests of society as a whole. If messages are continually adapted to individual characteristics, it becomes hard to assess whether parties are consistent and honest in the ideas they put across to voters. It also enhances the ability for parties to withdraw from public democratic debate. For example, if a strong social media campaign is enough to win a lot of votes, taking part in a television debate with other parties starts to seem more and more like an unnecessary risk. Once again, this circumvents journalism by preventing it from exercising its role as a gatekeeper. A democracy in which each party tries to shape its own version of political 'reality' online creates an information tunnel effect, making it challenging for voters to form autonomous opinions because they only get to see a part of the whole picture.

And yet, a total ban on profiling and political advertising does not seem like a good idea either. As previously mentioned, there is nothing new about wanting to target particular groups of voters. Moreover, most political debate is undeniably taking place online. Young people in particular make less and less use of traditional media, such as radio and television. It is therefore understandable that political parties want to reach out to voters online. For political engagement purposes,

is important for individuals to be involved in the democratic process through as many channels as possible. But individual privacy and autonomy must be properly safeguarded. There is therefore a need to establish clear pre-conditions.

In the Netherlands, a government advisory body has made a number of good recommendations in this area: i) political parties should have Transparency obligations with regard to their use of digital tools, ii) platforms and websites should be obliged to label political advertisements as such and to state who funded them, iii) there should be a legal limit on the percentage of political advertisements that are shown in a targeted way, and iv) there should be an independent regulator to oversee these transparency requirements, with the authority to impose appropriate sanctions.[56] Such measures would break open the current confidentiality policies surrounding the digital campaign strategies many political parties use. Greater transparency (and regulation thereof) would strengthen the information position of individuals and counteract manipulation. This would give people a better overview of the parties that are targeting them and how they are going about it. When it comes to these transparency requirements, besides political parties, it would also be necessary to strictly monitor the compliance of the third (market) parties they are partnered with, i.e. campaign marketing agencies.

4.5 Foreign political interference

In recent years, geopolitical tensions have increased between the West and countries like Russia (especially after the 2022 invasion of Ukraine), Iran and China. Political interference has become a popular means for some countries to influence, polarise and destabilise other countries. The open nature of democracy makes it particularly vulnerable to this. Digitalisation offers new and difficult-to-trace possibilities for running influence campaigns, and politicians and citizens are suffering the consequences of this. In the physical world, foreign political interference occurs through things like the covert financing of political parties or

56. Staatscommissie parlementair stelsel, *Lage drempels, hoge dijken. Democratie en rechtsstaat in balans,* The Hague, 2018, pp. 245-246.

by addressing citizens personally . In the digital domain, it is mainly about the spread of disinformation. But hacking is also an issue.[57] This can involve stealing and leaking secret documents. State actors are often behind this, although sometimes non-state actors – usually employed by a foreign government – try to influence the democratic process. These influencing operations are part of what the security domain has dubbed 'hybrid threats'.[58] Traditionally, the threat posed by enemy states was primarily military. Nowadays, other means are increasingly being used in geopolitical struggles, including campaigns for online political influence.[59] This is known as covert political influence, which is when states aggressively seek to bolster their political interests abroad while trying to keep their activities under wraps.[60]

Where strategies like the threat of military intervention or sanctions are aimed at enforcing particular behaviour, political interference is about using ideas to influence the population. So it less about changing behaviour, than it is about changing or strengthening the beliefs behind it.[61] It is a form of manipulation geared at upending political opinions or simply creating chaos and divisiveness by tapping into the polarising issues at play within a country.[62] The digital world lends itself well to this, because – as we saw earlier – it is easy to select and approach particular target groups. It is also a relatively easy and safe 'geopolitical weapon' to deploy as it does not cause direct physical harm and it is also difficult to trace back to the perpetrator.

Russia in particular, has often attempted to interfere in the politics of other countries through online political influencing campaigns like this.

---

57. B. Pijpers, *Influence Operations in Cyberspace: on the Applicability of Public International Law during Influence Operations in a Situation below the Threshold of the Use of Force*, University of Amsterdam thesis, Breda, 2022, pp. 224-228.
58. Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Χίμαιρα. Een duiding van het fenomeen 'hybride dreiging'*, The Hague, 2019, pp. 9-14.
59. F. Bekkers, T. Sweijs, R. de Wijk, *Hybride dreigingen en hybride oorlog: consequenties voor de Koninklijke Landmacht*, The Hague Centre for Strategic Studies report, The Hague, 2020, p. 10.
60. Algemene Inlichtingen- en Veiligheidsdienst, *AIVD jaarverslag 2020*, The Hague, 2021, p. 10.
61. P. Ducheine, B. Pijpers, *Influence operations in cyberspace. How they really work*, Amsterdam Law School research paper, Amsterdam, 2020, pp. 7-9.
62. A.J.H. Bouwmeester, *'Krym Nash': an Analysis of Modern Russian Deception Warfare*, University of Utrecht thesis, Utrecht, 2020, p. 283.

For example, it was proven that during the 2016 US presidential elections, Russia made active use of numerous fake accounts and disinformation to try to influence American citizens on social media.[63] This worked in favour of the Trump campaign, while the Democratic candidate Hillary Clinton was smeared. As well as pumping out large amounts of disinformation, Russian intelligence also hacked employees and organisations associated with the Clinton campaign. Damaging emails and documents were stolen and leaked to WikiLeaks.[64]

The Russian Internet Research Agency (IRA) deserves a special mention here. It is what is known as a 'troll factory' – a 'troll' being a deliberately antagonistic internet user – and is based in Saint Petersburg where the Russian government commissions them to carry out all kinds of influencing activities on the internet to promote Russian political interests. In particular, Russia tries to sow division within countries by stirring up polarising topics. In the United States, for example, it stoked the fire of racial tensions in response to the Black-Lives-Matter(BLM) movement and police violence. Russian trolls sought to popularise racial themes on social media while simultaneously spreading disinformation. They also used Facebook to organise both pro- and anti-BLM protests in the country.[65]

The Russian government does not target the United States exclusively. It also targets Europe. For example, during the 2019 European Parliamentary elections, Russia spread disinformation to influence the outcome.[66] The EU has also warned that Russia is trying to feed anti-European, populist and far-right sentiment in individual member states.[67]

---

63. U.S. Department of Justice, *Report on the Investigation into Russian Interference in the 2016 Presidential Election,* Washington D.C., 2019, p. 14.
64. Ibidem, p. 36.
65. D. Seetharaman, 'Russian-backed Facebook accounts staged events around divisive issues', *The Wall Street Journal*, 30 October 2017, URL: https://www.wsj.com/articles/russian-backed-facebook-accounts-organized-events-on-all-sides-of-polarizing-issues-1509355801, accessed: 1 July 2021.
66. 'EU: We have proof of Russia election meddling', *DW*, 14 June 2019, URL: https://www.dw.com/en/eu-russia-spread-disinformation-ahead-of-eu-elections/a-49210802, accessed: 19 July 2019.
67. Europees Parlement, 'EU moet optreden tegen buitenlandse inmenging in verkiezingen en desinformatie', 10 October 2019, URL: https://www.europarl.europa.eu/news/nl/press-room/20191007IPR63550/eu-moet-optreden-tegen-buitenlandse-inmenging-in-verkiezingen-en-desinformatie, accessed: 1 July 2021.

During the 2017 French presidential elections, the Russians spread large amounts of disinformation in favour of the EU-sceptic candidate Marine Le Pen, while the team of the eventual winner, Emmanuel Macron, was hacked.[68] Additionally, Russia also tries to cause discord by supporting separatist organisations. For example, in Spain, attempts were made to strengthen the Catalan independence movement through social media.[69] Therefore, Moscow appears to want to sow division at European, national and regional levels and believes that it can gain geopolitical advantage through its divide-and-conquer strategy. More recently, Russia has also tried to undermine European support for Ukraine in the Ukraine war. For example, it attempted to influence the Slovakian elections in the hope that a new government would stop supporting the Ukrainian side.[70] Russia is not the only state to try to interfere in European politics in this way. During the Covid-19 crisis, China also tried to sow confusion about the origins of the virus, fuelling criticism about the European handling of the pandemic.[71]

It is important for liberals to realise that democracy is particularly susceptible to foreign influences. The open and free nature of our political system provides more opportunities for this than authoritarian regimes that exercise strict controls over information flows within their countries. Liberalism is based on international politics in which *realpolitik* (power politics) is still very much present.[72] It should come as no surprise that rival or hostile states would want to attempt to weaken our country like this. But it's a major act of provocation. From a liberal perspective,

---

68. 'Russian hackers 'target' presidential candidate Macron', *BBC News*, 25 April 2017, URL: https://www.bbc.com/news/technology-39705062, accessed: 19 July 2023; A. Rettman, 'Russia-linked fake news floods French social media', *EUobserver*, 20 April 2017, URL: https://euobserver.com/world/137624, accessed: 19 July 2023.
69. R. Emmott, 'Spain sees Russian interference in Catalonia separatist vote', *Reuters*, 13 November 2017, URL: https://www.reuters.com/article/us-spain-politics-catalonia-russia-idUSKBN1DD20Y, accessed: 1 July 2021.
70. L. Bayer, 'Slovakia risks succumbing to Russian disinformation, president warns', *Politico*, 3 June 2023, URL: https://www.politico.eu/article/eu-risks-losing-slovakia-russia-disinformation-president-zuzana-caputova/, accessed 19 July 2023.
71. Algemene Inlichtingen- en Veiligheidsdienst, *AIVD jaarverslag 2020*, The Hague, 2021, p. 10.
72. H. ten Broeke, *10 vuistregels voor een realistisch buitenlands beleid,* political-scientific position III by Prof.mr. B.M. TeldersStichting, The Hague, 2016, pp. 7-9.

it is highly undesirable for our autonomy to be affected like this. The manipulative nature of foreign political influence is detrimental to the self-determination of citizens. Deliberate attempts are made to disrupt rational-critical debate within the democratic process and to fuel the polarisation within countries to the extent that it gives rise to security threats.

These hostile regimes are in fact trying to use the freedoms of the democratic system against democracy itself. Democracy is undermined by this corruption of open, public debate. Knowing that democracies are reluctant to ban political expression on account of freedom of expression, contradictions are fuelled with the aim of turning people against each other and letting emotion get the upper hand. Countries like Russia and China are trying to present democracy as a failing, outdated and unstable system, both in the eyes of their own peoples and in those of the rest of the world. They propagate an alternative political system in the form of authoritarianism. It is important for the stability of Western democracies to demonstrate that democracy can indeed defend itself against these forces, both for their own sake and to prevent other countries from following down the path of authoritarianism. Liberals stand for a resilient democracy. This means that liberals believe it is necessary to take action when the democratic process is sabotaged by foreign governments.

The security aspects of this issue mean that our intelligence and security services have an important role to play here. They must be given the authority and the means to identify and combat influence campaigns from enemy states. Private actors and knowledge institutes can also play a part here. The exchange of information on these matters between the various Western democracies is essential too. These countries must take joint action by openly criticising hostile states and weighing up the imposition of economic sanctions. For example, the EU recently came up with a Cyber Diplomacy Toolbox for imposing sanctions at EU level.[73]

73. Council of the European Union, 'EU imposes first ever sanctions against cyber-attacks', 30 July 2020, URL: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/, accessed: 29 September 2021.

Sweden is an interesting country to look at as an example. In the run-up to their 2018 parliamentary elections, Sweden formulated a multidisciplinary approach to arm itself with against foreign influence campaigns from Moscow. National and local level politicians were given training in recognising disinformation and not letting it influence them. The major media channels also worked together to combat disinformation. A coalition of students, international journalists and fact-checkers, was also set up to detect disinformation and alert news organisations on a daily basis. Additionally, a digital literacy education programme that already existed in schools was rolled out across society as a whole. These combined measures proved very successful in combatting Russian attempts at interference.[74]

The author Mikael Wigell also advocates for a society-wide approach, and for the active involvement of civil society, in particular. This would include non-governmental organisations and political think tanks. He also argues in favour of fostering civil activism. He believes that citizens should keep a watchful eye and alert the authorities whenever they suspect foreign political interference.[75] We previously looked at imposing transparency requirements around the funding of online political advertisements. This could also help identify foreign interference. A searchable ads library, like the one created by Facebook, is very practical for this. The legislation proposed to tech companies to counter disinformation and information tunnels is also crucial if the effects of political interference are to be contained.

When it comes to elections, some countries still vote with a pen or pencil in the traditional way, while others have adopted digital systems. The Netherlands is an interesting country in this regard. So-called 'voting computers' were previously used there, but from 2007 onwards, pencils were reintroduced after a study showed that the digital system was not sufficiently secure.[76] This is why all forms of digital voting are

74. M.L. Taylor, 'Combating disinformation and foreign interference in democracies: Lessons from Europe', *Brookings*, 31 July 2019, URL: https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/, accessed: 2 July 2021.

75. M. Wigell, 'Democratic deterrence: how to dissuade hybrid interference', *The Washington Quarterly*, 2021, no. 1, pp. 52-55.

76. W.J. Derksen, 'Digitaal stemmen versus het rode potlood', *Liberaal Journaal*, publication by Prof.mr. B.M. TeldersStichting, The Hague, 2020, p. 11.

best avoided in major elections, even now that the technology is more advanced than it used to be. After all, even the illusion of tampering can be enough to undermine an election result. Imagine a manipulated photo of a voting machine, made to look as if a USB stick that should not be there has been plugged into it. Furthermore, voting computers usually mean that manual recounts are not possible. In light of recent cases of foreign political interference, digital voting simply creates unnecessary risks.

Democracy does not have to limit itself to being defensive in matters of foreign political interference. We have already discussed the use of economic sanctions. Some countries have also undertaken preventive cyber attacks, working outside their own networks to neutralise certain cyber capacities of their opponents at an early stage (this is known as 'persistent engagement 'in military circles).[77] For example, in 2018, the United States undertook a cyber attack on the Russian IRA to disrupt their disinformation campaign targeting the US Congressional elections.[78] Nonetheless, such cyber attacks are controversial from a liberal point of view, as they undermine the international legal order. In any case, it would not be a good idea to retaliate with disinformation. Not only would it be less effective in authoritarian countries, it would also negate the liberal values we stand for in our democracy.[79] It could delegitimise the importance of these values in the eyes of citizens which would be detrimental to our democracy in the long run. It would also undermine liberal democracy as an international standard for other countries to follow.

However, we can shine a light on actual issues in countries such as Russia. A good example of this is the Dutch-based citizen-journalist network Bellingcat, which uses open source research to investigate crimes,

77. B.M.J. Pijpers, M.C.P.J. Smits, 'Persistent engagement: de nieuwe cyberstrategie voor Nederland?', *Militaire Spectator*, 2022, no. 2, pp. 76-77.
78. 'Trump confirms he ordered a cyberattack on a notorious Russian troll farm during the 2018 midterms', *Business Insider*, 13 July 2020, URL: https://www.businessinsider.nl/trump-confirms-us-cyberattack-russia-troll-farm-ira-2020-7?international=true&r=US, accessed: 5 July 2021.
79. D. Broeders, 'Consequences for election interference', *Directions*, 15 May 2020, URL: https://directionsblog.eu/creating-consequences-for-election-interference/, accessed: 3 May 2022.

corruption scandals and other problems in these sorts of countries.[80] We can also support the democratic forces active within these authoritarian countries. In the digital world, these include activist internet bloggers who inform their fellow citizens about their country's issues, often risking their own lives in the process.

4.6 Conclusion

This chapter was dedicated to the effects of digitalisation on democracy. It began by emphasising how significant the problem of disinformation has become. While this is not a new phenomenon, digitalisation has created new ways to produce disinformation. This includes worrisome technologies like *deepfake*. Above all, digitalisation offers new opportunities for spreading disinformation among the population on a mass scale. We are also seeing the emergence of information tunnels, which only reinforce its effect. Conspiracy theories have gained ground in Europe in recent years, resulting in serious safety risks. This also undermines the control function of the traditional media. Citizens therefore need to be made aware of this through increased media literacy. This helps individuals learn to better recognise disinformation and to develop a critical view of the digital world.

But this alone is not enough. Social media has become a major platform within democracy and a defining element in public debate. For this reason, social media companies have begun to take various measures, including fact-checking. Liberals argue that rational-critical discussion is only possible if it is based on facts. At the same time, there also needs to be room for freedom of expression. From a liberal perspective, there are various ways of looking at fact-checking and the need for it. Many supporters, in any case, will believe that fact-checking should first and foremost be restricted to labelling of disinformation, and that it should only be removed in extreme cases. Above all, it is important for fact-checkers to always be independent third parties. Liberals are unanimous when it comes to measures against hate speech on social media platforms, while also arguing for caution to prevent undue restrictions on

80. Wigell, 'Democratic deterrence: how to dissuade hybrid interference', p. 56.

the freedom of expression of citizens. It is also clear that self-regulation by social media companies is not enough. They are not very transparent about how their algorithms operate because transparency would work against their financial interests. Not only do these algorithms reinforce the effects of disinformation, they also form a threat to the liberal ideal of citizenship, in which the individual's beliefs and opinions are challenged by those of other people. Therefore, there is a need for improved regulation in this area, aimed at creating transparency and societal control over the algorithms of Big Tech.

Political parties employ digitalisation for their own purposes. Political campaigns now take place mostly online. This allows politicians and citizens to come into contact with each other directly. However, this is to the detriment of the gatekeeper role of traditional media in democracy. Politicians sometimes also use disinformation as a political weapon. Political profiling is of particular concern. In the USA, Cambridge Analytica showed just how far this can go. In Europe, we can also see how political parties try to target voters in sophisticated ways through personalised political advertisements. This compromises both the privacy and the autonomy of the citizen. Therefore, we also need regulation to impose greater transparency upon political parties. This would give individuals a clear idea of who is approaching them online and why.

The digital world is without national borders and some states have shown that they view foreign political interference as an interesting geopolitical weapon. It is a simple, safe, cheap and difficult-to-trace way of destabilising a society by digital means. The open nature of society in European democracies makes them particularly vulnerable to this. Russia in particular employs this strategy, but so do countries like China. The security aspect means that intelligence and security services have an important role to play in this, although a society-wide approach is needed if our society is to be adequately protected. Countermeasures can also be taken in the form of economic sanctions, as well as support for democratic powers within authoritarian states.

All in all, we have seen that digitalisation poses several significant challenges for democracy, especially with regard to public debate. As previously mentioned, liberals stand for a resilient democracy, in which freedoms must not be misused to the detriment of society's open nature. Liberal values can serve as the starting point for the ongoing

safeguarding of democracy. At a time when countries with less freedoms are employing digitalisation to reinforce their authoritarian regimes, it is particularly important to demonstrate how digitalisation can be used to perpetuate democracy. Clear guidelines drawing upon liberal values can ensure that democracy continues to prove itself to be a well-functioning system that brings peace and prosperity in the 21st century. Not in spite of, but actually because of the new opportunities that digitalisation offers.

5. Government & Citizens

5.1 The digitalisation of central government

Many European countries have embraced digitalisation in recent years. Central governments have followed this digitalisation trend and this has altered the citizen-government relationship. This has had various positive consequences. Digital means allow governments to engage with citizens more easily and *vice versa*. Information flows have become faster and clearer. Furthermore, a lot of unnecessary administrative paperwork is avoided on both sides. For example, in some countries tax returns can be completed online nowadays and citizens only have to check their pre-filled data, instead of looking everything up and filling it in themselves. In several countries, people can easily verify their identity online in order to access all sorts of government services and deal with their affairs digitally, instead of having to visit a government office in person. Things like informing the municipality of a change of residence can be done in just a few clicks.

Governments are also using digitalisation to make public spaces safer and more liveable for the people who use them. For example, sensor data is used to measure river water quality and cameras are installed on the streets to reduce crime. Smart waste bins send out notifications when they need to be emptied and data-driven traffic management reduces congestion. More and more municipalities are conducting 'smart city' experiments. This includes things such as smart lampposts that measure sound and air quality and register mobile phone signals to map movement flows in urban areas.[1]

---

1. S. Naafs, 'De muren hebben sensoren', *De Groene Amsterdammer*, 6 December 2017, URL: https://www.groene.nl/artikel/de-muren-hebben-sensoren, accessed: 28 July 2021.

Nonetheless, the impact of digitalisation on the citizen-government relationship is not only positive. The relationship has become more impersonal. Instead of being able to address a question to a government official directly, nowadays people are often referred to a website or *chatbox* instead. This means that citizens no longer have face-to-face contact with the government. And the other way round, the fact that government officials have ever less direct contact with citizens can cause them to miss out on the human aspect when implementing policies.

The installation of sensors and cameras in public spaces can also make people suspicious. Comparisons with George Orwell's *1984* are never far away, in part because of developments seen elsewhere in the world. We have previously seen how the Chinese government uses digitalisation to control its citizens. In China, the 'Social Credit System' observes and assesses citizens – and businesses – according to a range of metrics, awarding each a score.[2] A low score can result in things like getting turned down when applying for a loan or buying a plane ticket.[3] In Chapter 2, we looked at Jeremy Bentham's panopticon design with its inbuilt system of control. In China, surveillance has a disciplinary effect on the population. An entire population group, the Uyghurs, is systematically monitored and oppressed. The situation in China serves as a warning sign concerning the extent to which government is able to control the lives of citizens thanks to digitalisation.

Liberals believe that the government should stick to its core tasks, leaving citizens alone as much as possible. Government power should be limited and monitored using the necessary '*checks and balances*'. In essence, power should reside with the citizens and not with the government. At the same time, citizens need the government in various ways if they are to live good lives, so the government needs to have the resources and powers to provide this. Balance in the citizen-government relationship should therefore always be maintained. However,

2. The system is still under development and is actually an umbrella term for separate public and private systems.

3. K. Kuo, 'China bans 23m from buying travel tickets as part of 'social credit' system, *The Guardian*, 1 March 2019, URL: https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system, accessed: 28 July 2021.

digitalisation changes the dynamics of this relationship, creating an imbalance in some areas.

This chapter explores how liberal values can serve as a code guaranteeing a healthy and balanced citizen-government relationship. For example, we see that some people appear to fall by the wayside, because they cannot or do not want to follow the digitalisation trend. The application of automated government technology does not always lead to happy outcomes for citizens. This raises questions about transparency and accountability. Finally, we will look at the Dutch government's use of digitalisation during the Covid-19 pandemic.

5.2 A government for all citizens

If you grew up in the information society, digitalisation will have been an integral part of your life from an early age. Educator Marc Prensky coined the term '*digital native*' for people born after 1980, who have been surrounded and engulfed by digital technologies since childhood. They are used to fast information processing, multitasking and interactive forms of learning. Prensky contrasts them with the '*digital immigrant*' – people born before 1980 who had to learn to deal with digital technology at a later age. Just like when learning a new language, they have more difficulty acquiring digital skills because their formative childhood years took place in the non-digital era.[4] There are even suggestions that there are differences between the brains of these two groups.[5] [6]

Even today, digital literacy within the population is not a certainty. In 2021, some 8 percent of the EU population had never used the internet. Most of them were over-65s.[7] But it is not only the elderly, other groups often struggle with digitalisation too. People with disabilities, immigrants, the illiterate and the less-educated are more likely to encounter

4. M. Prensky, 'Digital natives, digital immigrants', *On the Horizon*, 2001, no. 5, pp. 1-2.
5. M. Prensky, 'Digital natives, digital immigrants part II: do they really think differently?', *On the Horizon*, 2001, no. 6, pp. 1-6.
6. Neuroplasticity causes the brain to undergo physical changes as a result of the input it receives. The brain development of anyone who has been exposed to digital technology from an early age is thus different to someone who has not had this exposure.
7. Big Think, 'Europe's stunning digital divide, in one map', 26 January 2023, URL: https://bigthink.com/strange-maps/europe-digital-divide/, accessed: 20 July 2023.

difficulties than others. Not only do some people lack the skills they need to survive in the digital world, a lack of material access can also be an issue. Not everyone has a smartphone, tablet or laptop.[8]

This poses a dilemma to governments in the process of digitalisation. Some people risk getting left behind. Some individuals do not know how to deal with online government services. They struggle with technology, but feel obliged to go along with the government's digital plans. In the Netherlands, for example, government post is sent out exclusively via digital means. And yet, in 2016, 20 percent of people who had activated this feature took more than a year to check their account after receiving a new message. This can have unwanted consequences if, for example, you miss a reminder. Sometimes people activated digital accounts by accident and missed government mail as a result.[9] Furthermore, these people may find themselves unintentionally dependent on others to handle confidential government matters. Caregivers describe how they regularly find themselves seeing privacy-sensitive data, such as credit card details and login codes, when helping people with government matters.[10] This compromises these individuals' privacy and creates an uncomfortable situation for both the caregiver and the person receiving assistance.

As well as people being unable to keep up with the government's push to digitalise, there are others who simply do not want to do so. Some people have privacy concerns about how the government collects their data. Digitalisation provides new possibilities for government surveillance, and from a liberal perspective, it is easy to understand how this can make people suspicious. Added to which, people worry about the security of this data. This is not unfounded. A significant number of all data breach reports come from the government.[11]

The issue then becomes the extent to which the government should make allowances for these digital abstainers and sceptics. For example,

---

8. Ibidem, pp. 23-24.
9. De Nationale ombudsman, *Hoezo* Mijn*Overheid? Onderzoek naar knelpunten voor burgers bij MijnOverheid / de Berichtenbox*, The Hague, 2017, pp. 15-22.
10. L. Das et al., 'Hulp aan digibeten schiet tekort, identiteitsfraude ligt op de loer', *NOS*, 22 February 2019, URL: https://nos.nl/nieuwsuur/artikel/2273004-hulp-aan-digibeten-schiet-tekort-identiteitsfraude-ligt-op-de-loer, accessed: 5 August 2021.
11. Autoriteit Persoonsgegevens, *Jaarrapportage meldplicht datalekken 2020*, The Hague, 2021, p. 3.

should the government continue to offer non-digital alternatives to its services? Liberals maintain that every citizen should be treated equally by the government. As a liberal value, equality means that the government cannot differentiate between citizens. Therefore, when it comes to digitalisation, the government cannot afford itself the same liberties as private parties. Private companies are free to fully embrace digitalisation and customers cannot insist that non-digital alternatives remain available. This would hinder the market's creative destruction process. However, the government – unlike businesses – does not act from a profit standpoint, but in the overall interest of society. After all, citizens have no choice when it comes to government services, unlike the businesses they choose to use.

The government exists for all of us, and this should mean digital abstainers and sceptics too. This means that citizens should in principle always be able to communicate with the government in a non-digital way. From a government perspective, continuing to provide non-digital channels might seem like an unnecessary expense, but the government needs to remember that every individual citizen is entitled to equal treatment. The principle point of departure in this relationship should always be the interests of the citizen rather than the wishes of the government.

At the same time, we cannot overlook how essential it has become in today's society to have digital skills and material access to the digital world. Life nowadays is largely online, whether you are looking for work or maintaining social contacts. Liberals attach great importance to self-reliance. Anyone excluded from the digital world finds it increasingly hard to hold their own in today's society. Groups that were already in an inferior position in society, such as immigrants and the less well-educated, seem to be victims of digital exclusion.[12] This is also an obstacle to active citizenship and is detrimental to the idea of a participatory society. It is important for citizenship that people feel truly connected to the society they live in.[13] When citizens feel that their access to society is restricted, they can end up feeling frustrated and apathetic towards it.

12. Van Deursen, *Digitale ongelijkheid in Nederland anno 2018*, p. 38.
13. A. Ellian et al., *Bezielend verband: Basisgrammatica van het Nederlandse burgerschap*, politiek-wetenschappelijke stellingname 4 van de Prof.mr. B.M. TeldersStichting, The Hague, 2018, p. 24.

Liberals believe that the government is justified in facilitating digital inclusion. In line with the ideas of John Rawls, this can increase opportunities for individual self-development.[14] Without the need for drastic government redistribution policies. In fact, developing digital skills can help people avoid the need to claim social security benefits, because they find it easier to seek employment and are able to secure better, more qualified work, for example. In this sense, liberals on both the left and right sides of the spectrum should be able to agree on this policy.

At European level, there are initiatives such as the Digital Education Action Plan.[15] The EU intends to ensure that citizens develop the digital skills they need the function in society. At national level, some countries offer courses tailored to different target groups. Teaching things like how to look up information online, make online payments and deal with online government services.[16] Another great initiative is the collection of old laptops and tablets to donate to children and other vulnerable groups who lack the financial resources to buy them.[17] In the Netherlands, special information points for government matters have been set up in libraries, that citizens can turn to with questions.[18] Such initiatives promote digital inclusion in society and this, in combination with maintaining non-digital government channels, should ensure that no citizen is left behind. This type of approach by the government – which facilitates rather than compels – might convince citizens who struggle with digitalisation, so that they too may remain equal citizens in the digital age.

5.3 Government use of automated systems

Digitalisation allows the government to work more efficiently. When processes are automated, work is taken out of the hands of government

14. See Rawls' second principle of justice in section 2.5.
15. European Commission, 'Digital Education Action Plan (2021-2027)', URL: https://education.ec.europa.eu/focus-topics/digital-education/action-plan, accessed: 20 July 2023.
16. Digisterker, *Digisterke verhalen: mensen op weg naar digitaal zelfvertrouwen*, Enschede, 2017, p. 3.
17. Allemaal digitaal, 'Over ons', URL: https://www.allemaal-digitaal.nl/#over, accessed: 5 August 2021.
18. Informatiepunt Digitale Overheid, 'Informatiepunt Digitale Overheid', URL: https://www.informatiepuntdigitaleoverheid.nl/, accessed: 5 August 2021.

employees, giving them more time for other things. These technologies also help the government gain a better understanding of certain societal matters. For example, algorithms can help calculate the likelihood of particular children dropping out of school[19], or which streets appear to suffer an increased risks of loneliness and depression.[20] Algorithms can help support the government in making decisions and formulating policy. Limited capacity can be put to better use. Some governments have embraced automation and want to be data-driven. There is a lot of techno-optimism among these governments, who want to get the most out of the new opportunities that digitalisation offers.

Nevertheless, there have already been incidents in which government use of algorithms has led to problems. A case in point is the Netherlands, where algorithms were used to detect fraudulent requests for social benefits. This gives rise to what has come to be known as the 'childcare benefits scandal'.

The Dutch childcare benefits scandal demonstrated two ways in which government digitalisation can lead to policy failure. Firstly, because the digital systems struggled to process all the requests. This meant that applications were only checked after benefits had already been paid out, opening the door to fraudsters. Subsequently, the imbalance swung in the other direction and a digital risk detection system wrongly identified innocent people as fraudsters. This went as far as to deem certain people as more suspicious than others from the outset, simply on the grounds of their origins. As the organisation executing the operation, the Tax Authorities took things too far, but this was only because the government and parliament had encouraged them to do so. The role of politics in implementing systems like these should not be overlooked.[21] Moreover, although this incident took place in the Netherlands, it is impossible to rule out similar incidents happening in the future in other

19. W. de Jong, J. Schellevis, 'Overheid gebruikt op grote schaal voorspellende algoritmes', *NOS*, 29 May 2019, URL: https://nos.nl/artikel/2286848-overheid-gebruikt-op-grote-schaal-voorspellende-algoritmes-risico-op-discriminatie, accessed: 9 August 2021.

20. S. Beerends, 'Voorspellende algoritmen versimpelen en maken ongelijker', *Sociale Vraagstukken*, 9 Januari 2019, URL: https://www.socialevraagstukken.nl/voorspellende-algoritmen-versimpelen-en-maken-ongelijker/, accessed: 9 August 2021.

21. The handling of the childcare benefits scandal also turned into a drama. It revealed how when large groups of citizens find themselves in (digital) bottlenecks, the government lacks the means to find fast solutions.

European countries. For example, the Spanish and Danish governments are now using algorithms to detect benefit fraud cases too.[22]

The role of digitalisation in the childcare benefits scandal

In the Netherlands, citizens whose income is below a certain threshold are entitled to certain government benefits. 2006 saw the introduction of a new benefits system carried out by the Dutch Tax Authorities. The implementation of this new system left a great deal to be desired, above all because its supporting ICT system was substandard. As a result, money was often paid out to people who were actually not entitled to it. In 2013, Bulgarian gangs were found to have collected millions of euros in unjustified benefits. At the request of politicians, the Tax Authorities took a tough new line in combatting fraud. Including when it came to requests for childcare benefits. As a result of this strict approach, thousands of parents were unjustly deemed to be fraudsters, for reasons as minor as making small administrative errors. They had to pay back all the money paid out to them as well as being labelled as fraudsters. Many got deep into debt and some even had their children taken into care. The government refused to listen when they tried to object. The Tax Authorities had used an algorithm-based risk signalling system to detect fraud. One of the indicators of fraud included in this system was having dual nationality. It subsequently transpired that the government's handling in the affair had been far too strict and that innocent citizens had fallen victim to it. The childcare benefits scandal ultimately resulted in the fall of the Dutch government in 2021, following the publication of a damning report.

22. 'La Seguridad Social tiene una AI con la que vigila las bajas laborales para cazar fraude', *Business Insider*, 17 April 2023, URL: https://www.businessinsider.es/seguridad-social-vigila-ia-posibles-fraudes-baja-laboral-1231448, geraadpleeg: 24 July 2023; G. Geiger, 'How Denmark's welfare state became a surveillance nightmare', *Wired*, 7 March 2023, URL: https://pulitzercenter.org/stories/how-denmarks-welfare-state-became-surveillance-nightmare, accessed: 24 July 2023.

We also see automated technologies being used in controversial ways by other government organisations. For example, the police now regularly engage in '*predictive policing*', where they use algorithms to make risk assessments. This system has been copied from the United States and is used to anticipate criminal incidents. For example, there are now algorithms that calculate the probability of '*high impact crimes*' such as home burglaries, street robberies and muggings. Areas are divided up and assigned risk scores. This score is determined by an algorithm that looks at things like the crime history of an area and the types of businesses that are located there, as well as the demographic and socio-economic data of local residents.[23] This risk prediction can help the police deploy agents in a more targeted manner. *Predictive policing* can also be used to calculate risk scores not only for neighbourhoods, but also for specific individuals. For example, systems like these can be used to calculate which individuals have an increased chance of committing a serious crime or becoming radicalised.[24]

There are several major drawbacks to the use of these types of algorithms by government bodies. First and foremost, risk assessments can lead to unintended feedback loops. For example, when it comes to *predictive policing*, the algorithm leads to the deployment of extra police in certain areas. The increased police presence means that more criminal incidents are detected. This data is fed back into the algorithm, which then interprets these areas as being at even greater risk of crime, requiring even greater police presence. Meanwhile, incidents in other areas are overlooked. As such, a degree of confirmation bias sneaks into the algorithm, because it only processes incidents of reported crime and unreported incidents stay out of sight.[25] This unintended feedback loop can occur in other government risk detection systems too.

Furthermore, the data itself can be defective. Governments do not always maintain their data management systems properly. Data can be

23. R. Doelemans, D. Willems, '*Predictive policing* – wens of werkelijkheid?', *Tijdschrift voor de Politie*, 2014, no. 4, p. 41.
24. R. Rienks, *Predictive policing. Kansen voor een veiligere toekomst*, Apeldoorn, 2015, pp. 125-126.
25. R. van der Kleij et al., 'Wat is er mis met predictive policing', *Tijdschrift voor de Politie*, 2018, no. 7, p. 18.

outdated or entered incorrectly. Furthermore, data is frequently but incorrectly assumed to be completely objective. But the choice of which data you use and how it is categorised is a subjective matter and can give a distorted image.[26] However cleverly an algorithm is set up, if the quality of the data input is poor, the output will be of little value. Algorithms can also carry the – often unconscious – bias of the designer. For example, researcher Marlies van Eck showed how the algorithm used by the Dutch Tax Authorities in the childcare benefits scandal was programmed to reach a flag up incidents of fraud very quickly upon detecting errors in benefits applications.[27]

The greater the complexity of data sets and algorithms, the more likely errors are to creep in. As we have already seen, companies also use complex predictive algorithms to map individual behaviour in the surveillance economy. However, the consequences of an error there are much less likely to be as serious as when this happens with the government. A personalised Facebook advertisement shown on the wrong basis will do little harm, while a wrongful accusation of fraud by the government has far-reaching consequences. Algorithms can also give government employees an unjustified sense of security, because they often work on the assumption that the computer is always right. Many government employees have said that they find it hard to deviate from an algorithm's assessment on the basis of their own expertise.[28]

From a liberal perspective, there are significant risks to the government using automated technologies of this type. It puts the equal treatment of the individual at stake. In a democratic legal system, there is always a 'presumption of innocence'. This means that an individual is always considered innocent until proven guilty. When governments use risk detection systems, individuals can be suspected of certain illegal activities in advance. Algorithms can factor in discriminatory elements such

26. K. van Teeffelen, 'Een algoritme is niet neutraal, ook een overheidsalgoritme niet', *Trouw*, 30 March 2021, URL: https://www.trouw.nl/binnenland/een-algoritme-is-niet-neutraal-ook-een-overheidsalgoritme-niet~bbc021do/, accessed: 10 August 2021.
27. P. van den Brand, 'De digitale lessen van de toeslagenaffaire', *iBestuur*, 31 March 2021, URL: https://ibestuur.nl/magazine/de-digitale-lessen-van-de-toeslagenaffaire, accessed: 10 August 2021.
28. Doove, *Verkennend onderzoek naar het gebruik van algoritmen binnen overheidsorganisaties*, p. 8.

as ethnicity. The government then treats citizens differently depending on their origins, which conflicts with the right to equal treatment of the individual. In addition, there are also risks to the privacy of citizens. A government that wants to make data-based decisions needs to collect and link as much data as possible about its citizens. And just like in the surveillance economy, all sorts of other data can be derived from this.

Nowadays, governments often use semi-automated decision-making, where a government official is always involved and the algorithm only serves as support. Nevertheless, the increasing complexity of algorithms – especially of the self-learning type – means that government employees are becoming increasingly removed from the decision-making process.[29] This makes it even harder for them to draw their own conclusions. Therefore, the fact that they, and not the algorithm, make the final decision is no guarantee that errors will be avoided. Occurrences like the childcare benefits scandal show how such systems can lead to process-oriented decisions that lose sight of people's individual situations. Therefore, semi-automated decision-making is not without risk either. Moreover, it regularly transpires that governments lack an overview of exactly which algorithms they are using.[30] To be able to properly test the extent to which systems like these can be reconciled with liberal values, we need a better understanding of how the government uses technologies of this type. This is the only way to enable citizens to hold the government accountable.

5.4 Transparency and accountability

Government techno-optimism can result in technocratic policy. The government relies on technology which it views as neutral. However, technology is never neutral, because as we saw above, its designers make choices – consciously or otherwise – during its design. The great danger of technocratic policy is that governments end up reducing societal matters to merely technical ones. As a result, they overlook the underlying

29. Algemene Rekenkamer, *Aandacht voor algoritmes*, The Hague, 2021, p. 6.
30. 'Rekenkamer: nauwelijks aandacht voor ethiek bij algoritmes overheid', URL: https://www.rtlnieuws.nl/economie/bedrijven/artikel/5210969/rekenkamer-nauwelijks-aandacht-voor-ethiek-bij-algoritmes, accessed: 11 August 2021.

socio-political discussions.[31] Democratic debate is necessary, because different values need to be weighed up against each other. However, as a consequence of automation, government has become less transparent and its choices have become hidden from public view. Therefore, creating greater transparency matters if citizens are not to be sidelined.

Transparency in the citizen-government relationship may be even more important than it is for the tech companies we looked at earlier, within the surveillance economy. The government does not have an *opt-out*-option. Citizens are obliged by law to file tax returns, for example, and to register their residential addresses with the municipality. Due to digitalisation, the government is increasingly governing its citizens through data and algorithms. This demands control mechanisms with regard to these technologies.

First and foremost, it is often unclear what citizen data the government holds and how it is stored.[32] As a result, citizens are unable to assess how responsibly the government handles their data. There is often a lack of an overview within government and between different government bodies too. This means, for example, that people find themselves submitting their data more often than they should.[33] An additional problem is that government agencies often work with private companies on ICT matters,[34] and the latter can gain access to citizens' personal data as a result. When no clear agreements are in place, there is always a potential for misuse.

The biggest issue is that it is unclear who in government is ultimately responsible for all this data. As a result of digitalisation, systems are increasingly interconnected and data is shared between various government bodies. Horizontal data chains of this sort cannot be reconciled with a government in which responsibility is vertically structured.[35]

---

31. M. Janssen, G. Kuk, 'The challenge and limits of big data algorithms in technocratic government', *Government Information Quarterly*, 2016, no. 3, p. 371.
32. Ibidem.
33. L.S. Barbosa et al., 'Data governance: organizing data for trustworthy Artificial Intelligence', *Government Information Quarterly*, 2020, no. 3, p. 3.
34. M. de Ree, 'Hoe krijgen we algoritmen zo eerlijk mogelijk?', *Centraal Bureau voor de Statistiek*, 3 December 2020, URL: https://www.cbs.nl/nl-nl/corporate/2020/49/hoe-krijgen-we-algoritmen-zo-eerlijk-mogelijk-, accessed: 15 September 2021.
35. Wetenschappelijke Raad voor het Regeringsbeleid, *iOverheid*, Amsterdam, 2011, p. 120.

When many people share partial responsibility, no one feels responsible in practice. Government bodies then start referring people on to other places and citizens do not know who to turn to.

Therefore, people need to have a better understanding of their data and the opportunity to bring errors or misuses to the attention of a body who ultimately has the administrative authority. After all, under the GDPR, citizens have right of both access and rectification.[36] Furthermore, the process must be easy and clear. It could take the form of a 'digital safe', in which citizens could communicate with all government bodies, as well as an exact overview of their data that is being shared.[37] This would prevent all this data from becoming fragmented and would enable citizens to hold the government accountable for misuses. Were it properly implemented, a plan of this kind would provide greater transparency as well as giving citizens more autonomy around their data. Further investment and necessary legislation would be required.

In any event, people within the government would need to be given the authority and the final say, ensuring that citizens no longer find themselves being sent from pillar to post. They would also need to be able to specify which agreements had been made in cooperation with private parties to guarantee the privacy and security of citizens.

In addition to openness about data, the government needs to be more transparent about its use of algorithms. However, the government itself has also pointed out the disadvantages of such transparency. For example, the privacy of citizens would be compromised were it to publish the training data of its algorithms. Much of this data is personal in nature. In addition, it would also allow criminals to see which algorithms are used by investigative services, so they would find out even more about how to circumvent them.[38] These are two legitimate arguments that need to be taken into account when striving for transparency. A system of 'tiered transparency' could offer a solution to this. This would require a

36. European Parliament and Council, *Regulation (EU) 2016/679 (General Data Protection Regulation)*, Article 15-16, Brussels, 2016.
37. Tweede Kamer der Staten-Generaal, *Initiatiefnota van de leden Middendorp en Verhoeven: Online identiteit en regie op persoonsgegevens*, The Hague, 2018.
38. S. Hartholt, 'Transparantie over algoritmen kan innovatie schaden', *Binnenlands Bestuur*, 11 October 2018, URL: https://www.binnenlandsbestuur.nl/digitaal/nieuws/transparantie-over-algoritmen-kan-innovatie.9598927.lynkx, accessed: 15 September 2021.

designated party to monitor internal data on the basis of full transparency on the public's behalf. This party would then need to provide a redacted public report to the people.[39] [40]

It is sometimes argued that the government, as a client who procures these algorithms from private companies, it is obliged to protect the trade secrets of these companies. This is not a legitimate excuse for the government. This is because the government should check in advance whether working with a private party would prove an obstacle to its duty of transparency. If it proves to be so, the government should not enter into an agreement with it. Protecting trade secrets should not be used retroactively as a justification for a lack of openness on the government's part.

This is indicative of an underlying problem. All too often, transparency and accountability are mere afterthoughts, instead of being taking into consideration from the start of policy design. The government must draw up clear transparency standards and only use technologies compatible with them (see more on this in Chapter 7). What exactly the transparency requirements are that need to be met, when deploying these sorts of technologies, also needs to be clear to government employees from the outset. Government employees have previously expressed a need for this.[41] There is a need for a framework in which algorithms can be used in a responsible and careful manner.

According to researcher Marc Steen, it is also important to provide a clear definition of transparency. He emphasises the importance of speaking in concrete terms when it comes to transparency. Scientists, government employees and citizens do not always mean the same thing when they use this term. It is important to talk about specific aspects, such as the reliability or purpose of a particular algorithm.[42] For the regular citizen, the focus of transparency should be on explainability.

---

39. Wetenschappelijke Raad voor het Regeringsbeleid, *Big Data in een vrije en veilige samenleving*, Amsterdam, 2016, p. 144.
40. This model is also familiar when providing business financial accountablility in business.
41. Doove, *Verkennend onderzoek naar het gebruik van algoritmen binnen overheidsorganisaties*, pp. 10-11.
42. M. Steen, 'Discussie over de transparantie van algoritmen blijft nodig', *Het Parool*, 19 July 2020, URL: https://www.parool.nl/columns-opinie/discussie-over-de-transparantie-van-algoritmen-blijft-nodig~b882ed5f/, accessed: 15 September 2021.

This means that the government needs to provide information about algorithm use in clear language. Why is an algorithm being used and what exactly is it for? On the technical side, there is a need for transparency about the exact way in which algorithms work. As this is often too complicated for the average citizen, independent technical experts need to look at this. For example, assessing algorithms by looking at their source code. The government can only practise accountability if it complies with these different aspects.

However, when the government deploys automated technologies, transparency and accountability do not always suffice. In some cases, the government needs to ask itself whether it is wise to use automation at all. The more complex government processes become, the greater the risk that the use of technology will lead to complications. This needs to be thought through very carefully, especially when it comes to government procedures in which errors could cause great harm to the those affected. We previously saw how the complexity of the benefits system played a major role in the problems that arose in the childcare benefits scandal. The saying 'first organise, then automate' is particularly pertinent here,[43] and all the more so when the government wants to use more advanced technologies like AI. Nor should we overlook the risk of automation causing the government to lose its human element. When it comes to complex issues, citizens need to be able to talk to real people, instead of losing their way in a digital labyrinth. Digitalisation should not make the citizen-government relationship more complex, but should simplify it instead.

5.5 Lessons from the Covid-19 pandemic

The coronavirus outbreak in late 2019 drove the world into a pandemic. The Covid-19 crisis that ensued proved a major challenge for society and strained the citizen-government relationship. The crisis had a major digital component when digitalisation proved essential in keeping society running while *lockdowns* forced everyone to stay at home as much

43. In this way, the need to use algorithms can also become a driving force in making government processes more transparent in a general sense.

as they could. Digitalisation was crucial both for the government to continue its work, and to combat the virus. In many countries during this period, digital initiatives emerged rapidly and often developed into matters of public debate. This makes it interesting to take a closer look at Covid-19 policy and to see the extent to which liberal values can be identified within it. This section focuses on the Netherlands, but we would like to emphasise that the developments that took place in the Netherlands occurred in other European countries too, and the lessons that can be drawn from them are also applicable elsewhere.

In April 2020, about a month and a half after the first Dutch Covid-19 infections were identified, the Dutch government announced plans to develop a mobile app to track Covid-19 infections. In the event of a positive Covid-19 infection case, an automatic notification would be sent to everyone who had been in contact with them. However, the Minister of Health, Welfare and Sport (VWS) at the time also emphasised the need to guarantee everyone's privacy.[44] The government took a rather unusual approach when it came to developing this app. It invited software companies to submit their own ideas. Of the 750 proposals submitted, seven were selected and publicly tested during an event dubbed the 'appathon'.[45]

The results were disappointing. The privacy and security risks of almost all the proposed apps were widely criticized. Indeed, one of the apps even suffered a data breach.[46] The Ministry of Health, Welfare and Sport decided instead to develop the app internally with the involvement of various experts from different fields. This ultimately resulted in the CoronaMelder app, available for download nationwide as of 10 October 2020. The app did not use names, email addresses, phone addresses, or

44. 'Apps moeten verspreiding coronavirus tegengaan, maar hoe zit het met privacy?', *NOS*, 7 April 2020, URL: https://nos.nl/collectie/13833/artikel/2329754-apps-moeten-verspreiding-coronavirus-tegengaan-maar-hoe-zit-het-met-privacy, accessed: 21 September 2021.

45. 'Overheid test dit weekend 7 corona-apps in 'appathon'', *RTL Nieuws*, 17 April 2020, URL: https://www.rtlnieuws.nl/tech/artikel/5093906/covid19-coronavirus-coronacrisis-corona-app-appathon-vws-privacy, accessed: 21 September 2021.

46. H. Bahara, 'Presentatie mogelijke corona-apps laat veel slordig haastwerk zien', *de Volkskrant*, 19 April 2020, URL: https://www.volkskrant.nl/nieuws-achtergrond/presentatie-mogelijke-corona-apps-laat-veel-slordig-haastwerk-zien~bfe8143b/, accessed 21 September 2021.

location information.[47] Its source code was also made completely public, allowing anyone to examine and test it.

Two key liberal values took centre stage in the public debate surrounding the Covid-19 app: (medical) safety and privacy. The Dutch population was extremely divided on the subject. Researchers from the TU Delft emphasised in a report on the development phase of the app, that they had rarely encountered such strong discord among the Dutch people when it came to government policy. A third of the population stated that they would definitely not install the app, a third doubted they would, and a third said that they intended to install the app.[48] These societal divisions must have been one of the motivations behind the government's decision to opt for a highly transparent development process and to involve civil society. They must have hoped it would increase support. Unfortunately, it seems that the rushed launch of the various apps during the appathon had actually damaged trust among the people. After the event, the minister claimed that the communications around the appathon had been unclear, and that it had been intended as a market consultation only, rather than the rollout of a definitive app.[49] Although valuable lessons were undoubtedly learned during the process, a lack of clarity regarding the government's intentions meant that it ultimately was not a success story.

This was not the only place where communications fell short. Many citizens were unaware of how much consideration had been given to privacy in the CoronaMelder app's technology. A survey at the end of the app's first nine months found that 56 percent of users and 67 percent of non-users incorrectly believed that the app tracked location data.[50] It is worth noting that there appeared to be a direct correlation between app use and overall trust in the government.[51] It is important to recognise

47. CoronaMelder, 'CoronaMelder', URL: https://www.coronamelder.nl/nl, accessed: 22 September 2021.
48. M. Collewet, R. Kessels, N. Mouter, *Nederlanders zijn het niet eens over de wenselijkheid van de corona app*, TU Delft report, Delft, 2020, p. 31.
49. 'Jacht op corona-app 'was eigenlijk marktconsultatie'', *AG Connect*, 2 September 2020, URL: https://www.agconnect.nl/artikel/jacht-op-corona-app-was-eigenlijk-marktconsultatie, accessed: 22 September 2021.
50. W. Ebbers et al., *Evaluatie CoronaMelder: een overzicht na 9 maanden*, The Hague, 2021, p. 18.
51. L.N. van der Laan, N.E. van der Waal, J.M.S. de Wit, *Eindrapportage CoronaMelder Evaluatie. Survey LISS panel – Wave 1*, Tilburg University report, 2020, p. 65.

that when it comes to support, digital initiatives like this should never be seen as distinct from government policy as a whole.

The development of the CoronaMelder app was not the only difficulty for the government during the Covid-19 crisis. There were other incidents in which the problems lay not with the technology itself, but with its users. For example, a journalist managed to hack his way into a confidential video conference between various European Ministers of Defence. He was able to do this because the Dutch Minister of Defence had previously tweeted a picture showing the meeting's login address and five of its six pin numbers.[52] A minor slip-up, but one that could have had serious consequences. It could easily have been a foreign intelligence service rather than a journalist gatecrashing a European defence meeting.

A somewhat less fortunate incident occurred at the Dutch Municipal Health Service (GGD), the government agency responsible for the Covid-19 testing and vaccination programmes. This was a data breach, in which the personal data – including home addresses, telephone numbers and social security numbers – of at least 1,250 (but probably many more) private individuals was stolen and possibly resold to criminals.[53] What made it worse was that it was GGD employees who stole this data. They were able to access it easily, although they were not authorised to do so. What was particularly neglectful was that the GGD had been aware of privacy and security risks in the system for months, but had done almost nothing about them. Nor had all employees been asked to provide a Certificate of Conduct (VOG).[54]

The Covid-19 crisis was a unique challenge for the government. From the outset, technology was seen as pivotal in getting through the crisis. Crisis situations demand a quick and resolute response. Various digital

52. 'RTL Nieuws kwam binnen bij geheim defensieoverleg Europa na fout ministerie', *RTL Nieuws*, 20 November 2020, URL: https://www.rtlnieuws.nl/tech/artikel/5198276/rtl-nieuws-hack-defensie-ministers-europa-overleg-bijleveld, accessed: 22 September 2021.

53. 'Datadiefstal GGD veel groter dan gemeld, gedupeerden niet geïnformeerd', *RTL Nieuws*, 12 August 2021, URL: https://www.rtlnieuws.nl/nieuws/nederland/artikel/5247728/datalek-datadiefstal-ggd-gedupeerden, accessed: 23 September 2021.

54. M. van de Klundert, J. Schellevis, 'Lek in GGD-systeem al driekwart jaar aanwezig', *NOS*, 28 January 2021, URL: https://nos.nl/artikel/2366341-lek-in-ggd-systeem-al-driekwart-jaar-aanwezig, accessed: 23 September 2021.

initiatives were rapidly assembled. But it's clear now that many errors were made in this haste. While it is easy to understand the government's wish to act quickly, the problems that arose as a result of this speed ultimately detracted from the support for these initiatives. A desire for quick results sometimes gives rise to less effective long term policy. It would be wise never to lose sight of liberal values like privacy and (cyber) security, even in crisis situations, and to not only consider them as afterthoughts.

When doing this, it is important to think not only about the technology, but also about the framework for action for users. The government's attempts to be optimally transparent about its digital plans is commendable. At the same time, we have seen that this can give rise to a great deal of public debate. In retrospect, when reflecting upon the CoronaMelder appathon, we have to wonder whether it was wise to involve the general public at such an early experimental phase of its development. It is clear that the government should have communicated its intentions more clearly from the get-go. At a later stage, it also failed to inform the public adequately about how the app handled privacy matters, including not using location data. So not only does the technology need to take liberal values into account, but it is important that public perception about this is accurate too. Good communication is key here too.

Last but not least, it is essential to remove any special measures taken during a crisis situation as soon as the crisis is over. All too often these are held in place long after the original reasons for their implementation have ceased to be relevant, a concept sometimes referred to as '*function creep*'. A clear 'sunset provision' should be laid down in advance, so that special measures lapse as soon as the situation permits it.

5.6 Conclusion

This chapter explored the effect of digitalisation on the citizen-government relationship. Although digital technology ensures ease of communication and efficiency, it is not entirely without negative consequences. Relationships become more impersonal and the human element is sometimes lost. In countries like China, it's clear that government deployment of digitalisation can give rise to a dystopian society. For liberals, it is important to limit government power and keep it in check. At

the same time, the government must be granted adequate scope to carry out its tasks. The new dynamics brought to the citizen-government relationship through digitalisation mean that it is necessary to sometimes look for a new balance in certain areas.

The government must not overlook citizens who either cannot or do not want to follow the digitalisation trend. There are still many people who struggle with technology or have limited material access to the digital world. Also, some citizens are understandably worried about how the government collects and secures all this data. According to liberals, every citizen is entitled to equal treatment by the government. After all, the government exists to serve us all. Therefore, as a matter of principle, citizens should always retain the option of communicating with the government in a non-digital way, independently of the government's own view on the matter. Nonetheless, digital skills are important in today's society. This means that the government needs to focus on digital inclusion to ensure that citizens remain self-sufficient, feel connected to society, and can maximise their potential. It must be approached in a way that facilitates and does not appear compulsory.

We have also noted that the government is making increasing use of automated technologies like algorithms. This makes policy more efficient and creates a better understanding of society. But it also puts a strain on certain liberal values, like privacy and equal treatment. The Dutch childcare benefits scandal was a clear example of how far-reaching the consequences of this can be. The use of algorithms comes with major risks and the government must take this into account. For example, algorithms can contain confirmation biases or use flawed data. To ensure equal treatment of all citizens, the government must in the first instance presume innocence and not discriminate against citizens. Involving government officials within that decision-making process is not necessarily a guarantee, because they struggle to deviate from the assessments made by these automated systems.

This techno-optimistic vision carries with it the risk of allowing a technocratic government to emerge that ignores underlying political and social debate. As a result, we need greater transparency and accountability in the use of automated technology. Firstly, there needs to be improved awareness of exactly what data the government collects about us. Citizens should also have the possibility to correct errors in this data.

The government needs to have designated officials who carry the final responsibility for this data. Greater transparency is also needed around the use of algorithms. Therefore, the government should refuse to work with any companies unable to provide this transparency on the grounds of trade secrets. Furthermore, it is necessary to draw up straightforward transparency requirements to provide government institutions with a clear framework on how to use algorithms. Transparency must be expressed in concrete terms, with on the one hand a focus on its explainability to the average person, and on the other, providing technical insight to independent technical experts. More importantly, the government must first thoroughly assess whether or not it is wise to use automated technology to begin with. This is particularly true when it comes to complex government procedures in which anything that goes wrong can prove hugely detrimental to the people involved, as we saw with the Dutch benefits system. The saying 'first organise, then automate' applies here.

The Covid-19 crisis was also an interesting case study in exploring how governments can use technology to combat crises. Digitalisation allowed the government both to continue its work and was used as a means to contain the virus. The haste with which digital initiatives were introduced in the Netherlands gave rise to more errors . These errors undermined public support for these initiatives. Various incidents demonstrated that even in a crisis, liberal values like privacy and (cyber) security should not be overlooked. This is true not only of the technology itself, but also of the design of the operating frameworks of the people who use them. In a crisis, ensuring that the public has the correct perception of matters surrounding policy helps avoid misunderstandings. The Dutch government's attempt to provide transparency in a socially sensitive initiative such as the CoronaMelder app was commendable. Unfortunately, this was undermined by inadequate communication, both during the development stage and after the rollout of the app. Furthermore, it must be emphasised that any special measures taken in a crisis situation should be removed as soon as the crisis is over.

The government needs to understand that if it wants to find a new balance in the citizen-government relationship, digitalisation will not be the answer to all of society's problems. Various incidents have already made citizens suspicious, and this will not change unless the government

draws clear lessons from them. Digitalisation is of great value in supporting the implementation of government policy, but it should never be the end goal in itself. Human contact remains essential. After all, citizens do not want to be governed by computer systems, but by human beings who can be held accountable. For liberals, the government's principle point of departure for digitalisation should not be its own interests, but those of the public.

6. Security in digital society

6.1 The digital world in the spotlight

Many European countries are investing heavily in their digital infrastructure. Countries including France, Poland and Romania more than doubled their internet speed between 2019 and 2021.[1] Recently, more than half of all European businesses said to be investing in their digital capabilities.[2] Digitalisation can offer us a great deal, but it also makes us dependent. The consequences of digital malfunctions can be far-reaching. For example, there have been incidents in several countries in which a malfunction caused the national emergency number to be unavailable for hours. In addition to disruptions, this dependency means that cyber attacks are a major concern for society as a whole. Threat actors try to hack into and damage our digital systems for a variety of reasons.

The abstract nature of digitalisation makes it difficult sometimes to predict the potential implications of this threat. Nevertheless, various recent incidents have shown that this threat also has consequences in the physical world. For example, 'ransomware attacks' are a growing problem, in which systems are hacked and locked, and victims are obliged to pay money to get them unlocked. At the end of 2019, Maastricht University in the Netherlands was hit by such an attack and made to pay 200,000 euros.[3] We have also seen slaughterhouses run by JBS, the world's largest meat processing company, get hacked and temporarily

1. European Investment Bank, *Digitalisation in Europe: 2022-2023*, Luxembourg, 2023, p. 16.
2. European Investment Bank, *Digitalisation in Europe: 2022-2023*, p. 2.
3. 'Hackers Universiteit Maastricht zaten maanden in netwerk; 200.000 euro betaald', *NOS*, 5 October 2021, URL: https://nos.nl/artikel/2321732-hackers-universiteit-maastricht-zaten-maanden-in-netwerk-200-000-euro-betaal, accessed: 5 October 2021.

shut down in the USA, Canada and Australia.[4] A ransomware attack on the US oil transport company, Colonial Pipeline, also caused serious fuel shortages in the USA.[5]

Such incidents turn an abstract threat into a concrete danger. What if, for example, a particular drug could no longer be delivered to pharmacies? Or what if a cyber attack caused our now largely digitalised financial system to suddenly stop functioning? In the future, we will become ever more dependent on digital technology, creating ever greater risks. Just imagine what might happen once self-driving cars get on the road were they to be hacked. The more devices that are connected to the Internet, the bigger the target for malicious parties. Growing interconnectivity is also creating chain dependency. As a result, issues with a given component can reverberate across the entire network.[6]

Nevertheless, the measures taken to protect against such attacks are often insufficient. Cybersecurity is seen as an annoying added expense, rather than as a priority. Many people still believe that they will never be affected, leaving them with an unfounded sense of security.[7] Only once it is too late and things have already gone wrong, do they become aware of the consequences. Something that does not help here either is that in many cases, the knock-on effects are not felt by the immediate target.[8] Imagine a data breach at a company which results in customer data being leaked into the public domain. We have to wonder whether companies are stimulated enough to put cybersecurity measures in place. Liberals believe that the harm principle justifies government intervention to prevent someone from harming his fellow citizens. Although this does not mean that we ought to prevent all possible harm, when we see how

4. 'Cyberaanval legt grootste slachterij van de wereld plat', *NOS*, 1 June 2021, URL: https://nos.nl/artikel/2383125-cyberaanval-legt-grootste-slachterij-van-de-wereld-plat, accessed: 22 December 2021.
5. V. Romo, 'Panic drives gas shortages after Colonial Pipeline ransomware attack', *NPR*, 11 May 2021, URL: https://www.npr.org/2021/05/11/996044288/panic-drives-gas-shortages-after-colonial-pipeline-ransomware-attack, accessed: 22 December 2021.
6. Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Cybersecuritybeeld Nederland (CSBN 2020)*, The Hague, 2020, p. 21.
7. Rijksoverheid, 'Nederlander bewuster maar blijft naïef over eigen digitale veiligheid', 26 September 2019, URL: https://www.digitaleoverheid.nl/nieuws/nederlander-bewuster-maar-blijft-naief-over-eigen-digitale-veiligheid/, accessed: 17 December 2021.
8. Nationaal Coördinator Terrorismebestrijding en Veiligheid, *CSBN 2020*, p. 31.

far-reaching the damage that cyber attacks wreak on society can be, we have to ask whether the government should have a role here.

This chapter will explore how societies can make themselves resilient to digital disruptions. We need to identify the actors behind cyber attacks, as well as their motives. We will also explore the different critical processes in society that are vulnerable to this, as well as examining what measures need to be taken in the risk management sphere, and how these can be introduced in a liberal and responsible manner.

6.2 Different types of cyber threats

Cybercrime is a growing problem in many European countries. If we take the Netherlands as an example, we can understand how, thanks to a good digital infrastructure and relatively high use of internet banking, make it a popular target for criminals.[9] In fact, in 2020, the Netherlands was found to have the highest risk of cybercrime in Europe.[10] But other countries including Bulgaria, Lithuania and France also regularly fall victim to it.[11] Cyber criminals do not only target private individuals. Companies, institutions and governments are increasingly falling victim to cybercrime too. We saw several examples mentioned in the section above. The ruthlessness of these criminals is demonstrated by the fact that, during the Covid-19 crisis, they tried to attack not only hospitals, but also institutions like the World Health Organization.[12]

There are two different types of cybercrime. '*Cyber-enabled crime*' refers to long-standing, traditional forms of crime for which digitalisation provides new opportunities. This includes, for example, fraud, which now has a new incarnation in the form of internet scams. Cases

9. H. Modderkolk, *Het is oorlog maar niemand die het ziet*, Amsterdam, 2019, p. 143.
10. 'Cyberaanvallen: Nederland nummer 1 van Europa', *Cybercrimeinfo.nl*, 2 March 2020, URL: https://www.cybercrimeinfo.nl/cybercrime/403654_cyberaanvallen-nederland-nummer-1-van-europa, accessed: 7 October 2021.
11. Specops, 'The European countries most at risk of cyber-crime', 19 February 2020, URL: https://specopssoft.com/blog/european-countries-cyber-crime/, accessed: 25 July 2023.
12. 'NL-initiatief tegen cyberaanvallen op ziekenhuizen', *ICT&Health*, 26 March 2020, URL: https://www.icthealth.nl/nieuws/nl-initiatief-tegen-cyberaanvallen-op-ziekenhuizen/, accessed: 7 October 2021.

of 'pure' cybercrime are known as '*cyber-dependent crime*', in which one digital system is used to break into or attack other systems. This includes hacking computers or spreading viruses.[13]

The best-known types of cyber attack include the ransomware attacks discussed above, where malware is used to take computer systems hostage and lock them. There are also numerous cases of 'phishing', in which attempts are made to lure victims by email, SMS or text message, to a fake website, where they are asked to enter sensitive information such as login and credit card details. Distributed Denial of Service 'DDoS' attacks also occur frequently, in which a website is flooded with internet traffic from a botnet, rendering it unavailable.

For victims, the consequences of cyber crime are often severe. Vulnerable groups like the elderly are often favoured targets. As we've mentioned previously, these groups often struggle with digitalisation. 'WhatsApp fraud' has recently become common practice, with criminals posing as a friend or family member and asking victims of these crimes to transfer money to them. A senior citizen shared how someone posing as a bank employee warned him over the phone that his bank account had been hacked and that he needed to transfer his money to another 'safe' account. But this was a scam and the man lost thousands of euros.[14] Research shows that not only do such scams have financial consequences, but victims also suffer from long-term emotional harm leading to feelings of shame, fear and anger.[15] Feelings of guilt also mean that victims often keep their experiences to themselves and fail to report them to the police. Cybercrime can also have far-reaching consequences on companies and institutions. For example, one victim describes how his thriving advertising agency went bankrupt following a cyber attack in

13. J. Bellasio et al., *The Future of Cybercrime in Light of Technology Developments*, Cambridge, 2020, p. 2.

14. 'Nando's vader werd kaalgeplukt door criminelen via truc: 'Hij is 27.500 euro kwijt'', *RTL Nieuws*, 29 May 2021, URL: https://www.rtlnieuws.nl/nieuws/nederland/artikel/5138011/oplichting-ing-helpdesk-spoofing-man-spaargeld-pensioen-voorburg, accessed: 11 October 2021.

15. R. Leukfeldt, R. Notté, M. Malsch, *Slachtofferschap van online criminaliteit. Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving report, Amsterdam, 2018, p. 115.

which all his files were erased.[16] Europol estimates that the total annual cost of cybercrime to the economies of EU member states is around 265 billion euros.[17]

Criminals use the '*dark web*', the hidden part of the internet where individuals are difficult to trace which makes it well-suited to criminal activity. It can only be accessed through a dedicated internet browser.[18] The anonymity the *dark web* provides makes it a popular place to sell things like stolen credit-card information. However, whether this aspect of the internet should be seen as entirely unwelcome is not a straightforward question to answer. The *dark web* also gives journalists and political dissidents living in dictatorships the ability to communicate with one another safely. This is a good example of how the same technology can be used for both socially desirable and socially undesirable purposes. 'Cryptocurrency' is another example of a double-edged sword. Although it is widely seen as the future of online payments, it is also a popular means for cybercriminals to receive payments anonymously and is next to impossible to detect.

According to the RAND Europe research institute, there are four types of cyber threat actors, each with their own motivations. Firstly, there are individuals seeking personal gain. This can be financial, but can also be something as simple as gaining status. For example, in 2012, a major Dutch telecommunications company was hacked by a 17-year-old boy, whose main motive was to boast about it on an online chat forum afterwards.[19] Secondly, we have the 'hacktivists' who carry out attacks for ideological reasons. One well-known organisation of this type is Anonymous, an international hacker collective that attacked Donald Trump's presidential campaign website in 2015. Thirdly, there are

16. L. Bomers, S. 't Sas, 'Xanders bedrijf ging failliet na cyberaanval: 'Je kan voor honderd dollar een hack bestellen in China'', *EenVandaag*, 5 February 2020, URL: https://eenvandaag.avrotros.nl/item/xanders-bedrijf-ging-failliet-na-cyberaanval-je-kan-voor-honderd-dollar-een-hack-bestellen-in-chi/, accessed: 11 October 2021.
17. Security Delta, 'Europol', URL: https://securitydelta.nl/partners/overview-partners/europol, accessed: 25 July 2023.
18. The '*deep web*' is the 'invisible' part of the internet whose contents are not indexed by search engines like Google. The *dark web* is the part of this in which criminal activity takes place.
19. '17-jarige bekent hacken KPN', *NU.nl*, 27 March 2012, URL: https://www.nu.nl/internet/2773417/17-jarige-bekent-hacken-kpn.html, accessed: 7 October 2021.

criminal organisations who seek financial gain. There are often gangs behind ransomware attacks who operate from abroad. The lack of borders on the internet allows them to carry out large-scale attacks remotely. And fourthly, state and state-sponsored actors aimed at espionage and exploitation.[20]

This last group of actors merits particular attention, as they pose significant safety risks to society as a whole. The increased geopolitical tensions in recent years have increasingly caused states to attempt to undermine each other in the digital world. We have already seen how enemy states try to disrupt democratic processes by exerting political influence online. We are looking specifically at cyber attacks orchestrated by states here, targeting the digital systems of companies, institutions and government organisations. Several countries include these sorts of cyber attacks as an integral part of their government policy. It is a good way for countries under international sanctions, such as North Korea, to access money. According to a report by the United Nations, in the year 2020, some 316 million dollars was stolen by North Korean cybercriminals. The UN estimated that North Korea had already stolen a total of around two billion dollars in the previous period before that. The North Korean regime probably used this money to develop nuclear weapons.[21]

Countries use cyber attacks not only to gain money but also to try to obtain confidential information. For example, hackers working on behalf of the Iranian government attempted to break into various European universities to steal academic knowledge.[22] In early 2018, Dutch military intelligence caught Russian hackers targeting the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague. The cyber operation probably sought to access the OPCW's investigations into the poison gas attacks carried out by the Syrian regime (a Russian ally) and

---

20. Bellasio, *The Future of Cybercrime in Light of Technology Developments*, p. 3.
21. E.M. Lederer, 'UN expert: North Korea using cyber attacks to update nukes', *AP News*, 10 February 2021, URL: https://apnews.com/article/technology-global-trade-nuclear-weapons-north-korea-coronavirus-pandemic-19f536cac4a84780f54a3279ef707b33, accessed: 8 October 2021.
22. J. Engels, 'Iraanse cybercriminelen zijn vooral uit op academische kennis', *Trouw*, 14 February 2020, URL: https://www.trouw.nl/nieuws/iraanse-cybercriminelen-zijn-vooral-uit-op-academische-kennis~boe66d44/, accessed: 8 October 2021.

the poisoning of Russian double agent Sergei Skripal.[23] China in particular has been found to have used cyber espionage to try to obtain trade secrets and knowledge about important technologies from European companies and institutions.[24] In doing so, Chinese companies seek to profit from our investment in '*research and development*'. Digital espionage was also used to steal medical knowledge during the Covid-19 pandemic.[25] What is perhaps most concerning is that these actors also seek to use these cyber attacks to cause social disruption, by specifically targeting our critical infrastructure.

6.3 The vulnerability of critical processes

There are a number of critical processes in our society that are crucial to everyone. If they are disrupted, it can have serious consequences for society as a whole. This includes critical processes in the field of energy, telecoms, water supply, transport, chemistry, nuclear, financial, public order and defence.[26] Digitalisation has become integral to almost all critical processes. These processes all rely on digital systems to carry out important work. This dependence on digitalisation means that all critical processes are now vulnerable to cyber attacks. Although companies and government institutions are investing heavily in digitalisation, their cybersecurity is often substandard. And even if it's not substandard, they may still be vulnerable as a result of chain dependencies, as we saw above. This is because they often also work with external parties, such as software suppliers, or logistics service providers. And when they fall victim to cyber attacks, this can then have knock-on effects further on in the chain.

---

23. NOS, 'MIVD: Russische hack van OPCW voorkomen, MH17-onderzoek ook doelwit', *YouTube*, 4 October 2018, URL: https://www.youtube.com/watch?v=Qg2bSVkWVNs&ab_channel=NOS, accessed: 8 October 2021.
24. Militaire Inlichtingen- en Veiligheidsdienst, *Vooruitziend vermogen voor vrede en veiligheid. Public annual report 2020*, The Hague, 2021, pp. 10-11.
25. Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Cybersecuritybeeld Nederland (CSBN 2021)*, The Hague, 2021, p. 24.
26. Nationaal Coördinator Terrorismebestrijding en Veiligheid, 'Overzicht vitale processen', URL: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen, accessed: 13 October 2021.

Critical processes are good targets for cyber attacks, given how far-reaching an impact they can have. As we saw above, this can also involve state – or state-sponsored – actors. For them, social disruption is their primary goal. But cybercriminals can also be behind cyber attacks like this. Their main motives are often financial, but they can cause social disruption as a side effect.[27] For example, they might use a ransomware attack to paralyse a critical process with the intention of asking for ransom money, but this would cause disruption to society at the same time. The importance of ensuring business continuity for these companies makes them ideal targets for cybercriminals, because there is high societal pressure to resolve the attack as quickly as possible.

Several incidents have taken place in which critical processes have proved vulnerable. Take the case of DigiNotar, which was hacked in 2011. This Dutch company was responsible for issuing websites with security certificates. As a consequence of the cyber attack, fraudulent security certificates went into circulation, so that the security of these websites could no longer be guaranteed. Government websites were also affected, which meant that the security of citizens' data was compromised too. Later it turned out that this hack was intended as a way of spying on civilians in Iran and that the Iranian government was behind the attack.[28] DigiNotar proved a suitable target because the company did not have adequate security measures in place. It used outdated software, had weak passwords, and had no virus scanner. Furthermore, the company sought initially to keep knowledge of the hack under wraps, so that parties affected only learned about it later.[29]

In 2017, two large container companies were hacked bringing the port of Rotterdam to a standstill. It was weeks before work could be fully resumed and the final damage was estimated at about 300 million euros.[30] As the port is a trading hub, the standstill affected the entire

27. Nationaal Coördinator Terrorismebestrijding en Veiligheid, *CSBN 2021*, p. 9.
28. Modderkolk, *Het is oorlog maar niemand die het ziet*, p. 54.
29. 'Diginotar deed geen aangifte hack', *NU.nl*, 2 September 2011, URL: https://www.nu.nl/internet/2605567/diginotar-deed-geen-aangifte-hack.html, accessed: 13 October 2021.
30. L. van Heel, 'Cyberkorps voor Rotterdamse haven tegen groeiende dreiging hackers', *De Ondernemer*, 26 Januari 2020, URL: https://www.deondernemer.nl/innovatie/cybersecurity/cyberkorps-voor-rotterdamse-haven-tegen-groeiende-dreiging-hackers~1928737, accessed: 13 October 2021.

supply chain and this was highly problematic when it came to perishable products like fruit and vegetables, for example.

In 2020, the American company Citrix also appeared to have suffered a security breach. Citrix servers are used to log into internal networks remotely, making it possible to work from home, for example. The leak enabled third parties to hack into these networks to install hostage software. Companies and organisations in critical industries were advised to turn off their servers. However, this would have had dire consequences for the continuity of their work. Ultimately, the companies had to make trade-offs between shutting down the servers, or running them with additional security measures.[31]

The EKANS ransomware virus first emerged in 2020. It was a particular cause for concern because it focused specifically on industrial control systems used for things like energy and drinking water supplies.[32] That same year, hackers introduced malware into a program by the software company SolarWinds, most likely with the intention of spying. This software was used by different organisations within critical industries, as well as government services. It later transpired that the Russian intelligence service was behind the hack.[33]

Municipalities are also popular targets of cyber attacks. In the Netherlands, for example, an easy-to-guess password made it possible for a municipality to be hacked, resulting in damage amounting to around 3.9 million euros.[34] In December 2022, the city of Antwerp in Belgium was also hacked by cybercriminals. Large volumes of personal data were stolen and many payment systems were shut down for days. The damages cost an estimated 70 million euros.[35]

---

31. 'Dingend advies aan overheid: schakel Citrix uit', *NOS*, 17 January 2020, URL: https://nos.nl/artikel/2319103-dringend-advies-aan-overheid-schakel-citrix-uit, accessed: 13 October 2021.
32. Nationaal Coördinator Terrorismebestrijding en Veiligheid, *CSBN 2020*, p. 16.
33. Nationaal Coördinator Terrorismebestrijding en Veiligheid, *CSBN 2021*, p. 21.
34. 'IT-bedrijf wil reputatieschade privé verhalen op burgemeester Hof van Twente', *NOS*, 28 April 2021, URL: https://nos.nl/artikel/2378646-it-bedrijf-wil-reputatieschade-prive-verhalen-op-burgemeester-hof-van-twente, accessed: 14 October 2021.
35. '"We konden nog tegen een stootje, maar dat hebben we nu gekregen": zo veel zal cyberaanval stad Antwerpen kosten', *Nieuwsblad*, 5 January 2023, URL: https://www.nieuwsblad.be/cnt/dmf20230105_92703877, accessed: 25 July 2023.

Foreign states don't just try to gain access to our critical processes through covert cyber attacks. They also attempt to infiltrate the core of our digital infrastructure through investments and acquisitions. Foreign investors can cause unwelcome security risks in this way. The discussions around the 5G network are a good, recent example of this.

Security requirements for rollout of 5-G network
The 5G network is the fifth generation mobile phone network. This network provides the infrastructure for all data exchange between digital devices. The transition from 4G to 5G is a major step in the implementation of new technologies including (semi-) self-driving cars and virtual reality. Only a small number of market players supply the equipment for this. The largest player in this area is the Chinese tech company Huawei. It offers high-quality 5G technology, which it sells for a relatively competitive price. However, Huawei is accused of being a state-owned enterprise in disguise, spying on behalf of the Chinese government. This has raised much discussion around the security issues that his company presents. Intelligence services have warned of the dangers of espionage and sabotage if market parties from countries that conduct offensive cyber programs against European interests – such as China – gain access to critical parts of the 5G network. Several countries ultimately decided not to use Huawei as a supplier of key equipment for the 5G network.

The decision to ban certain market parties can lead to economic loss. For example, European companies including Ericsson (Swedish) and Nokia (Finnish) are now the designated suppliers of key 5G equipment, rather than Huawei. This means higher costs for the rollout of the 5G network and potential delays as a result. Telecom companies will have to replace key Huawei equipment that they already own.[36] Reduced market competition could also cost the European economy billions of euros.[37]

36. 'Huawei verbannen kost Nederland tientallen miljoenen', *RTL Nieuws*, 2 July 2020, URL: https://www.rtlnieuws.nl/economie/tech-business/artikel/5168842/huawei-ban-kostenpost-5g-verbannen-mobiele-netwerken-china, accessed: 15 October 2021.
37. G. Barzic, 'Europe's 5G to cost $62 billion', *Reuters*, 7 June 2019, URL: https://www.reuters.com/article/us-huawei-europe-gsma-idUSKCN1T80Y3, accessed: 25 July 2023.

The 5G debate serves to demonstrate how economic and security interests are not always in alignment. This also true of investments in other critical processes, including transport and energy. Intelligence services warn against investments and acquisitions by foreign companies with geopolitical motives, who are under state control. This can result in an unfavourable strategic dependency and make us vulnerable to sabotage.[38] For example, China is known to be trying to gain economic influence around the world, and it sometimes uses this influence to blackmail countries politically. Furthermore, strategic knowledge about high-tech or defence, for example, can also be leaked to countries that do not share our geopolitical interests. Threats of this sort therefore demand a broad interpretation of security that needs to include the active involvement of the private sector.

6.4 Risk management in the digital world

As mentioned above, liberals believe that security, freedom and prosperity are closely linked. Digital security should now also be added to the list. After all, a digitalised society cannot rely on a foundation that lacks adequate security guarantees. Citizens will then become wary of digital technology. which will ultimately harm our economy and society.

The known security risks in the digital world need to be better managed. The role of the government is important here, as liberals view security as its primary task. If we leave security entirely to private parties, we will see that short-term thinking and self-interest will too often get the upper hand over the importance of a secure digital society. Imagine working with suppliers from high-risk countries, while also wanting to save on cybersecurity. Liberals believe that economic interests like these should never come at the expense of the national security interest. Liberals recognise that, in the physical world, security cannot be achieved through the market and that we need legislation and certain government services to ensure security. This is also true of the digital

38. Nationaal Coördinator Terrorismebestrijding en Veiligheid, 'Economische veiligheid', URL: https://www.nctv.nl/onderwerpen/economische-veiligheid, accessed: 15 October 2021.

world. The government must establish the clear framework for action, within which digital traffic can occur in a safe manner.

When it comes to the 5G network, we see that many European countries so far have made sound choices by focusing on 'strategic autonomy'.[39] This means that they have properly shielded this critical process from foreign market parties that could pose a security risk. Security interests must be weighed up carefully against other economic interests. However, it is important that countries dare to make their own choices. For example, the USA government placed a full ban on Huawei 5G equipment and urged other countries to do the same.[40] Nonetheless, this cannot be viewed in isolation from the ongoing trade war between the United States and China. European countries do not have to make their decisions on the basis of the USA's economic interests. After all, liberals do not believe that strategic autonomy should be used as an excuse for unnecessary protectionism. Therefore, several countries decided only to exclude Huawei from the network core, allowing the company to continue supplying other pieces of equipment.[41] At this time, this seems like a suitable measure to counteract the safety risks. However, the EU notes that several Member States, including Germany, have taken next to no measures, out of fear of economic harm.[42] However, commercial interests should not ultimately come at the expense of national security.

Generally speaking, allowing a critical process to depend on a single market party can present an unwanted risk. It is advisable to diversify suppliers, so that if one party disappears, it does not lead to large-scale social disruption. We need to look at what should be considered critical in this regard. Not only do the direct suppliers of critical processes, such as water and electricity companies, need to be protected, but so do other

39. It should be noted that we are still at the start of this process.
40. 'Huawei: which countries are blocking its 5G technology?', *BBC News*, 18 May 2019, URL: https://www.bbc.com/news/world-48309132, accessed: 20 October 2021.
41. 'Huawei definitief uit kern van Nederlandse telecomnetwerken', *RTL Nieuws*, 21 May 2021, URL: https://www.rtlnieuws.nl/tech/artikel/5232314/huawei-5g-telecom-netwerk-provider-kpn-t-mobile-vodafone-china-spionage, accessed: 4 May 2022; 'Portugal's telecoms exclude Huawei from core 5G networks', *CLBrief*, 31 July 2020, URL: https://www.clbrief.com/portugals-telecoms-exclude-huawei-from-core-5g-networks/, accessed: 26 July 2023.
42. 'EU considers mandatory ban on using Huawei to build 5G', *Financial Times*, 6 June 2023, URL: https://www.ft.com/content/a6900bof-08d5-433d-bfbo-f57b6041e381, accessed: 26 July 2023.

companies that can cause problems indirectly because of the essential role they play within the production chain.[43] In a digital context, this includes suppliers of major software and hardware products. Therefore, critical infrastructure companies need to have a good overview of the many links in their production chains.

In the Netherlands, the government only shares information about cyber threats with companies involved with providing critical processes. We feel the need to question whether this distinction between critical and non-critical is relevant when it comes to sharing this information. After all, cybercrime is a major issue for all businesses. For example, a flower exporter told us that he does not receive any information about cyber threats from the government, despite the importance this sector has to the Dutch economy. He's indicated that he could clearly use it.[44] We would argue that, when it comes to sharing information about cyber threats, it's better to be safe than sorry. The sheer scale of these threats and the harm they can cause to the economy means that it is necessary to ensure all market parties, large or small, stay informed of new developments and recommendations.

We have also seen that when it comes to ransomware attacks, victims are faced with the dilemma of whether to pay the ransom or not. It is often in an organisation's best financial interest to pay up rather than cease operations and wait to recover. Indeed, the latter can even lead bankruptcy. Nonetheless, there are many reasons not to pay a ransom. There is no guarantee that paying up will bring an end to the hack. After receiving an initial payment, cybercriminals may decide to ask for more money. They can also introduce vulnerabilities to a system, to exploit at a later stage and commit subsequent successful attacks, or they may copy sensitive data, and use this for further extortion.[45]

A major issue for society at large is that criminal behaviour gets rewarded by paying up and this means that the problem persists. Some of the ransom money may even get reinvested in resources for carrying out further attacks. Cybercriminals have gone as far as to set up

43. Cyber Security Raad, *Advies inzake de digitale veiligheid van Industrial Automation & Control Systems (IACS) in de vitale infrastructuur in Nederland*, The Hague, 2020, p. 3.
44. Zembla, 'Gehackt en gegijzeld' (documentary), *BNNVARA*, 7 October 2021.
45. Nationaal Coördinator Terrorismebestrijding en Veiligheid, *CSBN 2020*, p. 34.

professional help desks to provide victims with instructions on how to purchase cryptocurrency and pay ransoms.[46] Therefore, it is in society's interests that as little ransom money gets paid out as possible. Liberals believe that the government has a role to play here. Initiatives such as 'No More Ransom' have already been set up, in which the police work across international borders with Europol and two major cybersecurity companies, to help ransomware victims unlock their data without paying a ransom.[47] One of the things they do is to provide 'decryptor' software, which renders certain types of ransomware harmless. Unfortunately, this does not solve the problem in all cases, whereby paying up can still appear to be a company's best option.

Given how potentially serious the financial consequences of not paying up can be for organisations, it is difficult to say whether governments should impose a legal ban on ransom payments. However, organisations that are victims of attacks do need to report them. Unfortunately, this does not happen often enough, because organisations are too afraid of any subsequent damage to their reputation. In cases where personal data may have been stolen, under the GDPR, organisations have to report this to regulators as a data breach within 72 hours.[48] However, this does not always happen, out for fear of damaging their reputations as mentioned above. Furthermore, there is no obligation to report ransomware attacks that do not involve stolen personal data. Therefore, there is a great need for a general obligation to report ransomware attacks and to enforce this strictly, to gain a better understanding of the scope of the problem and to motivate organisations to invest more time and money in prevention.

All organisations need to ensure they have their basic cybersecurity hygiene in order. By this, we mean that all basic cybersecurity measures have been taken. This includes things like setting strong passwords (with multi-factor authentication), updating software, installing virus scanners and making *back-ups*. It also involves measures in the physical world, for

46. D. Allen, 'A helping hand with a dirty trick: ransomware now offers helpdesks to victims', *TechRadar*, 14 April 2016, URL: https://www.techradar.com/news/internet/a-helping-hand-with-a-dirty-trick-ransomware-now-offers-helpdesk-to-victims-1319034, accessed: 26 October 2021.

47. No More Ransom, 'Over het project', URL: https://www.nomoreransom.org/nl/about-the-project.html, accessed: 26 October 2021.

48. European Parliament and Council, *Regulation (EU) 2016/679 (General Data Protection Ruling)*, Article 33, Brussels, 2016.

example, securely storing USB sticks that contain sensitive information. It is also wise to test the security-risk awareness of employees within organisations, by doing things like sending out test phishing emails and requiring anyone who clicks on them to follow training aimed at preventing this from happening in future. There is also added value in using 'ethical hackers'. These are hackers who are employed by organisations to hack into their systems to uncover vulnerabilities so that they can subsequently be addressed. Basic measures like these can mitigate many risks.

It is especially important for companies in critical sectors to have their basic cybersecurity hygiene in order. In the Netherlands, this duty of care is defined by law. Nonetheless, companies often neglect to do so. Research done by the television programme *Zembla* showed that no fewer than 43 out of 100 Dutch companies in critical sectors failed to meet modern security standards, leaving them vulnerable to cyber attacks. These included corporations like KLM, as well as a major nuclear power plant.[49] The government needs to monitor and enforce this much more strictly.

Members of the public also need to become more aware of the basic measures they should be taking. The government can play a major role in raising awareness. For example, by organising information evenings for the elderly and including cybersecurity in the school curriculum. Now that young people are engaged in the digital world from a tender age, it is of vital importance that they become aware of the risks and know what safety measures to take. This is part of digital literacy.

The public also needs to be made aware of the risks posed by certain internet-related products without having insufficient security measures in place. There are all kinds of 'smart products' with useful applications nowadays, however, these are often easy to hack. For example, criminals can hack into smart thermostats to see if they have been off for a few days and thus work out that you are probably on holiday. This is very appealing to burglars. They can even sometimes use one device to hack into another, thus managing to switch off your alarm system, for example.[50]

---

49. Zembla, 'Gehackt en gegijzeld' (documentary).
50. K. Kafle, 'A study of data store-based home automation', paper for the 9th Conference on Data and Application Security and Privacy, Dallas, 2019, p. 10.

Authors Maurits Martijn and Dimitri Tokmetzis point out that the safety standards required of products in the physical world rarely apply in the digital world. Products are often brought to market with all kinds of digital security defects that are only resolved through subsequent software updates. Meanwhile, non-digital products are required to undergo rigorous testing prior to sale.[51] This lack of digital security causes all sorts of security issues in the physical world too. The government must therefore insist upon much stricter safety requirements for products of this type. The European Commission has already announced measures that will be defined by law as of 2024, but it is important that these are actually enforced.[52] At the same time, people are increasingly importing products from non-EU countries that do not meet these safety standards. For example, many people buy cheap electronic products from Chinese online stores. They need to be made aware that these products often lack adequate cybersecurity, thus posing significant security risks.

All these protective measures are of great importance, but it is also necessary to be proactive. Liberals are committed to national security. Traditional security interests – such as nuclear non-proliferation – can also be safeguarded by digital means. For example, intelligence agencies are believed to have played a role in spreading a computer virus (the Stuxnet virus) within an Iranian nuclear complex.[53] Many of the centrifuges used to enrich uranium were ruined by this virus. This probably set the Iranian nuclear program back by several years. *Vice versa*, traditional security tools can also be used to defend digital security interests. This includes things like navy patrol units to prevent enemy submarines from tapping into or sabotaging submarine communications cables.

Many European countries have relatively strong digital capabilities. Still, this ongoing battle in the digital world, as yet, appears to be a mismatch, with democracies on the losing end. For example, government security agencies in democracies often have to contend with legislation that does

51. M. Martijn, D. Tokmetzis, *Je hebt wél iets te verbergen: over het levensbelang van privacy*, Amsterdam, 2018, p. 65.
52. Europa Nu, 'Commissie versterkt cyberveiligheid van draadloze apparaten en producten', 29 October 2021, URL: https://www.europa-nu.nl/id/vlngfy5dwivd/nieuws/commissie_versterkt_cyberbeveiliging_van?ctx=vim2bzqlxcsy, accessed: 2 November 2021.
53. Modderkolk, *Het is oorlog maar niemand die het ziet*, p. 58.

not apply to their authoritarian counterparts. Liberals insist that such legislation is critical to safeguarding the fundamental rights of citizens. For example, the right to privacy. Intelligence services are not allowed to eavesdrop on people without good cause. At the same time, security also needs to be guaranteed as a liberal value. In a society undergoing digitalisation, it is important to continually check whether these values remain in balance.

Cyber threats are putting a strain on society and this is only set to get worse in the future. Many European countries have legislation that allows the police and the judiciary to hack suspects in certain cases.[54] Special powers of this kind are usually subject to strict requirements and can therefore be justified from a liberal perspective. If we take the Netherlands as an example, we see that excessive bureaucracy actually reduces the power of government security agencies and is an impediment to intelligence gathering.[55] It can therefore take too long to deploy special powers. Lawmakers need to look at how to organise this process in a faster and more efficient manner, without compromising fundamental rights.

Capacity is also a bottleneck for many government security agencies. For example, organisations such as intelligence services, the Ministry of Defence, and the police, regularly face staff shortages in the cyber field. These organisations struggle to recruit the few highly educated people in this domain, as they are often better paid in the private sector. Experts warn of a discrepancy between the urgent need for greater digital resilience that governments claim to seek, and the actual investments they are making in the field.[56] These organisations have a structural

54. Rijksoverheid, 'Nieuwe wet versterkt bestrijding computercriminaliteit', URL: https://www.rijksoverheid.nl/actueel/nieuws/2019/02/28/nieuwe-wet-versterkt-bestrijding-computercriminaliteit, accessed: 3 November 2021; Edri, 'Swedish law enforcement given the permission to hack', 26 February 2020, accessed: 27 July 2023; 'New German surveillance law allows phone hacking', *DW*, 22 June 2017, URL: https://www.dw.com/en/new-surveillance-law-german-police-allowed-to-hack-smartphones/a-39372085, accessed: 27 July 2023.

55. Algemene Rekenkamer, *Slagkracht AIVD en MIVD. De wet dwingt, de tijd dringt, de praktijk wringt*, The Hague, 2021, pp. 63-67; Evaluatiecommissie Wiv 2017, *Evaluatie 2020. Wet op de inlichtingen- en veiligheidsdiensten 2017*, 2021, pp. 97-98.

56. 'Experts waarschuwen: budgetten cyberveiligheid niet realistisch', *RTL Nieuws*, 23 September 2021, URL: https://www.rtlnieuws.nl/economie/tech-business/artikel/5255799/kabinet-steekt-te-weinig-cyberveiligheid, accessed: 3 November 2021; Nextgov/FCW, 'Professionals across the globe agree: governments don't invest enough in cyber', 27 July 2016, ULR: https://www.nextgov.com/cybersecurity/2016/07/professionals-across-globe-agree-governments-dont-invest-enough-cyber/130272/, accessed: 27 July 2023.

need for funds to allow them to expand their cyber capabilities in the coming years.

As many cyber threats are international in nature, greater international cooperation is necessary. Many cybercriminals operate out of Eastern Europe. We can find and arrest these criminals by sharing information and intelligence with our partners. International police operations regularly take place that manage to catch ransomware gangs.[57] And, as we saw earlier, the EU now has its own Cyber Diplomacy Toolbox for imposing sanctions on countries that use cyber attacks on EU Member States (see section 4.5). Joint action of this sort has become essential in a digital world without national borders.

6.5 Conclusion

The focus of this chapter was digital security. It focused on the fact that European countries are in the process of digitalising and how this makes them vulnerable to cyber attacks. The threat this poses is not always immediately apparent because it is more abstract than other security risks. Nevertheless, a growing number of incidents in recent years have shone a light on the practical implications of these risks. Nevertheless, citizens and organisations often take inadequate security measures, putting both themselves and society as a whole at risk. Liberals draw upon the harm principle, and argue that the damage to society that this can cause legitimises government intervention. After all, the government's primary task is to ensure adequate security, including in the digital world.

A shift from traditional crime towards cybercrime is underway. Ransomware, phishing, and DDoS attacks are all frequent occurrences nowadays. There are four different types of actors behind these attacks: individuals *(lone wolves)*, hacktivists, organised criminal gangs and state (and state-sponsored) actors. The cyber domain is a new area in which state actors fight geopolitical battles. Hostile states carry out cyber attacks to steal money, obtain sensitive information and cause social disruption.

57. 'Nederlandse politie helpt internationale ransomwarebende op te rollen', *NOS*, 29 October 2021, URL: https://nos.nl/artikel/2403533-nederlandse-politie-helpt-internationale-ransomwarebende-op-te-rollen, accessed: 3 November 2021.

This disruption is able to happen because of vulnerabilities in our critical processes. Any interference can have major societal consequences. Digitalisation plays a major role in nearly all critical processes, making it vulnerable to cyber attacks. The dependency chain means that companies operating in critical processes can also be affected indirectly. Several incidents have already occurred in Europe. They have often caused major economic damage, but it seems only a matter of time before an incident occurs that causes serious disruption to the society in which we live. As well as cyber attacks, companies from rival or hostile states who supply products and services used for critical processes, are also of major concern. They can create unwanted dependency, as became clear in the discussions around 5G technology. Economic interests can run counter to the interests of the security of our society.

We need to improve the management of all these safety risks. This means that we need to increase our strategic autonomy and shield critical processes from unsuitable investment. Some economic interests can be accommodated within this risk assessment. In general, it is wise to have a range of suppliers when it comes to critical processes, in order to avoid being dependent on a single market party. It is also important to carefully examine other links in the production chain, such as software and hardware suppliers. However, when it comes to sharing information about cyber threats, there seems little value in making a distinction between the critical and non-critical. It is something that all organisations have to deal with nowadays and they all need to be properly informed.

We also looked at how ransomware has become a particularly serious problem in recent years and what a dilemma it can be for organisations to decide whether or not to pay a ransom. Payment doesn't guarantee an end to the trouble. And by paying up the problem is perpetuated. Nonetheless, many companies are tempted to pay up, especially, for example, it they think they will go bankrupt if they do not. Placing an outright ban on paying ransoms is not a straightforward matter, but organisations need to be more open about these types of attacks. A general obligation to report them, coupled with stricter enforcement, would create a better overview, and the risk of any reputational damage might also incentivise organisations to put greater efforts into prevention. In any case, organisations need to ensure that their basic cybersecurity hygiene

is in order. This is especially true for companies who operate in critical processes. And yet they often fail to do so. Therefore, this needs to be better enforced.

More public awareness is needed. Everyone needs to learn about the importance of cybersecurity from a young age, and this ought to be included in the school curriculum. Citizens must also be made aware of the risks of bringing all kinds of smart products into the home, as these are often not adequately secured. Better legislation is required here, so that the strict security standards we are familiar with in the physical world are extended to digital products. Members of the public also need to know that there are risks involved in importing products from countries like China, as they have different safety standards.

Our government security agencies can also play a role in prevention and detection. In the mandate, strict checks need to be incorporated to ensure that fundamental rights – such as privacy – are safeguarded. This means that we have to behave differently to our counterparts in Russia and China, who are barely restricted by legislation of this sort. Therefore, it is even more important to make sure the right balance is in place. For example, the administrative burden that restricts the use of special powers like hacking. More importantly, government security agencies need to be given more funds to address their cyber capacity shortcomings. The borderless nature of the digital world means that we need to continue to work with our international partners in matters of policy surrounding security and sanctions.

Society as a whole will need to do far more to ensure it is equipped to handle to digital threats. The stark rise in cybercrime means we need to get our security measures in order and keep them that way. If we drop the ball, enormous problems can arise, with huge implications both for individuals and society at large. It is important for liberals not to be naive and to take digital security threats more seriously.

7. A liberal governance strategy for digitalisation

7.1 The need for a broader vision

In the very first chapter of this book, we looked at how technology has led to radical change for both people and society, throughout history. This can only make us wonder about the sort of future new technological developments will bring. Besides providing entertainment, works of *science fiction* sometimes also offer genuine warning signs. In the first half of the 20th century, two authors published major novels outlining their contrasting visions for the future. They depicted two different, and more or less opposing, visions of what a dystopian society might look like.

In the novel *1948* (1949), George Orwell portrayed a world in which the government uses technology to observe and oppress individuals across all aspects of their lives. His is a totalitarian society, in which the state utilises a range of technologies to monitor groups of citizens at all times, and to clamp down on any form of dissent.[1] [2] If we put what this book has to say in the context of our current times, we can find parallels with the digital authoritarianism model, which we explored earlier in this book. Authoritarian regimes use digital technologies to control their citizens and hunt down dissenters. But there have also been incidents of far-reaching government surveillance in the West. Consider the United States, where the National Security Agency (NSA), assisted by large American tech companies, uses phone data on a large scale to

1. G. Orwell, *1984,* London, 2008 [1949].
2. The people from the '*Outer Party*' (middle class) are monitored by the '*Inner Party*' (upper class). The '*Proles*' (underclass) are viewed in the book as unworthy and apolitical and are therefore not spied upon.

spy illegally on its own population, as well as on people elsewhere in the world.[3]

The second novel is *Brave New World* (1932) by Aldous Huxley. In this book, technology is used to condition individuals from a tender age while they are also administered with drugs to suppress all negative thoughts. While in Orwell's work, submission is achieved through oppression, in Huxley's it is achieved by ensuring people's happiness. Individuals are ruled by temptation and encouraged to consume as much as they possibly can.[4] There are similarities between the world portrayed in this book and the surveillance economy described earlier, in which large tech companies use data to profile us before attempting to manipulate us psychologically, to retain our attention while showing us as many advertisements as possible, tailored to our individual needs.

Where Orwell and Huxley's visions coincide is that both believe that technology can be detrimental to individual freedom. Consequently, both novels retain their relevance to liberals today. Their perspectives are worth examining in the context of a socio-technological theme like digitalisation. Perhaps more importantly, novels like these, despite being works of fiction, ponder the impact of new technology on people and society on a macro level. When we look at digitalisation and its effects on society, we can see that politics often lacks a clear narrative rooted in values, in which we have a definite vision of what we want and what we don't want, as the world goes through this transition. Liberals are wary of excessive 'social engineering', but that does not mean that as a society, we should just stand back and let things happen to us. An overall strategic policy on digitalisation, taking liberal values as a premise, would benefit us greatly.

The previous chapters have focused on a particular theme, exploring the impact of digitalisation on the free market, democracy, the citizen-government relationship and security, through context-specific analyses and recommendations. The focus was two-fold, looking at legislation on the one hand, and awareness on the other. However, the sheer scope of digitalisation means that these measures need to be embedded

3. R. Satter, 'U.S. court: mass surveillance program exposed by Snowden was illegal', *Reuters*, 3 September 2020, URL: https://www.reuters.com/article/us-usa-nsa-spying-idUSKBN25T3CK, accessed: 13 January 2021.
4. A. Huxley, *Brave New World*, New York, 2004 [1932].

within a broader strategy. By this, we mean an overall *governance strategy*, to clarify how politics should deal with digitalisation and its impact on society at all levels. One that would account for the dynamic nature of digitalisation and ensure that specific measures were not invariably rendered obsolete, due to ongoing technological developments.

This chapter will explore what such a governance strategy should encompass. For example, everyone needs to be made aware of the legal validity in force in the digital world, and there is a need for the government to coordinate digitalisation policy centrally. Thought also needs to be given to how this should be regulated and how individuals might claim damages from parties who violate their rights. We also need to explore how innovation policy can be used to ensure strategic autonomy. Last but not least, we need to draw up a long-term strategy that anticipates future technological developments.

7.2 Legal validity and central coordination

Despite the growing interdependence between the digital and physical worlds, all too often the digital space continues to be viewed as a separate reality to which the laws and rules of the physical world do not necessarily apply. The ethicists Dean Cocking and Jeroen van den Hoven argue that in this respect, individuals sometimes experience a kind of 'moral fog' in the digital world, adhering to different norms and values because they feel less responsible and accountable. This can cause them to be insufficiently aware of the real-world consequences of their actions in the digital sphere.[5] For example, we have seen politicians increasingly receiving threats, mostly over social media. In retrospect, perpetrators often claim not to have understood the real-world impact of their words.[6] The public needs to develop a greater awareness of the fact that things that are illegal in the physical world are also illegal in the digital space. This will become increasingly important, as the boundary

5. D. Cocking, J. van den Hoven, *Evil Online*, Padstow, 2018, pp. 86-87.
6. 'OM-baas over bedreigingen: 'Mensen beseffen impact van hun woorden niet'', *NU.nl*, 30 October 2021, URL: https://www.nu.nl/binnenland/6164652/om-baas-over-bedreigingen-mensen-beseffen-impact-van-hun-woorden-niet.html, accessed: 17 January 2022.

between these two worlds is blurred through things like augmented and virtual reality (AR/VR).

This is also true of fundamental rights which also have legal validity in the digital world. There is currently much talk about the alleged need for new 'digital fundamental rights', but we wonder whether these specific fundamental rights are necessary at all and whether they are not already sufficiently covered by the current constitution. For example, a separate law to protect against discriminatory algorithms is not really necessary when the right to equal treatment is already embedded in the constitution. Indeed, it would only serve to reinforce the illusion that there is a different legal reality in the digital world.

What matters more is that we give careful thought to how existing fundamental rights should be interpreted within the current technological context. Some articles contained in the law will need to be partially amended, to make them future-proof. For example, in the Netherlands, the wording of an article in the constitution which covered the confidentiality of letters, telephone calls and telegraphs came to be obsolete. The reformulated article now refers to the confidentiality of correspondence and telecommunications, thus including digital means of communication within the scope of the article. Other European countries will also need to examine whether the text contained in of some articles in their constitutions need to be amended too. Matters such as the rights to privacy and to physical integrity need to be interpreted in the light of *deepfake* technology, which can be used, for example, to produce 'revenge porn' videos.[7] It may not be necessary to reformulate the existing article in the law, but the case law addressing this problem needs to be clearer. Although civil rights may sometimes need to be reinterpreted in the context of technological developments, they still have legal validity in the digital world.

This also holds true for the government, whose key role in the physical world also applies in the digital sphere. For too long, the internet has been viewed as merely a private infrastructure beyond the public interest. As we saw in the previous chapter, security is a government responsibility that needs to be handled better in the digital world. The government

7. Some 96 percent of online deepfake videos are pornographic. See: Deeptrace, *The State of Deepfakes. Landscapes, Threats and Impact*, Amsterdam, 2019, p. 1.

needs to impose safety measures in the digital world, in much the same way that it ensures safety on public roads by enforcing speed limits. But, not only does it need to guarantee security, it also needs to protect other civil rights like freedom of expression, so that there can be space for differences of opinion on the internet (see section 4.3).

In this respect, the digital world needs to be considered a public space, where liberal values prevail over commercial interests, whenever there is a conflict between the two. The government must also enforce online the laws and regulations that allow individuals to move freely and safely through this space. After all, this is the foundation of the social contract between citizen and government. There is no reason to think this should be any different in the digital sphere. However, liberals believe that the government should limit itself to these core tasks and not abuse its mandate by intervening more than necessary. What matters is for the government to guard the digital boundaries within which fundamental rights will always be guaranteed.

Within this public space, the government must protect individuals from i) companies operating in the surveillance economy (see Chapters 3 and 4), ii) its own ambitions in the digitalisation sphere (see Chapter 5), and iii) other state and non-state threats (see Chapters 4 and 6). In this context, the government needs to be aware of when public-private interaction is appropriate or not. We have previously looked at two cases where this went wrong in the USA. In one, the NSA was shown to have collaborated with many large American tech companies for espionage purposes. This is an example of what should be considered from a liberal perspective to be an inappropriate public-private partnership, because it violated the privacy of citizens.[8]

But the opposite can also be true. We also looked earlier at the ransomware attack on oil transport company Colonial Pipeline, which caused fuel shortages in the USA. This ransomware attack did not shut down the entire company, but only its payment system, so it should still have been possible to deliver oil products.[9] However, the company chose not

8. Not only were these espionage practices illegal in themselves, but the fact that tech companies were so actively involved in government surveillance was especially shocking.
9. N. Bertrand et al., 'Colonial Pipeline did pay ransom to hackers, sources now say', *CNN*, 13 May 2021, URL: https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html, accessed: 22 February 2022.

to do so as it was unable to receive payment from its customers. As such, the company's financial interests trumped the public interest in having an adequate, country-wide fuel supply. From a liberal perspective, some degree of public-private partnership would have been appropriate here, to ensure that a critical process was not shut down due to commercial interests. The government needs always to maintain a clear overview of whether public-private interaction is appropriate or not, by looking at whether it upholds or detracts from liberal values.

The government will also need to establish a clearer organisational structure before it can arrive at a more effective digitalisation policy. As digitalisation occurs in almost all areas of policy, responsibility for it has been fragmented across all the various ministries for a long time. This is inevitable when it comes to the detail, since every ministry uses digitalisation in department-specific ways. Nevertheless, the broad terms of this policy need to be coordinated and the various ministries need to be provided with guidelines. We would therefore recommend coordinating governance strategy centrally. Although several European countries have now set up a separate ministry of digitalisation, this is not yet the case in all countries. Nevertheless, given the impact of digitalisation on society, this would be justified. A ministry of this kind could ensure better coordinated, cross-departmental digitalisation policy.

Central coordination would ensure better leadership, so that the urgency of establishing an appropriate digitalisation policy isn't just discussed, but actually put into practice. This doesn't relieve other ministries of all responsibility for their own particular digital applications. But by looking to establish broad outlines, we could reflect at a more abstract level on the extent to which digitalisation policy adequately guarantees liberal values. A central vision providing certain common guidelines would be a way of counteracting the compartmentalisation of policy that currently exists across the various ministries. This would work both horizontally and vertically. A central coordination point within the government would be a means of ensuring consistency across all the different levels of government, i.e. at local, national and European level.

As we saw earlier in this book, the borderless nature of digitalisation necessitates good partnerships with other countries. Digitalisation has developed into a new branch of diplomacy and it is useful for the

government to have dedicated government officials to represent it at international consultation forums. It also makes it possible to engage in dialogue not only with our direct partners, but also with countries that threaten to go down the path of digital authoritarianism (see section 4.1). This is all the more important, given that over the coming years there will be a demographic shift on the worldwide web, with increasing volumes of internet users coming from developing countries, especially Africa and Asia, in addition to those from the already saturated West.[10]

Last but not least, we would like to emphasise that although many digitalisation challenges need to be addressed at European level, we do not believe that every policy issue should by definition be referred immediately to the EU. Local and national politicians should always begin by looking at which steps can be taken close to home first, if only because they can trigger further steps at European level. This aligns with the principle of subsidiarity on which the EU is based and which is important to liberals, who believe that decisions should always be taken as close to the citizen as possible.

7.3 Regulation and damage claims

In the preceding chapters, we saw in several instances the need for strong regulation. Many countries have various regulators involved in digitalisation nowadays. However, critics point to a range of issues resulting from there being too many regulators in the digitalisation arena. Professor Corien Prins, for example, emphasises that these regulators are not democratically elected. Not only do they regulate, they often have a strong influence on the regulations themselves. As legislation on digitalisation – such as the GDPR – often has open standards (so as not to become irrelevant in the light of new technological developments), such legislation is often fine-tuned by the way in which the regulators themselves interpret and enforce this legislation.[11] This results in regulators

10. Wetenschappelijke Raad voor het Regeringsbeleid, *De publieke kern van het internet. Naar een buitenlands internetbeleid*, Amsterdam, 2015, p. 24.
11. C. Prins, 'Toezichthouders en publieke verantwoording', *Nederlands Juristenblad*, 22 June 2021, URL: https://njb.nl/blogs/toezichthouders-en-publiekelijke-verantwoording/, accessed: 20 January 2022.

playing an indirect role in shaping the law without being subject to any public accountability mechanisms. Large numbers of regulators can only make this democratic shortcoming worse and undermine the role of the legislature within the political system. Algorithm specialist, Frank van Praat, argues that another problem is that regulators act reactively, while digitalisation often requires proactive regulation. After all, you want to prevent incidents from happening and not only understand them once they have occurred.[12]

To ensure this happens, we need to think about whether there are other ways of carrying out regulation. For example, we could look into whether there is a role for 'system monitoring' for certain companies. Consider a bank or healthcare provider that uses data and algorithms. When doing so, such companies assume responsibility by setting up internal quality and risk management systems. Then regulators need no longer look at all individual incidents, they just have to see if the internal monitoring system is in order. It is therefore based on organisation-level responsibility. This can be combined with a form of tiered transparency by independent third parties (as previously discussed in section 5.3). This ensures a more scalable regulatory model, linking transparency with accountability. Additionally, this means that companies end up bearing a significant part of the costs of regulation themselves, rather than them being exclusively funded by the taxpayer (who provides the tax money to fund the government regulators).

When it comes to algorithms, the government should also consider creating a public register of algorithms. An initiative of this sort has already been set up in the Dutch city of Amsterdam (although it is still under development). In this case, it also aligns nicely with the two-fold requirements of 'explainability' for the average person on the one hand, and technical insight for experts on the other (see section 5.4). The register contains information stated in clear language about the purpose of the algorithm, the data it uses, and how it mitigates risk. In addition, it also often contains links to technical details such as datasets and source

12. F. van Praat, 'Blaffende waakhonden bijten te laat voor toezicht op algoritme', *AG Connect*, 26 January 2022, URL: https://www.agconnect.nl/blog/blaffende-waakhonden-bijten-te-laat-voor-toezicht-op-algoritme, accessed: 22 February 2022.

codes.[13] This enables citizens to exercise regulation themselves. Other municipalities (and organisations) could also set up public algorithm registers in this way.

Finally, we would like to emphasise that regulation, and its supporting legislation, should not focus exclusively on the technology itself, but on its potential consequences for the people who use it. In the Dutch childcare benefits scandal (see section 5.3), the damage inflicted upon the victims ultimately arose not from the algorithm itself, but from the actions that followed subsequently – false accusations of fraud and the recovery of money. It is therefore necessary to look at whether clear frameworks for action exist within organisations that also allow scope for professional autonomy. These should not rely blindly on the assessments of digital systems and should dare to shut them down as soon as discrimination or other unwanted side-effects are suspected.

Furthermore, as we recommended earlier in this book, regulators need to be empowered to hand out large fines, otherwise big tech firms in particular might choose to ignore regulations. Fines would need to be high enough to really hurt tech companies' bottom line. From a liberal perspective, it would also be good to look into how individuals might gain the ability to hold liable parties (market parties, but also the government) to account and potentially claim damages in cases of misuse. Digitalisation often involves small but 'scattered' damage. By this we mean a form of mass damage that is minor on an individual level, but when it affects a large number of individuals, it is significant when added together. This includes data breaches resulting in the personal data of thousands of people being exposed. Personal data is of minor value at the individual level, so individuals cannot easily claim damages on an individual basis. We also see the harm caused by companies that compile and sell data profiles to third parties without permission.

While the United States has a long tradition of large-scale '*class action*' lawsuits, this has not usually been the case in Europe. However, this looks set to change following the adoption of the EU's 2020

13. Gemeente Amsterdam, 'Amsterdam Algoritmeregister Beta', URL: https://algoritmeregister.amsterdam.nl/, accessed: 22 February 2022.

Representative Actions Directive (RAD).[14] This stipulates that EU Member States must introduce legislation surrounding *class action,* allowing interest groups to recover damages from guilty parties on behalf of larger groups of victims. In many countries in the past, victims have only been able to take legal action on an individual basis. As a result, compensation has rarely exceeded legal costs. Legislation specifically designed for *class action* cases now permits interest groups to file compensation claims on behalf of groups of victims. This prevents vast numbers of smaller lawsuits and makes it possible for individuals to file claims for damages on a collective basis. Thus, it has suddenly become worth pursuing legal action for scattered damage. However, there are requirements for interest groups in terms of representativeness and transparency.

Within Europe, the Netherlands now seems to be at the forefront when it comes to *class action* cases, with various damage claims filed against large tech companies including Apple, TikTok and Google, as well as against the Dutch state.[15] These are sometimes claims for billions of euros, which reveals the potential of this legislation, because damage claims of this amplitude can act as a deterrent for guilty parties. What is interesting from a liberal perspective, is that individuals, regardless of their expertise or financial means, may now be able to enforce a level playing field inside the courtroom, which is not the case in the outside world. It is there important to keep an eye on what future case law will yield and how far class action legislation may function as an instrument to enable individuals to better stand up for their rights in the digital world.

7.4 Innovation policy and European strategic autonomy

Earlier in this book, we looked at the importance of strategic autonomy. This protects against vulnerability and allows us to protect our interests

14. European Union, *Directive (EU) 2020/1828 on Representative Actions for the Protection of the Collective Interests of Consumers*, Brussels, 2020.

15. De Rechtspraak, 'Centraal register voor collectieve vorderingen', URL: https://www.rechtspraak.nl/Registers/centraal-register-voor-collectieve-vorderingen#6f1c15a9-f3e8-4b9b-ab79-4b3bb766c72f6bc1d2e4-e511-4e04-bf16-8ad720b8f8b332, accessed: 24 January 2022.

as best we can. We saw the need to safeguard against economic investments and acquisitions from countries that do not share our geopolitical interests. Strategic autonomy can be achieved not only on the demand side (by fending off unwanted parties), but also on the supply side. We can achieve this by stimulating innovation, so that home-grown market parties develop into relevant market players. Digitalisation innovation policy should therefore form a major part of our governance strategy. This is something that we can currently see reflected in the power struggle between the United States and China, where technological supremacy is seen as a critical factor in geopolitical world dominance.

It is disappointing that the EU is so far behind in this area. Only one of the 20 largest tech companies in the world is European (the Dutch ASML). The top 100 is also completely dominated by American and Asian market parties.[16] There are not many European tech companies, despite the fact that the EU was until recently the world's second largest economy (it has now been overtaken by China). More and more voices within the EU are expressing concern about the state of affairs in this respect, saying that we need more focus on improving technological sovereignty.[17] We have to ask ourselves how we should achieve this European sovereignty and what role individual countries should play within it.

It is exactly a policy like this that could ensure a type of innovation that emphasises safeguarding liberal values. The government could enforce certain concrete standards for this. Consider investment in so-called '*privacy enhancing technologies*' (PET). These are technologies designed from the outset to guarantee user privacy by processing minimal personal data. A good example of this is the French search engine Qwant, which does not collect any personal user data at all.[18] There are also companies that focus specifically on explainable algorithm technologies. Investing in '*open-source*' software and hardware products can also help ensure the safeguarding of liberal values. These are products

16. Companies Market Cap, 'Largest tech companies by market cap', URL: https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/, accessed: 2 February 2022.
17. S. Caravella et al. 'European technological sovereignty: an emerging framework for political strategy', *Intereconomics*, 2021, no. 6, p. 348.
18. Qwant, 'Over ons', URL: https://www.qwant.com/?l=nl&drawer=awareness, accessed: 23 February 2022.

for which the design is freely available to everyone, thereby providing complete transparency regarding their operations. Not only are these beneficial to liberal values, but a European Commission report revealed that the 1 billion euros that European companies invested in *open source* in 2018 yielded a profit of between 65 and 95 billion euros for the European economy.[19]

As many other Member States as possible need to adopt these standards for their investment policy, as this will motivate companies to align their innovation with these standards. Indeed, when it comes to international standardisation, a race is currently unfolding in which China in particular is trying to influence the formation of new norms and standards for digital technologies.[20] This makes it all the more important for the EU to draw up a clear standardisation strategy and for the Member States to adhere to it. However, this strategy needs to be grounded in liberal values and not just become a disguised form of protectionism for the economic interests of individual Member States (this is also necessary to prevent internal conflicts).

When it comes to our innovation policy we need to look beyond the amount of money invested, to where exactly it ends up and how it supports innovation in the broadest sense. A report by the Dutch Cyber Security Council (CSR) shows that while the EU invests in important academic research, it provides far less support to innovation in the business sector. There are too few connections between academic research centres and industry. The CSR is also of the opinion that EU funding focuses too heavily on vested interests, with insufficient room for market disruption.[21] This runs counter to liberal ideas which hold that creative destruction is essential to a healthy free market.

---

19. K. Blind, *The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy*, European Commission report, Brussels, 2021, p. 14.
20. B. Groothuis, L. Schreinemacher, 'Parlementaire vragen – Betreft: Wedloop op het gebied van technologische standaardisatie', *Europees Parlement*, 15 December 2021, URL: https://www.europarl.europa.eu/doceo/document/E-9-2021-005572_NL.html#def1, accessed: 9 March 2022.
21. F. Dezeure, P. Timmers, *Nederlandse strategische autonomie en cybersecurity*, Cyber Security Raad report, The Hague, 2021, p. 25.

It is also worth noting that companies outside the EU often do manage to find their way to academic research centres.[22] The pitfall of this is that academic research gets financed by high-risk parties. A recent example of this is the commotion around two Amsterdam universities partnering with Huawei for research into AI. All the more so because Huawei also supplies technologies of this sort to oppress the Uyghurs in China[23] Therefore, governments need to develop guidelines for situations like this to ensure scientific integrity and prevent collaboration with unwanted parties.

The government must also act as a link between academia and business. Drawing upon this idea, we have seen a range of public-private partnerships emerge in recent years at both national, as well as European level. The GAIA-X project, for example, is working to create data storage and *cloud* infrastructure within the EU, based on values such as decentralisation, data protection and transparency.[24] The Important Project of Common European Interest Cloud Infrastructure and Services (IPCEI-CIS) is an extension of this. However, we have seen how such European projects can suffer as a result of political division. If we really want projects like this to get off the ground, we need to have clarity and consensus among the Member States about their precise objectives.[25]

Another crucial factor when it comes to innovation is the availability of adequate *venture capital* in the market. This means high-risk investments in companies that are often still in the start-up phase. The risk is bigger that the company fails, for investors stepping in at such an early stage. At the same time, the growth potential and potential return on investment are much greater too. Venture capital investment is needed to bring companies of this type to the *scale-up* stage that follows. Scale-ups

22. R. Brennenraedts et al, *Het Nederlandse investeringsklimaat*, Dialogic report, Utrecht, 2021, pp. 32-33.
23. 'Wetenschappers tegen samenwerking Amsterdamse universiteiten en Huawei', *NOS*, 15 October 2022, URL: https://nos.nl/artikel/2352470-wetenschappers-tegen-samenwerking-amsterdamse-universiteiten-en-huawei, accessed: 24 February 2022.
24. Gaia-X, 'Who are we?', URL: https://www.gaia-x.eu/who-we-are/association, accessed: 4 February 2022.
25. A. Monterie, 'Politieke onduidelijkheid fnuikend voor Gaia-X', *Computable*, 2 November 2021, URL: https://www.computable.nl/artikel/achtergrond/infrastructuur/7267654/1444691/politieke-onduidelijkheid-fnuikend-voor-gaia-x.html, accessed: 23 February 2022.

also need venture capital investment to continue to grow and, if possible, achieve coveted '*unicorn*'-status (a market valuation in excess of 1 billion dollars). Rapid growth matters in the tech sector, in part because most tech companies only become profitable once they have reached a certain size. Access to sufficient venture capital is essential for them to get this opportunity.

When we compare the situations in Europe and the United States, we see that Europe has been falling short for a long time. The CRS report states that there is as much as three times more venture capital available for the tech sector in the USA. There is also more focus on growth over immediate profit. Investors have a longer term vision and are willing to accept more risk. At the same time, investors are more willing to pull the plug on companies that fail to reach agreed targets, leading to a much more dynamic market. Moreover, in the US, there is more interaction between different companies and it is easier for start-ups and scale-ups to get help.[26] This is why many European tech companies choose to leave to the USA at an early stage. Not only because there is more money to be made there, but also because the entire innovation ecosystem there is better set up.

For example, European pension funds only made around 450 million euros (0.012 percent of their total assets) available to venture capital investments in 2021.[27] A significant increase in venture capital funding could have a very positive effect on the European tech industry. In general, European investment in the tech sector is increasing. For example, in 2021, European countries invested more than $100 billion in the tech sector, equalling the US for the first time.[28] It is therefore important to ensure that a substantial part of these funds end up as venture capital for start-ups, and especially scale-ups. While, in recent years, it has become easier to raise start-up capital in Europe, it still proves a challenge to raise the large-scale investments required for scale-ups.[29] Furthermore,

---

26. Dezeure, *Nederlandse strategische autonomie en cybersecurity*, pp. 30-32.
27. State of European Tech, 'Investors', URL: https://stateofeuropeantech.com/4.investors/4.1-fundraising, accessed: 28 July 2023.
28. 'European tech industry is on track to reach $100B invested in single year: The State of European Tech 2021 report', *Silicon Canals*, 8 December 2021, URL: https://siliconcanals.com/news/startups/european-tech-100b-investment/, accessed: 4 February 2022.
29. H. Hueck, 'Europees groeikapitaal breekt in 2020 alle records', *Het Financieele Dagblad*, 29 October 2020, URL: https://fd.nl/futures/1362382/europees-groeikapitaal-breekt-in-2020-alle-records, accessed: 24 February 2022.

these investments need to be embedded in a strong innovation ecosystem, ensuring a good exchange of ideas.

Added to this, we should also look into the government taking on the role of '*launching customer*'.[30] After all, the government uses all sorts of digital applications and can foster their development by presenting itself as a client to innovative start-ups and scale-ups. Companies can grow faster when they have a large customer like this from a very early stage, in part because it makes them more attractive to other potential clients. The government can set a good example by choosing companies that take values such as privacy, autonomy and security as a premise for their products.

Finally, it is important to continue investing in ICT training. There have been staff shortages in this area for years. Not only does this hold back the tech sector, but it holds back the economy as a whole. It limits the abilities of other companies to make the digital transitions they need.[31] As society continues to digitalise, there is a growing need for more people to take up careers in ICT. Retraining can play an important role in plugging the gap. The government is currently trying to facilitate this by making grants available to people who want to retrain in ICT.[32] Companies can also look at whether they can provide training opportunities themselves, thus finding their own solutions to the ICT staff shortages.

7.5 The development of a long-term strategy

While it is not possible to predict technological developments, we do know that we will be confronted with new technologies that will have long-term, far-reaching consequences for society. Politicians need to

30. P. van Boheemen, *Cyberweerbaar met nieuwe technologie. Kans en noodzaak van digitale innovatie*, Rathenau Instituut report, The Hague, 2020, p. 68.
31. 'Tekort aan ict'ers remt bedrijvengroei', *Computable*, 30 September 2021, URL: https://www.computable.nl/artikel/nieuws/carriere/7251826/250449/tekort-aan-icters-remt-bedrijvengroei.html, accessed: 7 February 2022.
32. Sociaal-Economische Raad, 'Nieuwe subsidieregeling maakt omscholing naar ICT en techniek mogelijk', 12 October 2021, URL: https://www.ser.nl/nl/actueel/Nieuws/subsidie-ict-techniek, accessed: 4 February 2022.

anticipate this. In this section, we will look at developments which we haven't yet mentioned and briefly explain the dilemmas they may present from a liberal perspective. By thinking about them ahead of time, we can prevent society from becoming overwhelmed at a later stage. Although we cannot hold technological developments back, we can guide the way we use them in the right direction. It would be a good idea for politicians to work with special committees, focus groups and other circles of expertise to give serious thought to how they might achieve this.

For example, '*quantum computers*' are now being developed worldwide. These are computers that work on the basis of quantum mechanics. This complex technology allows these computers to perform extremely fast calculations. Many times faster than conventional computers.[33] Therefore, quantum computers have enormous potential for all kinds of applications. They would allow very detailed simulations to be made. This includes things like mapping particular molecules, on the basis of which new drugs could be developed. They would enable GPS systems to be much faster and more accurate. A worldwide race is currently playing out between large tech companies like Google and Microsoft, as well as Chinese parties, to get the first quantum computer operational for such applications.

But there is a major concern when it comes to this technology. They will be able to defeat many current forms of encryption. The unprecedented computing power of quantum computers will make it quite easy to open encrypted messages by working out the lock code. This will have major consequences, because a lot of information will cease to be secure. This will include state secrets stored in the systems of our security services. But the trade secrets of companies are also at risk. Furthermore, the access codes for critical processes could also be cracked. It seems that the first real quantum computer applications are still several years away. Nevertheless, the government, industry and other organisations already need to start thinking about how to mitigate this risk. It is particularly important to invest in the development of 'post-quantum cryptography',

33. See the following video for a clear explanation of how quantum computers work: Bright, 'Deze computers gaan de wereld veranderen', *YouTube*, 6 March 2019, URL: https://www.youtube.com/watch?v=wqFOFAY4OQo&ab_channel=Bright.

to allow information to continue to be securely encrypted. The development of the so-called 'quantum internet' could potentially enable secure forms of communication.

A second development that is coming our way is what is known as the '*metaverse*'. This is an AR/VR-based digital space displayed three-dimensionally, in which individuals can move around freely. By putting on special VR glasses, you can find yourself alongside other people in a shared virtual space, where you can do all sorts of everyday things like shopping or going to parties. You can also have meetings with associates and colleagues. For example, an office would be able to create a virtual workplace where employees could meet one another, while in reality they would be working from home. Some people go as far as to call the metaverse the next stage of the internet, where the internet will literally manifest itself around us, instead of being something we observe through flat screens as we do today.[34] Although different types of metaverse are already in existence, the big tech companies are expected to bring this technology to the next level. Facebook demonstrated its ambitious plans to build a metaverse when it changed its name to Meta in 2021. Microsoft is running a similar initiative called Mesh and the other major market players are also working on their own ideas for the metaverse.[35]

The metaverse will further blur the dividing line between the physical and digital worlds. Recently, the country of Barbados even announced the opening of a virtual embassy in one of the current metaverses.[36] This only reinforces the perspective we highlighted earlier, in which the internet is more of a public space, rather than a separate, stand-alone reality. However, this is not always self-evident, especially in the legal sphere.

34. See the following video for a visual representation of the metaverse: BBC, 'What is the metaverse', *YouTube*, 20 December 2021: https://www.youtube.com/watch?v=V6Vsx-cVpBVY&ab_channel=BBCNews.
35. K. Leswing, '2022 will be the biggest year for the metaverse so far', *CNBC*, 1 January 2022, URL: https://www.cnbc.com/2022/01/01/meta-apple-google-microsoft-gear-up-for-big-augmented-reality-year.html, accessed: 9 February 2022.
36. A. Thurman, 'Barbados to become first sovereign nation with an embassy in the metaverse', *CoinDesk*, 15 November 2021, URL: https://www.coindesk.com/business/2021/11/15/barbados-to-become-first-sovereign-nation-with-an-embassy-in-the-metaverse/, accessed: 24 February 2022.

For example, there was recently uncertainty concerning the legal validity of the marriage of a couple who got married online.[37] Discussions of this kind are also currently playing out as to whether virtual sexual assault is a criminal offence or not. Additionally, virtual objects and pieces of land are being sold nowadays which is raising questions about property rights. From a liberal perspective, the metaverse also raises issues when it comes to the privacy of citizens. As individuals increasingly live their lives in virtual spaces, large tech companies are finding opportunities to collect even more of their personal data. The fact that Facebook, which has a questionable reputation in matters of privacy, wants to be at the helm of this development, must be cause for some scepticism among policymakers.

One technological development already underway, the long-term impact of which will only grow, is the emergence of *cryptocurrencies*. Digital currencies that use '*blockchain*'-technology, to verify and record transactions in a decentralised system of interconnected computers,[38] [39] without the need for a bank. This gives individuals greater autonomy when making transactions. Furthermore, as digital identity is disassociated from physical identity, it allows users to remain anonymous. No transaction fees have to be paid to any intermediaries and transferring money to other countries is fast and cheap. Many people view cryptocurrencies as an alternative to the traditional financial system (in which they have lost lot of confidence). The better-known cryptocurrencies include Bitcoin and Ethereum.

However, cryptocurrencies have shown themselves to be highly volatile and, as such, they present a major risk to investors. Cryptocurrencies are still currently seen as a speculative investment and are not

37. 'Stel getrouwd in de metaverse: bindend of niet?', *RTL Nieuws*, 7 February 2022, URL: https://www.rtlnieuws.nl/tech/artikel/5286369/metaverse-huwelijk-decentraland, accessed: 9 February 2022.

38. See the following video for a short explanation of how cryptocurrencies work: BBC, 'Bitcoin explained: how do cryptocurrencies work?', *YouTube*, 12 February 2022.

39. Blockchain technology alongside cryptocurrencies can also serve as a foundation for other applications. In would allow the entire Internet to be organised in a decentralised manner. See: 'Web3 komt eraan: hoe gaat het internet veranderen?', *RTL Nieuws*, 17 February 2022, URL: https://www.rtlnieuws.nl/tech/artikel/5286548/web3-dao-bitcoin-nft-metaverse.

widely accepted as means of payment. This may change in the longer term as cryptocurrencies become increasingly integrated into the traditional financial system. In 2021, for example, El Salvador became the first country in the world to use Bitcoin as legal tender.[40] For as long as the value of cryptocurrencies remains volatile, there is a risk that this volatility will spread to the rest of the economy, with disastrous consequences.[41] The anonymity of cryptocurrency means it's a good way for criminals to launder money and get rich themselves, which is not desirable from a security perspective. Cryptocurrencies also provide a means for regimes like North Korea to circumvent sanctions. Above all, they provide cybercriminals with a convenient way to extort money, for example, through ransomware attacks, as we saw earlier in this book. The owners of cryptocurrency also face cybersecurity risks, because the digital wallets in which they are stored can be hacked, causing them to lose all their cryptocurrency. Finally, some cryptocurrencies such as Bitcoin generate enormous amounts of CO_2 emissions, because they are highly energy-intensive.[42] Cryptocurrencies obviously provide society with a great number of dilemmas, which politicians need to be conscious of.

The emergence of automated and autonomous technology means that we are dealing increasingly with '*robotisation*'. Robots are going to carry out more and more work that was traditionally done by humans, with major consequences for the labour market. The use of robots is a solution for sectors in which there are labour shortages. For example, robots are already being used for certain tasks in elder care.[43] But self-driving cars

40. W. Boonstra, 'Waarom El Salvador de deur opende voor de Bitcoin', *Rabobank*, 31 December 2021, URL: https://www.rabobank.nl/kennis/s011220522-waarom-el-salvador-de-deur-opende-voor-de-bitcoin, accessed: 10 February 2022.
41. 'Bank of England says crypto's rapid growth could pose stability risks', *Bloomberg*, 13 December 2021, URL: https://www.bloomberg.com/news/articles/2021-12-13/boe-says-rapid-growth-of-crypto-could-pose-stability-risks, accessed: 10 February 2022.
42. 'Beter zicht op klimaatimpact Bitcoin', *De Nederlandsche Bank*, 13 January 2022, URL: https://www.dnb.nl/actueel/algemeen-nieuws/dnbulletin-2022/beter-zicht-op-klimaatimpact-bitcoin/#:~:text=Niet%20alle%20crypto's%20zijn%20gebaseerd,functionaliteit%20die%20momenteel%20beschikbaar%20zijn, accessed: 10 February 2022.
43. See the following video for a demonstration of this care robot: NOS Jeugdjournaal, 'Gaat deze robot straks voor je opa of oma zorgen?', *YouTube*, 13 November 2019, URL: https://www.youtube.com/watch?v=Kg8xEcxJa4s&ab_channel=NOSJeugdjournaal.

and lorries are also robots, and in the future, we will increasingly see them on the roads. This will make transport and travel easier, as well as significantly reducing road casualties, by preventing human error. The Ministry of Defence is also looking at how robots can be used in conflict situations.[44]

Robotisation will make a number of professions redundant, or change their nature to such an extent that they will require different skills. This will impact the job security of large groups of people. These people will probably have to retrain in order to remain self-reliant, which is something that matters to liberals.[45] Robotisation also raises various ethical issues. For example, should autonomous weapon systems be allowed to make life-or-death decisions? Self-driving cars will also become problematic if they cause fatalities. A well-known moral dilemma for self-driving cars is whether to choose to crash the car to save a child who has suddenly darted out into the road, or save the passengers by driving on and hitting the child. Which decision should a machine make and who is legally responsible for that decision? At the same time, self-driving cars could substantially reduce road fatalities. So is maintaining human autonomy and responsibility more important than limiting the number of road fatalities? These are matters which society, and therefore politics, will need to address in the years to come.

In the longer term, we will see increasing applications of '*human enhancement technologies*'. These are technologies which alter our physical and mental characteristics for the better. This may sound like the stuff of science fiction, but they are already a reality to some extent[46] For example, in China, CRISPR-Cas9 technology was used (illegally) to genetically engineer two babies to make them HIV resistant.[47] Tech-

44. Adviesraad Internationale Vraagstukken en Commissie van Advies inzake Volkenrechtelijke Vraagstukken, *Autonome wapensystemen. Het belang van reguleren en investeren*, The Hague, 2021, pp. 47-51.

45. In this context, the TeldersStichting recently published the book *Flexibiliteit en zekerheid. Naar een gelijk speelveld op de arbeidsmarkt* (2019).

46. These subjects are also key to the book *Gen-ethische grensverkenningen. Een liberale benadering van ethische kwesties in de medische biotechnologie* (2010) by the TeldersStichting.

47. B.C. van Beers, 'Rewriting the human genome, rewriting human rights law? Human rights, human dignity, and human germline modification in the CRISPR era', *Journal of Law and the Biosciences*, 2020, no. 1, p. 2.

nology like this could cure genetic diseases, but also potentially adjust things like intelligence and skin colour. Neurotechnology is another interesting human enhancement technology. While computers – in the form of smartphones – are already as good as extensions of ourselves, it is entirely possible that in the future we will have them literally implanted in our brains. Companies like Neuralink are focusing on the development of brain implants of this sort.[48] The current intention is to remedy neurological disorders like paralysis, but in the long termer they may be put to all kinds of other futuristic uses, including potentially enhancing certain cognitive functions.

Exactly what such technologies will achieve in the future remains uncertain. However, it would be unwise to fail to prepare now for the societal implications of breakthroughs in the development of these technologies. Human enhancement technologies raise all kinds of issues, especially on an ethical level. Equal opportunities are very important to liberals, who believe that individuals should have the opportunity to develop themselves to the best of their abilities. Should these technologies only become available to the most affluent due to the costs involved, this will greatly increase the inequality of opportunity in society. There could be a dichotomy within society between 'ordinary' and 'improved' people. From a liberal perspective, a further dilemma arises from the consequences of placing computers in our brains when it comes to our privacy and autonomy. Imagine unwittingly observing and manipulating the functioning of someone's brain. Dependency on suppliers for the maintenance of this type of technology might also become an issue.[49] There are also security risks arising from criminal hackers breaking into brain computers of this sort. Although science fiction scenarios like these are unlikely to become reality in the near future, it would be wise

48. See the following video for further explanation about how brain implants work: Bright, 'Hersenen hacken: is Elon Musk wel goed bij zijn hoofd', *YouTube*, 13 Augustus 2019, URL: https://www.youtube.com/watch?v=GF1XHFpcKO4&t=1s&ab_channel=Bright.

49. We are already seeing this happen. For example, several people with bionic eyes are at risk of becoming blind again because the manufacturer is in financial difficulties and can therefore no longer provide maintenance. See: 'Bionisch oog krijgt geen updates meer: Jeroen dreigt weer blind te worden', *RTL Nieuws*, 18 February 2022, URL: https://www.rtlnieuws.nl/tech/artikel/5289145/second-sight-bionisch-oog-jeroen-perk, accessed: 14 February 2022.

to establish frameworks for the direction we want these technologies to take while they are still in the development phase.

7.6 Conclusion

This final chapter looked at how digitalisation policy could be embedded within an overall governance strategy, based on liberal values. We have seen the importance of considering digitalisation at a macro level. Developments in the digitalisation sphere can definitely be steered to some level without getting bogged down in unrealistic ideals of feasibility. Whilst in previous chapters, we always included context-specific recommendations and analyses, this chapter touched upon various points we can use in a broader strategy, to ensure that liberal values serve as the premise for policy. This will help us deal better with the dynamic nature of digitalisation.

First and foremost, it needs to be made clear that the laws and rules that apply in the physical world also apply in the digital world. Threats that are made on social media, for example, are also punishable by law. In this sense, the call for new digital fundamental rights is unnecessary, because they are usually already covered in a country's existing constitution. However, we need to give some thought to the interpretation of fundamental rights in the current technological context. Some articles may need to be amended or updated by lawmakers, or there may be a need for clearer case law. The government needs to view the internet as a type of public space in which individuals should be able to move freely and safely. The government must uphold the conditions of the social contract online, and not allow commercial interests to trump liberal values, should these ever conflict. Individuals should be protected from any actors seeking to harm them in the digital world. The government also needs to establish when public-private interaction is preferable or not in this context, by looking at whether it upholds or detracts from liberal values.

The broad lines of the government's digitalisation policy need to be coordinated from a central point. This prevents compartmentalisation and ensures that cross-departmental and cross-level policies are aligned. As such, it would be highly advisable to set up a separate ministry for

digitalisation. The sheer scope of digitalisation justifies the appointment of various government officials. This would provide us with stronger representation at international forums and organisations, where we could establish working relationships with our direct partners, while also allowing us to engage in dialogue with governments looking to use digitalisation for authoritarian purposes. Furthermore, we must always approach digitalisation issues from the principle of subsidiarity, so that decisions are always taken at the closest possible level to the citizen.

When it comes to regulation, we have seen that an increase in regulators can be detrimental to a democratic process, given the legal consequences. Another issue is that regulators often act reactively and are insufficiently proactive. It is essential to look into other forms of regulation. System monitoring might be a solution for some businesses. Regulation would then focus on the risk and quality control systems set up by companies themselves. This would create a tiered model of regulation linking transparency to accountability. It would also save taxpayer money, because most regulation would be financed by the companies themselves. Added to which, a public algorithm register for the government and other organisations would enable citizens to carry out checks themselves. Furthermore, regulation should not focus solely on technology, but also on frameworks for action for the users, allowing space for professional autonomy.

Not only must regulators be empowered to issue large fines, individuals must also be empowered to demand financial compensation for cases of misuse too. New *class action* legislation allows interest groups to file damage claims on behalf of large groups of victims, in the event of data breaches or the misuse of personal data, for example. Previously, damages relating to scattered claims could typically only be filed on an individual basis, these can now be filed as collective claims, suddenly making it possible for claims to be made that can be worth billions. Vast sums like this can act as a deterrent to large tech companies – and the government – and encourage them to comply with laws and regulations. Above all, this could create a level playing field for individuals through the court system. It will be necessary to keep an eye on how the case law of this legislation unfolds in the near future.

Innovation policy and strategic autonomy would also be important parts of our governance strategy, but Europe is still far behind in this

area. There are not enough large European tech companies, which leaves us dependent on American and Asian alternatives. Our innovation policy would enable us to invest in technologies in which liberal values would prevail, such as *privacy-enhancing technologies*, explainable algorithm technologies and *open-source* software and hardware products. A standardisation strategy needs to be implemented for this at European level, supported by every Member State. Innovation policy should revolve around more than just the amount of money invested, it should also look at where this money ends up and how it supports innovation in the broadest sense. There is plenty of academic expertise in Europe, but the links between academia and the business community is severely lacking. Despite the fact that academia often forges risky links with foreign parties. We need to develop guidelines that guarantee scientific integrity and which prevent partnerships with unwanted parties.

The government can also act as a link to promote cooperation between academia and business. Partnerships of this sort can also reinforce innovation at European level. There is also a need for venture capital to help start-ups, and especially scale-ups, grow. For example, pension funds could dedicate a much larger share of their assets to venture capital investments. The government could also help by serving as a *launching customer* for innovation start-ups and scale-ups, who operate based on values such as privacy and autonomy. Given the shortage of ICT professionals on the labour market, it is also important to continue investing in ICT training and to provide retraining for existing workers.

Finally, we need to draw up a long-term digitalisation strategy which anticipates the various technological developments coming our way. This will allow us to capitalise on opportunities and mitigate risks. The quantum computer, for example, will have many uses, but it will pose an immediate threat to many current forms of encryption. The metaverse may also transform the internet and play a major role in our daily lives, while also raising many pressing issues around privacy and the legal interpretation of certain online activity. While cryptocurrencies may provide an interesting alternative means of payment, they are not without major concerns when it comes to financial stability, money laundering, cybercrime and environmental impact. Robotisation provides many opportunities and relieves us of a lot of work, but is a threat to job security for large groups of people and obliges us to think about

how autonomous a machine can be, for example, in matters of life and death. In the longer term, we will also be confronted with various human enhancement technologies like genetic modification and neurotechnology. They will allow diseases to be cured and may also enable us to *upgrade* ourselves in all kinds of other ways. However, this will have potentially drastic effects upon the equality of opportunity in society, while potential hacking of brain implants could pose threats to our privacy, autonomy and security. All these technological developments require a far-sighted policy. Different circles of expertise need come together to discuss this now in order to understand and address the implications.

All in all, many aspects need to be taken into consideration when forming an overall governance strategy. The specific guidelines discussed in the preceding chapters require the support of a coherent governance strategy which goes beyond just legislation and awareness. A broader vision based on liberal values would allow us to make a much-needed switch from a passive to a proactive attitude when it comes to digitalisation.

8. Closing remarks

In the introduction to this book, we emphasised that our main focus would be on the risks of digitalisation. We may therefore have struck a somewhat cautious tone, but this does not mean that liberals do not acknowledge the enormous potential of digitalisation. After all, many things are going well and ultimately, digitalisation brings society great prosperity and well-being. Digital technology can also support all kinds of societal interests such as participation in democracy and better education. From a liberal perspective, society should, to the greatest extent possible, be left to its own devices without unnecessary intervention. It is important to emphasise this but, at the same time, dwelling for too long on the technicalities of political writings doesn't serve anyone either. The overarching aim of this book has been to identify the more challenging aspects of digitalisation, because that is precisely where politics has a role to play.

We also aimed to impress upon the reader that digitalisation affects us all and involves fundamental political and social issues. The working group has tried to write an accessible book aimed at raising awareness, even among people with little technical knowledge of the subject. A message that we are particularly keen to convey is that it is not necessary to fully understand the technology. It's about the application of technology and this is something everyone can form opinions about, even if they lack knowledge of the actual technology behind it. Administrators, policymakers and other professionals should not let the technical nature of digitalisation deter them, but should instead focus on the societal impact of the process and discuss this together. The intention of this book is to outline a conceptual vision that can form a launchpad for such conversations. Policy should involve more than just combatting symptoms in a reactionary way, it should draw instead upon a broad normative

framework, which is exactly what liberal values can provide. We have not been able to provide answers to all the issued raised. With this book, the working group hopes to encourage important society-wide discussion around digitalisation, fully realising that it is a work-in-progress.

We have also found it encouraging to observe that there currently seems to be wide-ranging consensus within the European political landscape with regard to the approach to take to digitalisation. In many countries, political parties of various persuasions appear to agree that something needs to be done about it. This means that there will be plenty of scope for action in the coming years. The urgency behind improving digitalisation policy may have been acknowledged, but it is now time to act.

Recommendations

Recommendation 1: take liberal values as the foundation for digitalisation policy

Digitalisation raises all kinds of fundamental societal issues and presents us with a range of different interests to weigh up. Liberalism provides a political-philosophical framework on which to take decisions. There are five values that liberals deem essential when it comes to digitalisation: privacy, autonomy, security, equal treatment and democracy. Although liberals hold the non-interventionist principle dear, we can see that digitalisation poses certain unacceptable risks when it comes to liberal values. Therefore, politicians need to intervene in this area in a targeted manner through legislation, awareness and the formulation of a broad strategy. Our freedom can only be guaranteed by setting boundaries.

Recommendation 2: strengthen data protection measures

The revenue model for various market parties is based on collecting as much personal data as possible. This has brought about the emergence of a kind of surveillance economy in which individuals are not seen as consumers, but as products. The GDPR provides a legal framework for data protection which aligns with liberal values. Unfortunately, the practical infrastructure is insufficient for optimal use to be made of it. Furthermore, enforcement needs to be stricter with higher fines for violations. However, we need to explore whether the administrative burden of the GDPR could be lessened for SMEs, particularly as the main risks lie with the large tech companies. Market parties should adhere to the obligations that bind them and data should be anonymised as much as

possible. Additionally, individuals need to be made aware of the measures they can take to protect their data in the best possible way.

Recommendation 3: prevent large tech companies from abusing their market power

The current market is dominated by a select number of tech companies. A certain concentration of power in this market is probably inherent due to things like the network effect and positive data feedback loops. However, these parties abuse their power to hinder fair competition. There is therefore a need for pro-competitive legislation aimed at the separation of roles, interoperability, data portability and a ban on both tie-in sales and *buy-and-kill*-acquisitions. The final option, in combination with these measures, is to break up the tech companies. Legislation of this type (and its enforcement) will largely need to be realised at European level.

Recommendation 4: protect democracy against the harmful effects of disinformation and recommendation algorithms

Digital technology enables new forms of disinformation which it then disseminates on a mass scale. Tech companies' recommendation algorithms also create information tunnels which are detrimental to public debate. Politicians need to promote media literacy to raise awareness about this among citizens. Social media platforms can also take action against disinformation by using independent fact-checkers and labelling it at such. Nonetheless, the expression of controversial opinions should always be allowed. The greatest problem is the tech companies' algorithms. They aim to hold user attention for as long as possible and prioritise sensational, provocative and polarising content. However, the current self-regulatory approach will always fall short, because clamping down on this runs counter to the tech companies' revenue model. Transparency and societal control over these algorithms will need to be enforced through legislation and the tech companies will need to be held accountable given the current key role they play in democracy.

Recommendation 5: create transparency around profiling by political parties

Digitalisation offers political parties many new ways of getting in contact with citizens. This means that more citizens get involved in the democratic process and it also helps smaller parties get their message across. At the same time, political parties can also circumvent traditional media and spread disinformation through their own digital channels. By profiling voters, parties are able to tailor their political messages to individual personal characteristics, which hinders voters in forming an opinion autonomously. It also encourages parties to collect as much voter data as they can and to push the boundaries of privacy laws. Legislation is therefore needed to create greater transparency so that citizens know which parties are approaching them online and why.

Recommendation 6: protect democracy from foreign political interference

Political interference has become a popular strategy for certain states to influence, polarise and destabilise other countries. Digitalisation provides new, easy and difficult-to-trace means to achieve this. Democracies are particularly vulnerable, because information flows are uncensored. Countries like Russia and China in particular, now pose a threat to our democracy. We need to establish a multidisciplinary approach to counteract this, involving not only the security services, but other societal actors too. Economic sanctions can be imposed as a countermeasure. Furthermore, we recommend always holding major elections in a non-digital format and supporting democratic powers in authoritarian countries.

Recommendation 7: as the government, ensure that digitalisation does not result in the exclusion of certain citizens

Digital skills are not a given in certain social groups. Furthermore, not everyone has the same material access to the digital world. Not only are

certain citizens unable to keep up with the government's urge to digitalise, there are others who do not want to do so because they are – not entirely without justification – concerned about their privacy and the security of their data. The government exists for all of us, digital novices and sceptics included. Therefore, in principle, citizens must always be able to communicate with the government via non-digital means. At the same time, digital skills have become essential in today's society. The government must therefore foster digital inclusion through information and education. It is important that it does this by adopting a facilitating and non-coercive attitude.

Recommendation 8: as a government, be cautious about using automated technology and ensure sufficient transparency and accountability

The government makes use of automated technologies such as algorithms, for example, for risk detection. However, algorithms cause unintended feedback loops and the data entered into them is sometimes lacking. Discriminatory factors can play a role – often unintentionally – as we saw in the Dutch childcare benefits scandal. The government needs to be more transparent about the use of technologies like these and to be held accountable for them. On the one hand, transparency must ensure explainability to members of the public and, on the other hand, it must provide technical insight for independent experts in the field. In addition, government officials must be able to question an algorithm's assessment if, for example, they suspect discrimination. When it comes to the exchange of personal data, the government needs to appoint officials with ultimate responsibility for it, and citizens must be able to view this data easily. When it comes to complex government processes, the government must first organise properly, and only then automate. In any case, the government must always ask itself if it is wise to automate through algorithms and artificial intelligence.

Recommendation 9: When using digital technology, never lose sight of liberal values even in crisis situations

During the Covid-19 crisis, digitalisation provided ways of keeping daily life going while containing the virus. The government tried to be transparent when designing the Dutch Covid-19 tracking app, but failed to communicate this adequately to the outside world. This gave the wrong perception to the population, which proved detrimental to public support. In other incidents, the security measures taken fell short, resulting in a government data breach, among other things. More errors were made in the rush to manage the crisis. This makes it all the more important not to just dismiss matters like privacy and (cyber) security as afterthoughts. This is true of the technology itself, as well as the frameworks for action that are put in place for the people who use it. Furthermore, it is important to emphasise that any special measures taken in a crisis situation should be removed as soon as the crisis is over.

Recommendation 10: reduce the vulnerability of critical processes to cyber attacks

Various processes are critical to all of society, such as the provision of drinking water and the supply of energy. All these processes have been largely digitalised, making them vulnerable to cyberattacks. Firstly, these processes need to be adequately shielded from undesirable investments from enemy states. We must also diversify the suppliers of critical processes to prevent dependency. This is also true of other indirect links in critical processes, such as software and hardware suppliers. In addition, stricter checks must be put in place to ensure that these market parties take sufficient cybersecurity measures. When it comes to the government sharing information about cyber threats, the distinction between critical and non-critical is irrelevant because almost any company can fall victim to them.

Recommendation 11: encourage risk management for various cyber threats

Members of the public, businesses, the government and other organisations, all need to protect themselves better against various potential cyber threats. They all need to be made aware of the importance of basic cybersecurity hygiene. This can be addressed in the school curriculum and during local information evenings organised by municipalities. We need to develop better security standards, while also realising that cheap electronics imported from countries like China will always remain particularly vulnerable to cyber attacks. A general reporting obligation is necessary for ransomware attacks and must be strictly enforced. Our government security agencies also need to take preventative and investigative measures, and seek out international cooperation. It is important to continue to respect civil rights when making use of special powers. The process leading up to the deployment of special powers should be organised as efficiently as possible to minimise the bureaucratic burden. Furthermore, there is also a structural need for additional funding throughout the various government security agencies, due to the capacity shortage in many countries.

Recommendation 12: highlight the fact that the rights and obligations that apply in the physical world also apply in the digital domain

The digital world is not a separate, self-contained reality, it is simply another part of the 'real world'. Legislation in force in the physical world is also applicable in the digital domain. As a result, there is no need for separate digital fundamental rights, although some human rights will need be amended or updated in response to new technology. The government's core tasks in the physical world must also be carried over into the digital sphere. The internet should be viewed as a type of public space, with its borders guarded by government, within which digital services can be used freely and securely. The government also needs to be aware of when public-private interaction is preferable or not, by examining whether it upholds or detracts from liberal values.

Recommendation 13: create a ministry for digitalisation to coordinate digitalisation policy

As digitalisation plays a role across almost all policy areas, responsibility for it has been fragmented for a long time. This is true both horizontally across the various ministries and vertically throughout the various levels of government. Digitalisation policy needs to be coordinated centrally in order to prevent compartmentalisation. Consider drawing up general guidelines. This would facilitate the coordination of policy in broad terms, while also providing space to reflect upon the safeguarding of liberal values on a more abstract level. The sheer scope of digitalisation requires the appointment of various government officials within a dedicated ministry for digitalisation. This would also ensure better delegation at international level, where many of the decisions surrounding digitalisation are made. At the same time, policy must follow the subsidiarity principle and decisions should always be taken as close to the citizen as possible.

Recommendation 14: empower regulators to issue significant fines and consider more efficient and effective forms of regulation

Regulators must be able to issue much higher fines if these are to act as any real deterrent, especially when it comes to large tech companies, who will not pay much attention to this otherwise, given their vast capital. However, continually expanding the number of digitalisation regulators is unlikely to work. It is better to consider alternative forms of regulation. System monitoring might be a solution for some companies, in which they would set up their own quality and risk management systems that would subsequently be regulated in a scalable manner, through a tiered regulation system. A government-run public algorithm register would also make regulation easier.

Recommendation 15: investigate options for individuals to seek damages through the courts from parties who violate their rights

New legislation in class action law now allows interest groups to file damage claims on behalf of large groups of individuals. This allows damages to be collected from parties who break the law in cases of scattered damage, such as data breaches or misuse of personal data. This can act as a deterrent, even for large tech companies, because of the large sums of money that can be demanded. This ensures a level playing field for individuals going through the court system. We will need to keep a watchful eye on future case law to see whether this allows individuals to better defend their rights in the digital world.

Recommendation 16: promote European strategic autonomy through innovation policy

Europe has a disproportionately small number of large tech companies, making us highly dependent on American and Asian market players. We could achieve the strategic autonomy we need through our innovation policy. This would also enable us to invest in technologies in which liberal values are paramount. The government could act as a link between academia and business and ensure a strong innovation ecosystem. The government can also act as a *launching customer* for innovative companies. More venture capital is needed on the market to enable tech start-ups and scale-ups to continue to grow. European pension funds, for example, could make an important contribution to this. It is also important to continue investing in ICT training and retraining opportunities to resolve the current shortages in the labour market.

Recommendation 17: develop a long-term strategy to prepare society for any potential disruption arising from future technological developments

We cannot predict technology, but we are already seeing a number of developments that need to be anticipated. This may bring many positive things, but it is not without risk. Quantum computers are a threat to encrypted information. The metaverse will blur the distinction between the physical and digital, resulting in even more data being collected. Cryptocurrencies are risky in terms of financial instability, cybersecurity, money laundering and the environment. Robotisation will impact job security for large groups of people and raises all kinds of ethical questions. Human enhancement technologies could prove detrimental to the equality of opportunity in society and cause harm to privacy, autonomy and security. Politicians must already prepare for these potential consequences by working with experts from various fields.

Acknowledgements

Various experts provided input to the working group in writing this book. The working group would therefore like to thank the following people for their constructive comments:

- Hugo Bellaart, Managing Director at Camenai, a young *geospatial* AI company, who previously worked at Philips and Ziggo.
- Bart Groothuis, Member of the European Parliament on behalf of the VVD and former Head of Cyber Security at the Ministry of Defence.
- Douwe Lycklama à Nijeholt, founding partner of consultancy firm Innopay, specialised in the digitalisation of data, identity and payments for companies and government.
- Jan Middendorp, Head of Corporate Development at bunq and former VVD spokesperson for digitalisation in the House of Representatives.
- Queeny-Aimée Rajkowski, Member of Parliament for the VVD and responsible for the digitalisation portfolio. Former municipal councillor in Utrecht and previous experience in the IT sector.
- Frederik Zuiderveen Borgesius, Professor of ICT and Law and affiliated with the iHub at Radboud University.
- Gerrit-Jan Zwenne, Professor of Law and the Information Society in Leiden and Lawyer-Partner at Pels Rijcken in The Hague.

With regard to the TeldersStichting, the working group would like to express its appreciation for advisory board's constructive comments and to thank Marthijn Kinkel for his research work as an intern. In particular, the working group would like to thank director Patrick van Schie, who contributed to the book's content during all meetings. Finally, the working group would like to thank the European Liberal Forum (ELF) for making this English edition possible.

Digitalisation is having a fundamental impact on society. Over a relatively short period of time, things such as the internet, smartphones and social media have come to play a major role in our daily lives. It has never been easier to look up information and we can communicate effortlessly with one other digitally. It is no longer possible to imagine sectors like education or healthcare without the application of digital technology. Digitalisation has undoubtedly enriched people's lives and society as a whole. Nonetheless, there are major issues that raise questions when it comes to digitalisation. How do we keep the data greed in check with large tech companies? How can we minimise the harmful effects of disinformation? What can we do about the government's use of discriminatory algorithms? How can we protect ourselves from cyber attacks? Digitalisation presents a range of unique challenges that politicians will have to address.

Liberalism provides a framework for shaping digitalisation policy. Certain boundaries need to be drawn in the digital world for individual freedom to be safeguarded. The liberal values of privacy, autonomy, security, equality and democracy should be taken as a starting point. This book, from a liberal perspective, reflects upon the major challenges posed by digitalisation with regard to the free market, democracy, the citizen-government relationship and the security of society. It also explores how digitalisation policy could be embedded in a general governance strategy. This book seeks to put across in accessible language how digitalisation issues are relevant to us all, and that it is time for politicians to take action.

Dr. T. (Tamara) de Bel is a Risk Officer for the government and the founder of the thematic network De Impact van Verandering binnen de VVD (The Impact of Change within the VVD). She has a Master's in International Security & the Politics of Terror from the University of Kent.

Prof. dr. D. (Dennis) Broeders is professor of Global Security and Technology at the University of Leiden. He is also a Senior Fellow of The Hague Program on International Cyber Security and a Project Coordinator of the EU Cyber Direct initiative.

Dr. W.J. (Wilbert Jan) Derksen is a member of the scientific team at the TeldersStichting.

Brig. Gen. prof. mr. P.A.L. (Paul) Ducheine is Professor of Cyber Warfare at The Netherlands Defence Academy and Professor by Special Appointment of Military Law of Cyber Security and Cyber Operations at the University of Amsterdam.

Prof. dr. ir. M. (Marijn) Janssen is Professor of ICT & Governance at the Faculty of Technology, Policy & Management at the Technical University Delft.

Prof. dr. S. (Sander) Klous is Professor of Big Data Ecosystems for Business and Society at the University of Amsterdam and Partner in Data & Analytics at KPMG.

Commodore prof. dr. F. (Frans) Osinga is Professor of Military Sciences at The Netherlands Defence Academy and Professor by Special Appointment in War Studies at the University of Leiden.

Ir. J.R. (Jan Ronald) Prins is the founder of Hunt & Hackett.

Published by the **European Liberal Forum** in cooperation with the Prof. mr. B.M. Telders-Stichting. The publication received financial support from the European Parliament. The views expressed herein are those of the author(s) alone. The European Parliament is not responsible for any use that may be made of the information contained therein."

elf

TeldersFoundation
because knowledge matters

9 782390 670711 >