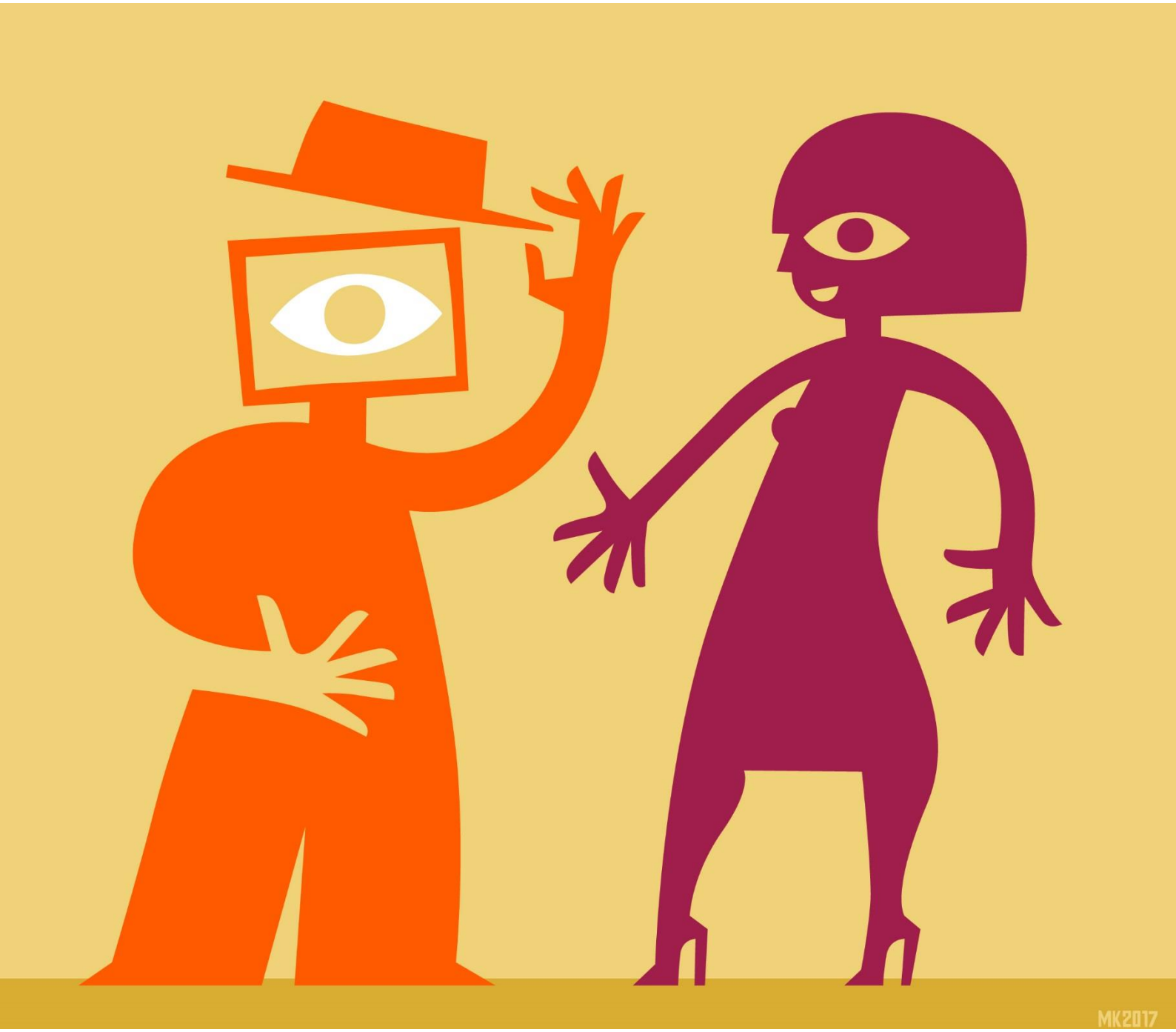
Rathenau Instituut

Decent Digitisation

Seventeen experts on an ethical digital society



Report

Authors
Jurriën Hamer and Linda Kool (ed.)

Editor
Arnold Vonk

Illustrations
Max Kisman

Preferred citation:
Hamer, J. & L. Kool (ed.) (2018). *Decent Digitisation – Seventeen experts on an ethical digital society*. Den Haag: Rathenau Instituut

Preface

The Netherlands is one of the most digitally literate countries in the world and has been for many years. That did not happen overnight. In 1979, the country faced a huge challenge: the advent of the personal computer. The government foresaw that the rise of the microchip would bring about dramatic changes in society. It was crucial for the Dutch to make a smooth transition. A committee under the leadership of Gerhart Rathenau took on the task of studying ‘the implications for society of Micro-Electronics’. Among his other achievements, Rathenau was one of the initiators of a project that would bring personal computers into the homes of many of thousands of Dutch people.

We need Rathenau’s prescience again today. Digitisation has become integral to our lives; it is critical to our businesses, it is changing our government, and it is even influencing our romantic relationships. The time separating each successive change is growing shorter, and the arrival of the super-fast national 5G network will only quicken the pace. That’s why it is high time for us to think about how we deal with digitisation.

On the one hand, digitisation puts pressure on such public values as decent work, security and human dignity. For example, a recent study by the Rathenau Instituut has shown that robots and artificial intelligence are taking over a growing number of human tasks. We have also recently discovered that ransomware poses a security threat to port terminals, power plants, hospitals – even our own holiday snaps. Digitisation puts other values at risk too: autonomy, justice, technological control, and a fair balance of power.

Digitisation also offers us all sorts of opportunities, as our publications ‘A fair share’ and ‘Urgent Upgrade’ show. But it’s up to us to take advantage of them. To create an ethical digital society, we need to follow the example of our predecessors in 1979 and work together to ensure that digitisation genuinely supports the values that we all share – the values laid down in our constitution and in human rights conventions.

For this publication, we have invited seventeen philosophers and practitioners to share their ideas and solutions. We thank them all for their insights. They have enriched our thinking and given practical meaning to important values.

Dr. Melanie Peters
Directr, Rathenau Instituut

Summary

Over the past months, we called in experts from a wide variety of disciplines to reflect on how we can bring decency to our digital society. We threw down the gauntlet and saw that government institutions, civil society organisations and researchers rose to the challenge. They shared their solutions in seventeen separate blogs, brought together in this publication.

The blog series focused on four questions: ‘How can we create an inclusive digital society?’, ‘How can we stay in charge of algorithms?’, ‘How can we help IT professionals to work ethically?’ and ‘How can we protect children?’ The authors reveal how they uphold public values, such as justice and autonomy, in an increasingly digital world and they encourage politicians, policymakers and IT professionals to do the same.

The insights generated by the series transcend their specific context, however. Those insights can be described in terms of four virtues that can help us deal decently with digital technology:

- personalisation: not everyone wants the same thing;
- modesty: know the limits of digital technology;
- transparency: watch out for an algorithmic ‘black box’; and
- responsibility: dare to take the plunge.

Contents

Introduction

The Rathenau Instituut has been studying digitisation at great length. Amongst other things, we noted the potential of digital applications to violate personal privacy and other public values. That is why, in 2017, we have proposed introducing the 'right to meaningful contact' and the 'right not to be manipulated, coached or tracked'.[1]

In addition, we proposed to improve the way that society takes decisions concerning digitisation. In other words, the Netherlands requires a better governance structure to speed up the process of turning ethics research into specific policy plans; to force businesses to take responsibility by agreeing on codes of ethics and by considering public values from the initial stages of product or service development; and to ensure that users have a greater say and are better organised.[2]

For this publication, we have invited philosophers and practitioners to reflect on these ideas and how they can be incorporated in an ethical digital society. We hope that collecting these different views in one place will inspire all those involved in digitisation.

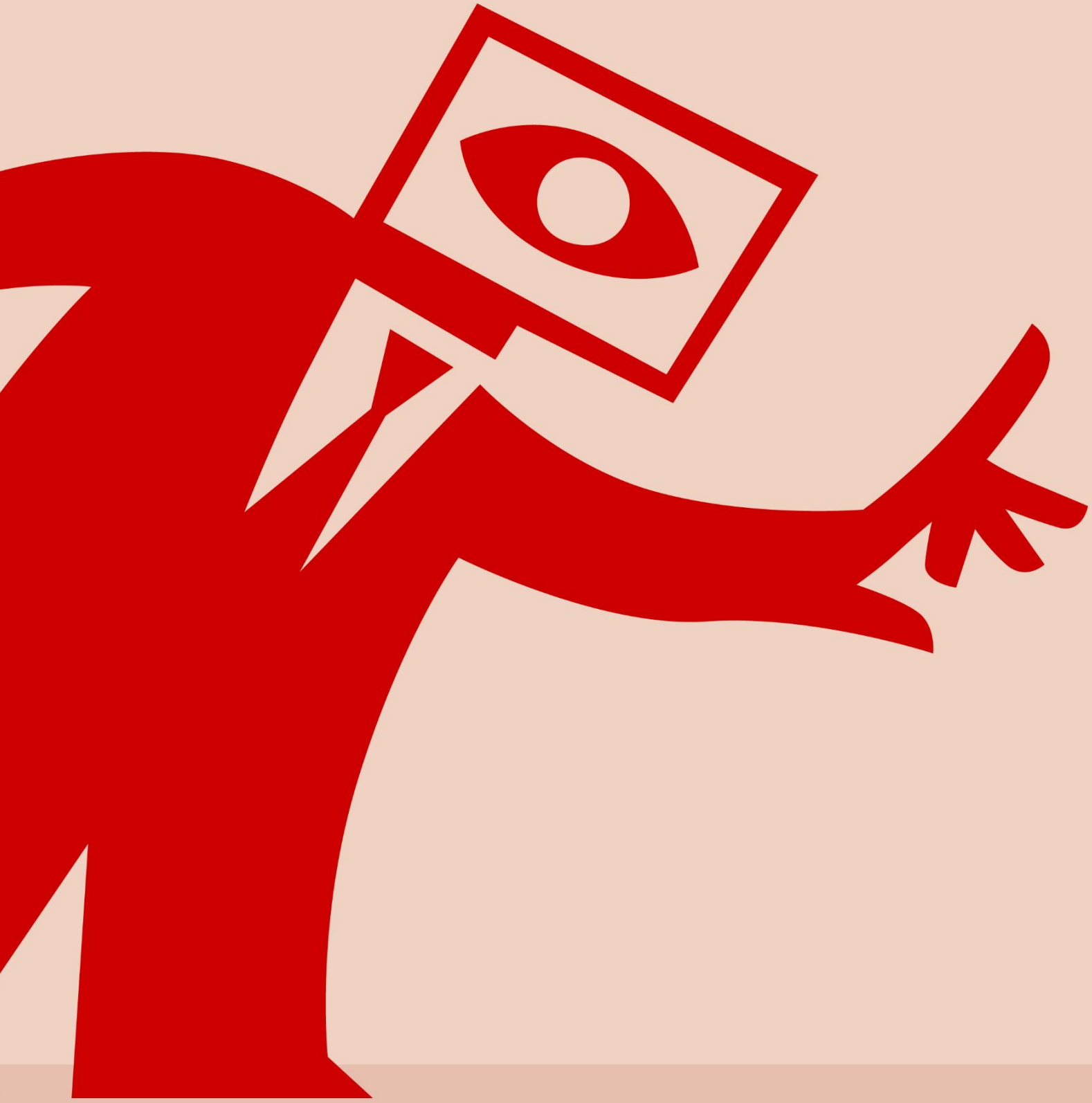
Reader's guide

In Chapter 1, the National Ombudsman, the UVW Employee Insurance Agency and experts from the knowledge institutes Nictiz and ICTU describe how society can ensure that everyone can participate. Chapter 2 discusses how we can stay in charge of algorithms. With contributions from the Dutch Police and Amnesty International, an algorithm expert and a cultural sociologist. The sector organization KNVI, academics and privacy experts write about the role of IT professionals in chapter 3. Chapter 4 discusses how we can protect children online; with contributions from eLaw, Kennisnet and the Youth & Media Agency.

1 See our report Human rights in the robot age: Van Est, R. & J.B.A. Gerritsen, with the assistance of L. Kool, Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality – Expert report written for the Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe (PACE), The Hague: Rathenau Instituut 2017, available on https://www.rathenau.nl/en/digital-society/human-rights-robot-age

2 See our report Urgent Upgrade: Kool, L., J. Timmer, L. Royakkers en R. van Est, Urgent Upgrade - Protect public values in our digitized society. The Hague, Rathenau Instituut 2017, available on https://www.rathenau.nl/en/digital-society/urgent-upgrade

1 How can we create an inclusive digital society?



Digitization can exclude a part of the population. How can this be avoided? In this chapter, the National Ombudsman, the UVW Employee Insurance Agency and experts from the knowledge institutes Nictiz and ICTU describe how society can ensure that everyone can participate.

1.1 Digitisation should not mean exclusion

By Reinier van Zutphen, National Ombudsman of the Netherlands, and Jeanine Verhoef (project coordinator).[3]

The world is digitising rapidly. People use their smartphones for messaging, to plot a route with Google maps, to shop online or to catch up with friends and family on Facebook. The fact that the Dutch government wants to support digitisation is both understandable and desirable. But digitisation also carries risks. For example, it could very well exclude a segment of the population. We must prevent that at all costs. Government must ensure that everyone can participate, and it must make a special effort to include those who are unable to keep up.

The Office of the National Ombudsman of the Netherlands has studied the topic of digitisation in recent years, specifically in projects focusing on the government's digital transactions with citizens, digital communication from the Tax and Customs Administration, and the government's online message box platform, as well as the digitisation of various government agencies. We are concerned about digitisation restricting people's access to government.

3 This paragraph is published as a blog on September 25, 2017 on https://www.rathenau.nl/en/digital-society/national-ombudsman-netherlands-digitisation-should-not-mean-exclusion

In addition to digital channels, other options must remain for those people who do not have the necessary cyberskills or who want personal contact. Not every problem can be resolved digitally. Also, government should exploit the potential of digitisation to ‘personalise’ its public services. For example, digital channels can in fact make it easier for social workers to act on a client’s behalf. And government must realise how easy it is to make a mistake in the digital realm and assist people when a situation threatens to get out of hand.

Some examples

We heard the following from Jan van Lieshout (70): ‘I’m a community caregiver and I take care of my sister-in-law’s administrative paperwork. She’s 83, lives alone, doesn’t have children and has some psychological issues. I receive and deal with her care allowance by post and that usually works out just fine. But it will be problematical if the Tax and Customs Administration expects my sister-in-law to arrange her tax matters online herself. Just applying for the DigiD login code will be a disaster. She can give me power of attorney to do that, but she doesn’t understand what it means. For example, when she receives the confirmation in the post, she’ll just throw it away.’

When Corry (70) heard about the Message Box – a personal, online mailbox for digital communications from government organisations – she wanted to know if it would be convenient for her. Out of curiosity, she surfed to the MijnOverheid [MyGovernment] website and clicked on a few options here and there. After a closer look, she decided that it all seemed a bit too complicated, so she closed the browser window. A few months later she received a letter stating that she had neglected to take her car in for its annual MOT several months back and she would now have to pay a heavy fine. She was shocked. She always kept close track of her affairs, but she had not received any letter reminding her of the MOT. She then discovered that the letter had been sent to her online Message Box. Without realising it, she had activated her account to receive all government communications there.

Piet (43) acts on a power of attorney for about a dozen clients – people who are unable to take care of themselves. He would like to communicate with government organisations digitally on behalf of his clients. That would make things much easier for him. Now, post from these organisations is sometimes sent to his clients’ homes instead of to his office. Not all of his clients are capable of managing their post, however; important documents get lost, and problems ensue. Unfortunately, it is not possible to administer matters for his clients digitally because he cannot apply for a business DigiD login code, and because only a limited number of government organisations permit him to act digitally on a power of attorney.

Government expects a great deal of people
Government expects a great deal of people. It expects them to participate and to keep their affairs in order. But participation requires a considerable level of skill these days. People are obliged to keep track of complex financial and other paperwork; they must be digitally competent; they must have a good command of written and spoken Dutch; and they must be capable of assessing whether or not a specific situation applies to them. A nodding acquaintance with conflict management is also handy, as well as some knowledge of how interests are assessed. Not everyone can do all of this or meet all these expectations.

People now have 24/7 access to the online forms they need to apply for official permits, government allowances or care assistance. About 80% are able to do so without a hitch, but there are still many people who are unable to manage in the digital world. It isn't always possible to describe someone's personal situation by ticking boxes on a form. When people enter the wrong values, they get an error message but don't know what they're doing wrong. And so they give up. Or they call the National Ombudsman.

Government ought to look at digitisation from the public's perspective
Government therefore ought to look at digitisation from the public's perspective. Will digitising a service actually make it better or easier for the people who use it, and in what way? Only after it has answered these questions should it proceed. After all, government doesn't operate in a free market; people cannot turn to a competitor to file their tax forms or apply for a passport.

That means that government must do its best for everyone. It should work a bit harder for those who are unable to keep up with the times. That is one of the tasks that the responsible government of an inclusive society should take upon itself. It should always offer personalised services, an alternative communication channel, and personal contact for those who require it.

We will continue to remind the government of its obligations in that regard and persuade it to look at digitisation from the public's perspective.

1.2 Make online services appealing, not compulsory

By Marije Wolsink, Director, Client & Service, UWV Employee Insurance Agency.[4]

Technology and digitisation have become indispensable to our everyday lives and to the UWV, for without technology we would be unable to disburse benefits, assess people's social and medical status, or help them find a job.

Much of the UWV's service delivery now proceeds through digital channels. People can apply for benefits, take courses, search for jobs, report job applications or change their personal data online. But is that the only option? The UWV believes that online services are the future, but we don't want them to be compulsory. Experience shows that there are many people who are unable to transact their business online.

Who is responsible for digitisation?
Who's responsible for the digitisation of government services? Is it the government itself, or is it the public? Most people find it absolutely normal to be able to transact business online whenever they please.

But there are still people who are not digitally skilled enough to submit an application online. This dilemma is forcing the UWV to make choices regarding its online services.

4 This paragraph is published as a blog on November 14, 2017 on https://www.rathenau.nl/en/digital-society/uwv-make-online-services-appealing-not-compulsory

I want to note straight away that most of our clients have the necessary digital skills. In other words, they have a DigiD login code and can work comfortably with a computer. As we proceed to digitise our information and communication channels and transactions, we look at what people are used to from other service providers, for example banks, web shops, insurers or power companies.

We also design our digital services to be as user-friendly and straightforward as possible. We've started by digitising services for unemployment benefits recipients. Because they were, until recently, in work, we know that they are likely to be experienced and skilled computer users.

We will make our online environment appealing

At the same time, we must bear in mind the clients who are (as yet) unable to communicate or work with us digitally. We must ensure that everyone can continue to access our information and services. That's why we are developing digital information and processes alongside our non-digital ones. We are retaining the non-digital processes to accommodate the clients who have not switched to digital channels yet, or who will never be able to do so. So we will continue to work with applications on paper, letters sent by post, a telephone helpdesk, and walk-in appointments.

Our strategy is to tempt clients into switching to digital channels. We believe that online processes are often faster and easier for them. We are working with local governments to improve the public's digital skills, for example by organising courses and workshops around the country and by using libraries to offer low-threshold assistance.

No UWV clients will be left behind who are (as yet) unable or unwilling to transact business with us online. We lavish as much attention on them as on people who want and expect us to offer them digital alternatives.

Driven by the need to cut costs

We began to digitise our services in a period of austerity. In fact, part of our digitisation campaign was driven by the need to cut costs. At the time, that meant that clients were compelled to communicate online with the UWV. The idea was that all of our print communication – and even much of our face-to-face service delivery – would eventually be replaced by digital communication and products.

The transition was successful for many of our clients, but certainly not all of them. For example, we noticed that not every client who applied for benefits online was capable of handling all their other business with the UWV online too, such as their work folder.

The UWV has had to admit that its digital products do not always live up to clients' expectations, meet their needs or, above all, match their abilities. That is why we decided not to make digital communication compulsory for clients. We offer them other options: communication by regular post, by telephone, or in person. Our aim now is to focus on making the digital channel more appealing. We encourage clients and offer them support in the form of courses, libraries and power-of-attorney options. We also tailor our digital services to clients' needs and abilities.

All this is making demands on our organisation. After all, we must develop and maintain two separate tracks. At the same time, the UWV must offer – and indeed wants to offer – every person the same level of service, regardless of the channel he or she uses. We will therefore always maintain the 'paper' track. We always offer people the non-digital option. It's a challenge, but we welcome it.

1.3 Don't take digital independence too lightly

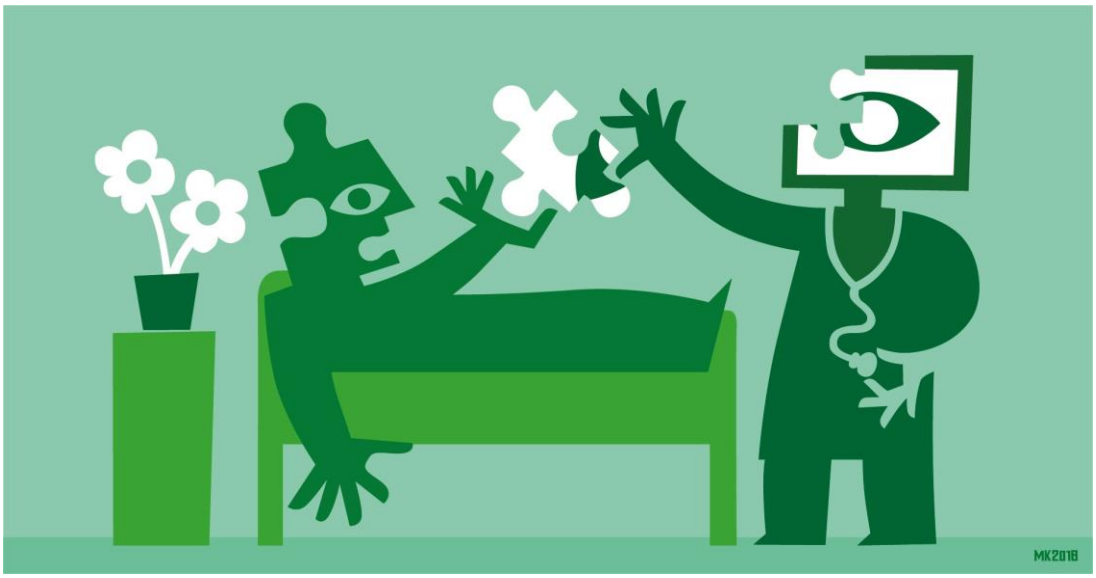
By Bettine Pluut, former senior adviser and action researcher at the e-health expertise centre Nictiz, and Marinka de Jong, manager of the Patient participation and eHealth programme at Nictiz.[5]

The ideal world does not exist, not even with e-health. But new digital applications are creating new opportunities to give patients more control and independence. Take the 'personal digital healthcare environment', for example. This is an online environment that allows patients to review all their medical information and share that information with care providers, family members and selected friends. It helps patients stay informed and makes it easier to take decisions about their health and health care together with people in their network.

But not every patient can access and manage his or her medical information in an online environment. Not every patient can organise a collaborative decision-making process. And not every patient is capable of asking their care provider questions online during an 'e-consultation'. In fact, there are many, many patients for whom e-health applications are out of reach. Access to some applications is restricted, while others are too complicated for many patients to use. Another common problem is that applications may be available without patients knowing about them.

5 This paragraph is published as a blog on June 5, 2018 on https://www.rathenau.nl/en/digital-society/e-health-experts-dont-take-digital-independence-too-lightly

Pharos, the Dutch Centre of Expertise on Health Disparities, observes that no less than 2.5 million people in the Netherlands are low-literate and another 1 million have trouble using digital tools.[6] Contrary to what many believe, two thirds of these 3.5 million people are Dutch in origin. In the most recent edition of its biennial report Staat van Nederland (The Social State of the Netherlands), the Netherlands Institute for Social Research (SCP) observes that low-educated individuals, including those with low literacy, are lagging ever further behind.[7] There are now large groups of people in Dutch society who find it difficult if not impossible to take control over their own lives, according to the Institute.



That means that as health care becomes increasingly digitised, we must pay closer attention than we do now to low-educated patients and those who have only a limited knowledge of health matters or IT skills. We must ensure that digitisation does not serve to widen instead of narrow the gap between vulnerable and resilient groups. In our view, the ideal of equal access to good health care must take priority in e-health policies and projects.

The good news is that we can link the ideals of patient independence and equal access to good health care by taking certain specific steps. We explain what they are below.

1. **Work with patients to devise, develop and test applications**
   Designers of e-health applications should start by making their tools easy for everyone to use, even low-literate patients. That means that we should

6 See pharos.nl/documents/doc/factsheet_beperkte%20gezondheidsvaardigheden_en_laaggeletterdheid.pdf
7 See https://www.scp.nl/Publicaties/Terugkerende_monitors_en_reeksen/De_sociale_staat_van_Nederland

devise, develop and test e-health applications in cooperation with a large variety of different patients. Working with patients will ensure that e-health applications are user friendly and comprehensible to all.

For example, when we tested a random portal among low-literate patients, it soon became clear that the portal had too many long sentences and blocks of text. That caused the users to skip the texts – in fact, many did not even try to read them. 'A lot of mistakes– unintentional ones– can occur in how people read information on a website. We really need patient input to develop truly user-friendly e-health applications,' according to our director Lies van Gennip in a blog about the conference at which low-literate persons tested the portals on the spot.[8]

2. **Provide clear information about e-health applications**
Second, it's important for patients to be properly informed about the e-health application. Many of the instructions now provided are too complicated for low-educated patients. As a result, they use e-health for the wrong reasons or they ask too much of their doctors.

Recently, a GP told us that she is unable to answer many of the questions she now receives through the e-consultation channel. For example, a patient may enquire about a painful knee, a complaint that requires a physical examination. She indicated that it was particularly difficult for low-educated patients to determine when an e-consultation is appropriate.

On the other hand, e-consultations can also have important advantages for low-educated patients. They can take all the time they need to read through their care provider's answer and advice. That message can also give them a link to confidential sources of information, or they can go over it with an informal care provider or family member. It might be useful to offer patients a simple leaflet or video that explains which complaints can be dealt with in an e-consultation. Tools such as the care provider's digital skills quick scan can help to assess patient skills.

3. **Advise people about the best application for them**
Finally, we need to make appropriate use of e-health applications. Not every application meets every need or is suitable in every situation. Online access to test results is one example. Some patients are capable of reading and interpreting the results themselves and want to do so; others would be better off having their doctor tell them their results personally.

8 See http://kennismagazine.nictiz.nl/het-ontwikkelen-van-gebruiksvriendelijke-ehealth

A video call is ideal for patients who find a trip to the hospital too painful or exhausting, whereas a hospital visit gives lonely elderly people a welcome opportunity to make contact with others. Care providers can advise patients about whether or not to use a certain e-health application and explain the specific advantages for certain patients.

Making e-health applications for all

We have explained what we must do to link the ideals of patient independence and equal access to good health care. We hope that everyone involved in using IT to improve health care will not take the issue of patient empowerment too lightly. We must ensure that e-health applications are suitable for all.

If we can create digital applications that help precisely those people with low health skills, we will reduce health disparities. If we can manage to link the ideals of patient independence and equal access to good health care, then e-health will improve the quality of life of all patients.

1.4 People with digital skills or services with people skills?

By André Regtop, director of the ICTU and ambassador for the 'User Needs First' community, and Victor Zuydweg, ICTU consultant and co-initiator of the 'User Needs First' community.[9]

Digital independence depends on mastering digital skills. Millions of people in the Netherlands are supposedly not digitally skilled enough. They are indeed missing the e-boat, a problem recently highlighted in a report by the National Ombudsman of the Netherlands.[10] But that does not mean that these people are 'digitally un-skilled'. Indeed, it says more about the extent to which digital services meet the needs of those who use them. After all, '[T]he share of the population that can manage their affairs independently in the digital domain and/or that require assistance doing so naturally also depends on the complexity of the service itself.[11]

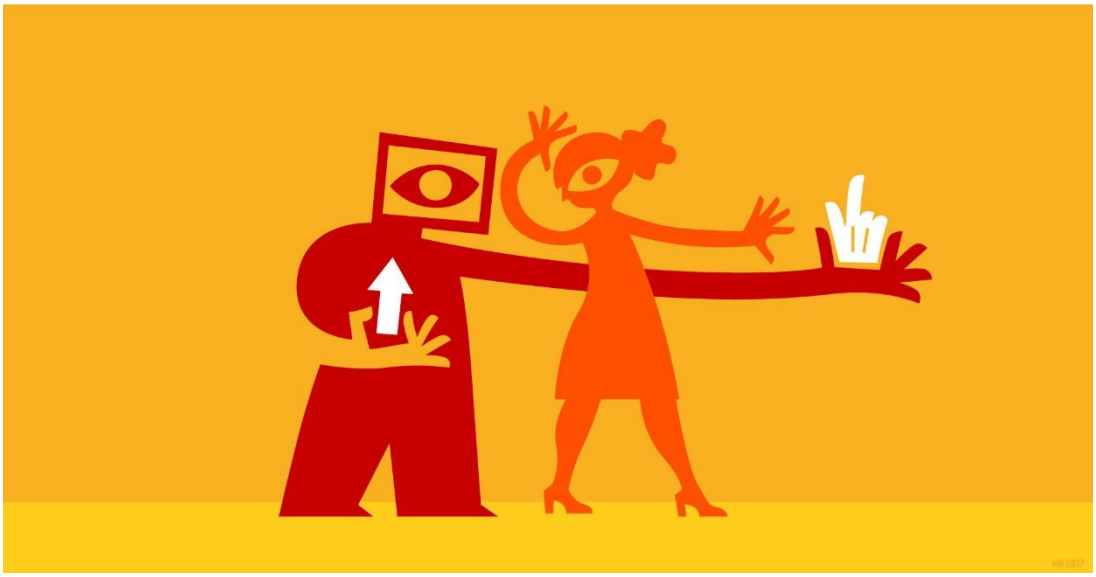
ICTU is an independent government foundation that works with and for authorities at all levels to build a better digital government. We too find it important to ask 'What can government do to optimise its digital services?'

9 This paragraph is published as a blog on September 29, 2017 on https://www.rathenau.nl/en/digital-society/ictu-people-digital-skills-or-services-people-skills

10 See https://www.nationaleombudsman.nl/nieuws/2017/hoezo-mijnoverheid

11 See https://www.kb.nl/sites/default/files/digitale_zelfredzaamheid_burger.pdf

We concur with the 2017 report Maak Waar[12] by the Information Society and Government Study Group, which states that the digitisation of government requires a radical change in attitude. And: ‘Digital service delivery is at the core of the primary process of government organisations. It must be actively organised around the wishes and requirements of the public and businesses.’ But how?



The ‘User Needs First’ community[13] thinks that online services can and should be more user-friendly. It is calling for government organisations to take a good look at those who use their services instead of putting the systems or the services themselves first. Looking at what users really need also helps boost people’s confidence in their digital skills and in government as a whole.

5 Design principles for user-friendly government services

The ‘User Needs First’ community has drawn up a list of design principles for more user-friendly government services. Similar principles already underpin the service delivery of such commercial organisations as Android, Windows and Facebook and the governments of the UK and the US. These five design principles are:

1. **Put the user first**
   Base the design on people’s needs, wishes and behaviour, and not on the technology or your organisation. Have real users test the process and design early on. Look at what users actually need, and don’t be obstructed by organisational or departmental boundaries.

12 See https://www.digitaleoverheid.nl/document/rapport-maak-studiegroep-informatiesamenleving-en-overheid/
13 See http://www.gebruikercentraal.nl/instrumenten/ontwerpprincipes/

2. **Do not rest until your user is satisfied**
   Design, test, measure, improve and then do it all again, and again. At ICTU we work with iterative processes, often according to the Scrum methodology. We work incrementally from the very start of the design process and test our outcomes continuously, leaving plenty of room for improvement. Even after implementation, there is a need to constantly monitor use and interpret the results.

3. **Make it easy for the user**
   Design straightforward processes, create user-friendly systems and write comprehensibly. A straightforward process needn't be simple, but it should always be clear to users where they are in that process, i.e. what they have already completed and what remains to be done. Service delivery doesn't start at the portal; how users get to the portal is at least as important. Are there links in relevant places? Is the service findable? And how do people know that they've arrived in the right place?

4. **Base yourself on facts, not on assumptions**
   Base your design on facts and don't assume that your user is just like you. Assumptions are made about the target group at every step of the process: demographic composition, needs, wishes, skills and behaviour. But 'assumption is the mother of all f***-ups', so test every single one.

5. **Be transparent and share your knowledge**
   Cooperate and share your knowledge and experiences. Remember the maxim 'Fail early, fail often, fail cheap'. The sooner you share results, the sooner you will get critical feedback, and the easier it will be to make changes. And as one unified government, we need to share lessons learned, both good and bad.

Let's stop talking about how to help people become digitally skilled or digitally independent; let's talk instead about how to improve our digital service delivery. Because maybe there is no such thing as digital illiteracy. At most, there are 'people-illiterate' systems, i.e. systems that don't know how to deal with real people.

Make digital facilities more people-literate
We can only increase the public's digital independence by making digital facilities more people-literate. Once we manage to do that, we may well see an automatic improvement in the people skills of digital government services.

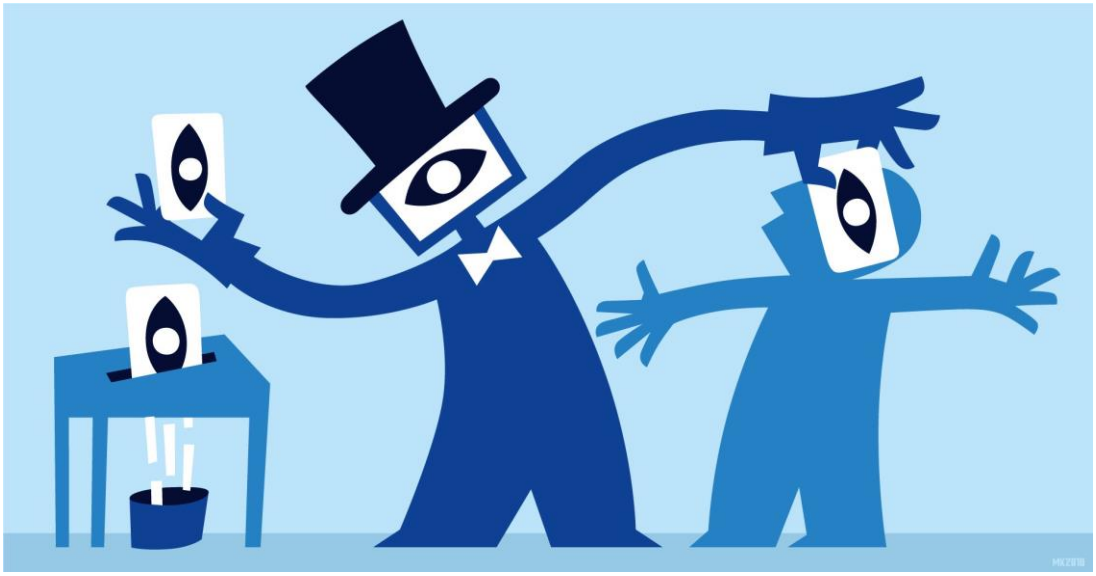
2 How can we stay in charge of algorithms?

Many people believe in algorithms. But do they understand how they work? This chapter discusses how we can stay in charge of algorithms. With contributions from the Dutch Police and Amnesty International, an algorithm expert and a cultural sociologist.

2.1 Algorithms are a magic show: super cool, but we just don't get it

By Marlies van Eck, writing in a private capacity. Her doctoral research at Tilburg University concerned automated chain decisions and legal protection. She works for the Dutch Ministry of Finance.[14]

Comedian Jochem Myjer's hilarious 'School Excursion' routine in his Yeee-Haa! cabaret show introduces us to country bumpkin Harm.[15] Harm is confused. Life to him is like a magic show; it's wonderful, but he doesn't understand it one bit. His standard expression is 'I just don't get it'.



In his 1976 book Computer Power And Human Reason: From Judgement to Calculation, Joseph Weizenbaum wrote that human beings approach artificial intelligence with too much respect and conviction, even though we don't understand it. He reached that conclusion after seeing how people responded to his ELIZA experiment, conducted between 1964 and 1966. Weizenbaum coded what we

14 This paragraph is published as a blog on May 18, 2018 on https://www.rathenau.nl/en/digital-society/marlies-van-eck-algorithms-are-magic-show-super-cool-we-just-dont-get-it

15 See https://www.youtube.com/watch?v=X2rQ3RaWGe8

would today refer to as a chat bot, a computer program that allowed people to communicate with a computer. The program, which he called ELIZA, parodied a 'real' psychotherapist by repeating or asking follow-up questions. A sample conversation:

> *Men are all alike.*
> *ELIZA: IN WHAT WAY*
> *They're always bugging us about something or other.*
> *ELIZA: CAN YOU THINK OF A SPECIFIC EXAMPLE*
> *Well, my boyfriend made me come here.*
> *ELIZA: YOUR BOYFRIEND MADE YOU COME HERE*
> *He says I'm depressed much of the time.*
> *ELIZA: I AM SORRY TO HEAR YOU ARE DEPRESSED*

It was patently clear to Weizenbaum that only a human being could help another human being resolve emotional issues. To his astonishment, however, the world beyond his lab embraced ELIZA with excitement. Various universities copied the program and it became famous across the United States. Weizenbaum was especially shocked at the enthusiasm of psychiatrists themselves, who felt that the program could be turned into an almost fully automated form of psychotherapy.

Weizenbaum observed something else: people who talked to ELIZA became addicted to the conversations they were having with it nd anthropomorphised the system. Even his secretary, who had seen him write the code, asked him to leave the room so that she could talk to ELIZA privately. While Weizenbaum's whole point was to prove that computers cannot truly understand our language, people thought that ELIZA demonstrated precisely the opposite.

This led Weizenbaum to observe that humans, regardless of their level of education, tend to ascribe exaggerated traits to technologies that they do not understand. This worried him, because he felt that some things were too important to entrust to computers.

Since Weizenbaum's day, government has come to use artificial intelligence or AI to take decisions for it. It isn't a civil servant who decides whether a person is entitled to benefit or how big a traffic penalty should be, but a computer. I wanted to study how the law is translated into computer instructions. But even when I was allowed to inspect certain documents, I ended up feeling just like Harm: I just didn't get it.

I had to conclude that in terms of automated decision-making, it isn't at all clear how government has interpreted the law. I was not able to study whether its

interpretation is correct and which choices it had made. That means that the law offers people less protection than before. Neither the public nor the courts know why a computer reaches its decision.

In essence, a judicial review consists of a conversation about the reasoning that government has applied. We are familiar with this mechanism in analogue society: when government takes action (grants a subsidy, frisks a person or issues a permit), that action is subject to numerous control mechanisms. People can object, they can submit a complaint, and they can take their complaint to a higher authority such as the national or municipal ombudsman or the court. The executive body must also account for the way in which it performs its tasks to the people's democratically elected representatives, such as the municipal council or the House of Representatives.

How strong are control mechanisms today?
But how strong are these control mechanisms when government uses algorithms? Over the next few years, this question will be an extremely important one in the relationship between government and the public, but also in the relationship between executive and judiciary powers. Perhaps we will need to seek new mechanisms, or perhaps algorithms will be required to explain themselves. Who knows?

We can start by disabusing ourselves of our belief in a smart algorithm that only does good things. Because what if it isn't so smart after all? Or if the black box turns out to be completely empty? To quote Weizenbaum, let's stop the 'sloppy thinking' and look critically at the things that we don't understand.

2.2 Technology is necessary to adapt to a rapidly changing society

By Erik Akerboom, Commissioner of the Dutch Police.[16]

Public discussion of self-learning algorithms justifiably focuses on the potential risks of software 'that we can't control anymore' and that leads to unwanted outcomes. Examples include software that tags certain neighbourhoods, communities or even individuals as high risk, leading to the police taking an unwarranted or excessive interest in them in their investigatory or law enforcement tasks. Or, conversely, they are tagged as low risk and, being largely ignored as a result, do not receive the

16 This paragraph is published as a blog on October 26, 2017 on https://www.rathenau.nl/en/digital-society/netherlands-police-technology-necessary-adapt-rapidly-changing-society

appropriate level of protection. People are also worried that their freedom will be severely restricted if historical data determines how they are perceived today and for the rest of their lives.

A job for the police

It is, however, also socially unacceptable for the police not to make use of technology that can improve public safety. In a constitutional democracy, the police must, by rights, steer a course between these two positions. Their task is always to strike the right balance; there are no conclusive answers.

There are many ways to use self-learning algorithms in the domain of security and justice, from detecting fraud to solving cold cases. At the same time, we understand all too well how important it is to supervise the algorithms themselves. See, for example, the recent policy briefing Big Data and Security Policies: Serving Security, Protecting Freedom by the Netherlands Scientific Council for Government Policy.[17]

Should we use algorithms to forecast crime?

An example: the Dutch Police recently featured in the news because of its Crime Forecasting System. The system uses historical data to detect patterns of crime, for example burglaries, muggings and robberies. The police uses these patterns to identify where best to deploy policing capacity. This then generates new data and follow-up questions about the efficiency, effectiveness and legitimacy of policing.

The Crime Forecasting System does not side-line professional judgement. Local, contextual knowledge remains important. Detecting crime patterns is not the same

17 See https://www.wrr.nl/publicaties/rapporten/2016/04/28/big-data-in-een-vrije-en-veilige-samenleving

as identifying the causes of crime. The Crime Forecasting System does not, for example, make it clear whether action on the part of a housing corporation would be more effective in certain cases than extra policing.

People adjust their behaviour in the light of new information. Targeted policing can, for example, cause criminals to move on to other victims, times of day, locations or methods. And it is not only real or potential criminals who are impacted by policing, but also numerous other parties, including ordinary people. Behaviour can shift, and it is precisely crime forecasting systems that can help us to remain agile as circumstances change.

Keep doing what we're meant to do

Having the police use self-learning algorithms does not mean we are moving towards a totalitarian state with omnipresent surveillance. In fact, almost the opposite is true. In an environment that is changing dramatically, it is important for the police to use technology to adapt quickly, so that we can continue to do what we're meant to do: be there for the people.

These two contrasting images are closely related to the sort of police that we – the people of the Netherlands – want in our society. On the one hand, we want the police to ensure the smooth and orderly operation of the state. In that respect, the police are primarily an instrument of the impersonal state, with the emphasis being on repression. On the other hand, the police are there to support and assist the people by protecting freedom and equality and by precluding the 'law of the jungle'. Striking the right balance – that is precisely the challenge that the Dutch Police faces. They do this in continuous and close interaction with many different parties and by contributing to the government-wide public debate, even at EU level.
We cannot limit ourselves to mere reflection. It is important to experiment with new information technologies, especially in the complex domain of security and justice. Because such experiments are critical to our ability to detect risks, assess outcomes and establish necessary criteria – for example for the protection of personal privacy. We focus largely on exploring options and also work with others in that respect, from local authorities to start-up firms.

Transparency and learning capacity

The deployment of these new technologies makes heavy demands on the learning capacity and transparency of the police. We involve academia, public and private parties, and civil society organisations – including those who are critical of us. There is an urgent need to carry on a sensitive and informed debate about technology and our fundamental rights. That debate will result in a police force that has gained enough trust to make significant advances in technology in cooperation with others.

2.3 Algorithms must respect human rights

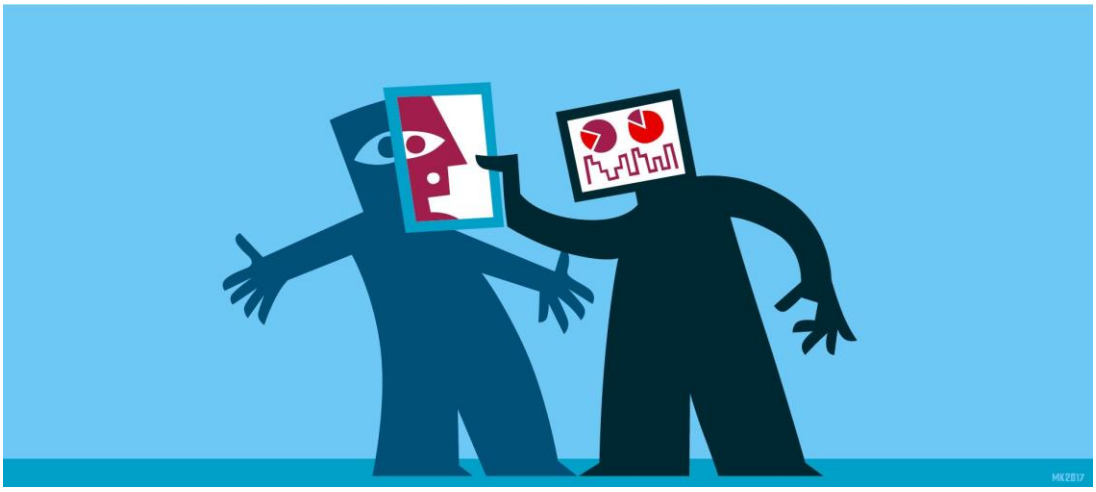
By Eduard Nazarski, Director of Amnesty International Netherlands[18]

The world will look very different in the near future than it does now. We are leaving more and more of our decisions to devices, based on data that they have collected and processed. Artificial intelligence is a tremendous advantage in many respects. Algorithms – sets of rules that draw conclusions from data – can relieve us of hazardous work and save us time. But we must be aware that they also pose numerous risks. Amnesty International has decided to investigate this subject.

Algorithms have infiltrated deep into our society:

- The Royal Netherlands Constabulary patrols the Dutch borders using profiles developed by an algorithm – in this case, a database assembled from road traffic surveillance data.
- The Municipality of Apeldoorn wants to use Big Data to predict the likelihood of juvenile crime in certain neighbourhoods.
- The Amsterdam police force uses software that predicts break-ins and muggings.

These organisations let computers search for data patterns and sometimes draw far-reaching conclusions from the findings. This form of data mining poses certain risks to human rights.



Algorithms seem objective. People have their biases, but technology does not – or at least, that's what we believe. Unfortunately, it's not that straightforward. Software

18 This paragraph is published as a blog on October 4, 2017 on https://www.rathenau.nl/en/digital-society/amnesty-international-algorithms-must-respect-human-rights

depends on the data that people feed into it. And those data aren't impartial by any means.

A study carried out by two researchers in the US, Kristian Lum and William Isaac,[19] is a case in point. They applied a predictive policing algorithm used in US police force software to the Oakland police department's drug crime databases. And what did they find? The software predicted that future drug crimes would occur in areas where police officers had already encountered many drug crimes. The researchers then added public health data on drug use. Based on the new data, the software predicted that drug crimes would also occur in many other parts of the city.

Fairness at risk

The police databases turned out to have a blind spot, in other words, and one that would have caused the Oakland police to overlook crimes in certain neighbourhoods. Self-learning software only makes it more likely that they would have continued overlooking these crimes in the future. Going by the software's advice, police officers would have only patrolled neighbourhoods with which they were already familiar. They would have recorded the crimes that occurred there in their database. The software would have then used the database to make subsequent predictions and would have overlooked any crimes unknown to the police in neighbourhoods with only minimum policing. Not only would this have put the effectiveness of policing at risk, but it was also unfair: the police would be addressing crime in one neighbourhood but not in another.

Attempts to circumvent this problem produce a human rights paradox: government either has databases with blind spots, or it links up many different databases, which is undesirable for privacy reasons.

Black box algorithm

One of Amnesty's other major concerns is the lack of transparency regarding what computer systems do with their data input. It is often impossible to see how the system reaches a certain outcome, making it difficult to test its accuracy. Users also don't notice if the system has made a mistake.

The lack of transparency has negative implications for the rule of law. Once an algorithm has identified you as a potential risk, how can you prove you are not if you have no insight into the rationale behind that assumption?
That brings us to the third important risk: who do we hold responsible for decisions, especially wrong decisions? If we allow algorithms to take decisions for us, either directly or because we base our own decisions on their advice, then who is

19 See https://hrdag.org/2016/10/10/predictive-policing-reinforces-police-bias/

ultimately responsible for that decision, the software developer or the person who uses the software? And who monitors whether the advice issued by the algorithm is actually correct? Where do victims obtain justice when no one can tell them who is responsible? These are questions that we need to discuss.

In June 2017, Amnesty International founded the Artificial Intelligence and Human Rights Initiative.[20] Its purpose is to arrive at a set of human rights principles for artificial intelligence and to launch a debate about the ethics of AI. In the Netherlands, we plan to organise a round-table meeting in the autumn about the police and the courts using predictive analyses. These are the topics that urgently call for dialogue:

1. **Prioritise human rights.** Programmers must understand the potential effects of their work on people and adhere to human rights standards.
2. **Promote justice.** We can do that by seeking solutions to the problem of biased data and software that compounds existing biases.
3. **Guarantee transparency.** We should not allow crucial decisions to depend on systems that we cannot monitor. The algorithms and the data that they use should be transparent for individuals as well.
4. **Agree on who's responsible.** We have to agree on who is responsible if an algorithm produces an erroneous outcome, and where victims can obtain justice.

Now is the time to start talking about how to deal with artificial intelligence. We need to talk to software developers and the organisations that use them: the government, businesses, the police and the court system. We also need a dialogue about this as a society. Because once algorithms become ubiquitous, there will be no way back.

2.4 We need civil weapons to protect ourselves against uncivil algorithms

By Siri Beerends, Cultural Sociologist at medialab SETUP.[21]

From tracking potential terrorists to hiring new employees, authorities and businesses are letting algorithms take more and more of their decisions. But what are the moral assumptions and mathematical simplifications lurking beneath these algorithms? And what decisions do we want to let algorithms take for us? To launch

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

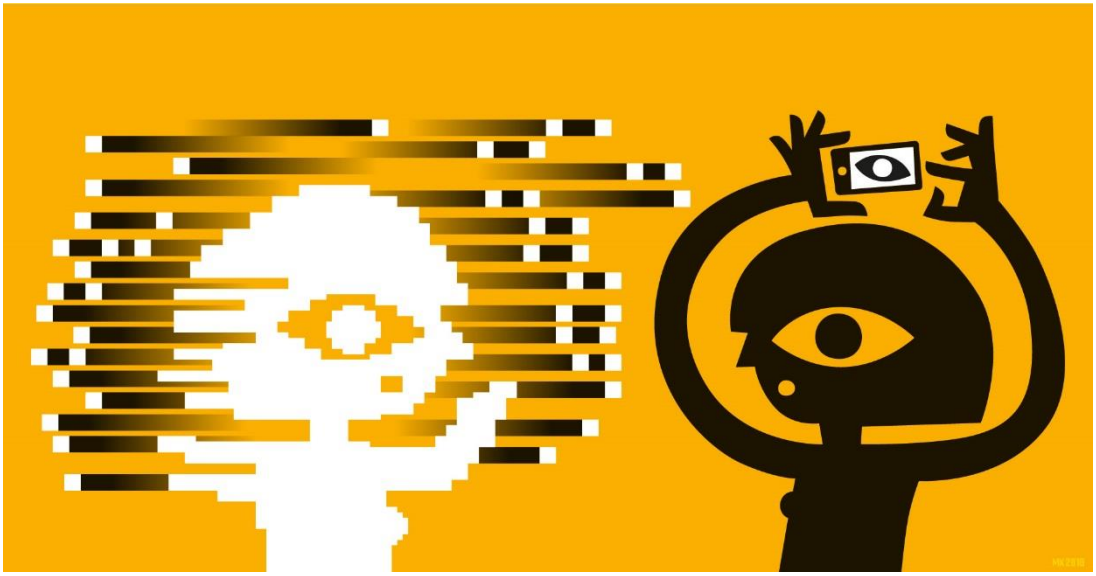
21 This paragraph is published as a blog on May 1, 2018 on https://www.rathenau.nl/en/digital-society/medialab-setup-we-need-civil-weapons-protect-ourselves-against-uncivil-algorithms

a public debate of this question, we need tools that will make decision-making by algorithms transparent and comprehensible.

One of the biggest misconceptions about algorithms is that they are neutral and that their decisions are therefore fair. Mathematician Cathy O'Neil shatters this illusion in her bestseller Weapons of Math Destruction. O'Neil claims that algorithms become 'weapons of math destruction' when:

- we don't know what moral assumptions underlie the scores that they produce and the decisions that they take, making it impossible to contest an algorithmic decision;
- algorithms encode human prejudices into software systems and disseminate them widely; and
- the decisions that algorithms take are destructive to society.

One example of a 'weapon of math destruction' is an algorithm that companies use to select the best CEO. Because women are under-represented among CEOs, the algorithm regards 'female' as a predictive factor for being an unsuitable CEO candidate.



GDPR offers weak protection

The EU's General Data Protection Regulation (GDPR) is due to enter into effect on 25 May. One of its purposes is to protect us against detrimental decisions by algorithms. It's a first step, but it doesn't go far enough. The regulation is vague about companies and authorities that take decisions based on derived data. It is also unclear about how to prohibit detrimental forms of algorithmic decision-making.

It does give individuals the right to object to their personal data being processed, but by then the damage has usually already been done. To what extent they can actually make effective use of that right is uncertain. How easy is it for an individual to intervene when algorithms take decisions in more complex environments and terms of reference?

There is still a clear distinction between police officers, the devices they use, and the IT company that develops their software, for example. But these separate worlds are merging and devices are taking more and more stand-alone decisions. Researchers warn that we are becoming a ‘black box’ society in which no one truly understands algorithmic decisions and how we can intervene.

All these developments make it vitally important that we understand the moral values, mathematical simplifications and biases that are encoded in algorithms. In addition to a public debate, we need tools to arm ourselves against detrimental decision-making by algorithms. Legal standards that limp along behind the commercial market are not enough.

That is why medialab SETUP is cooperating with artists and experts in a research programme that we have entitled Civil Weapons of Math Retaliation. The programme is meant to uncover the moral implications of algorithmic decision-making and ensure a fairer distribution of the power of moralising algorithms. That way people will not only have the right to object to a decision taken by an algorithm but will also be able to use algorithms to empower themselves.

Four design research projects

We will explore issues of autonomy, human dignity, and the desirability of algorithmic decision-making in a series of four design research projects. We will present two of our results on 25 May during the debate Living with Algorithms, organised by SETUP and the Rathenau Instituut.

Designer Isabel Mager is responsible for one of the four projects. On 25 May, she will introduce us to the world of recruitment algorithms. A growing number of companies are choosing to let algorithms screen job candidates. One of the leaders of the recruitment algorithm industry is HireVue, a company worth millions of euros that has Unilever and Goldman Sachs as clients. HireVue assesses videos of job candidates on word choice, tone of voice and micro-expressions that are said to reveal our true emotions.

Anyone who thinks that they are no longer being measured by algorithms once they’ve landed a job is wrong. The Dutch firm KeenCorp has developed an algorithm that measures the involvement of employees that measures employee

engagement by searching internal e-mails and chat messages for unconscious language patterns that indicate tension and personal involvement. In an extensive interview with SETUP[22] KeenCorp explains what their algorithm measures and how it contributes to improvements in the workplace.

Recruitment software companies claim that they liberate job candidates from the whims of biased employers. But this marketing promise is based on the misconception that technology is neutral. Consistency is not the same as neutrality, after all; the fact that an algorithm assesses every candidate in the same way does not mean that its assessment is neutral. In fact, the scores awarded by recruitment algorithms are based on all sorts of moral assumptions about personality types. For example, what about people who have friendly faces. Are they actually nice people?

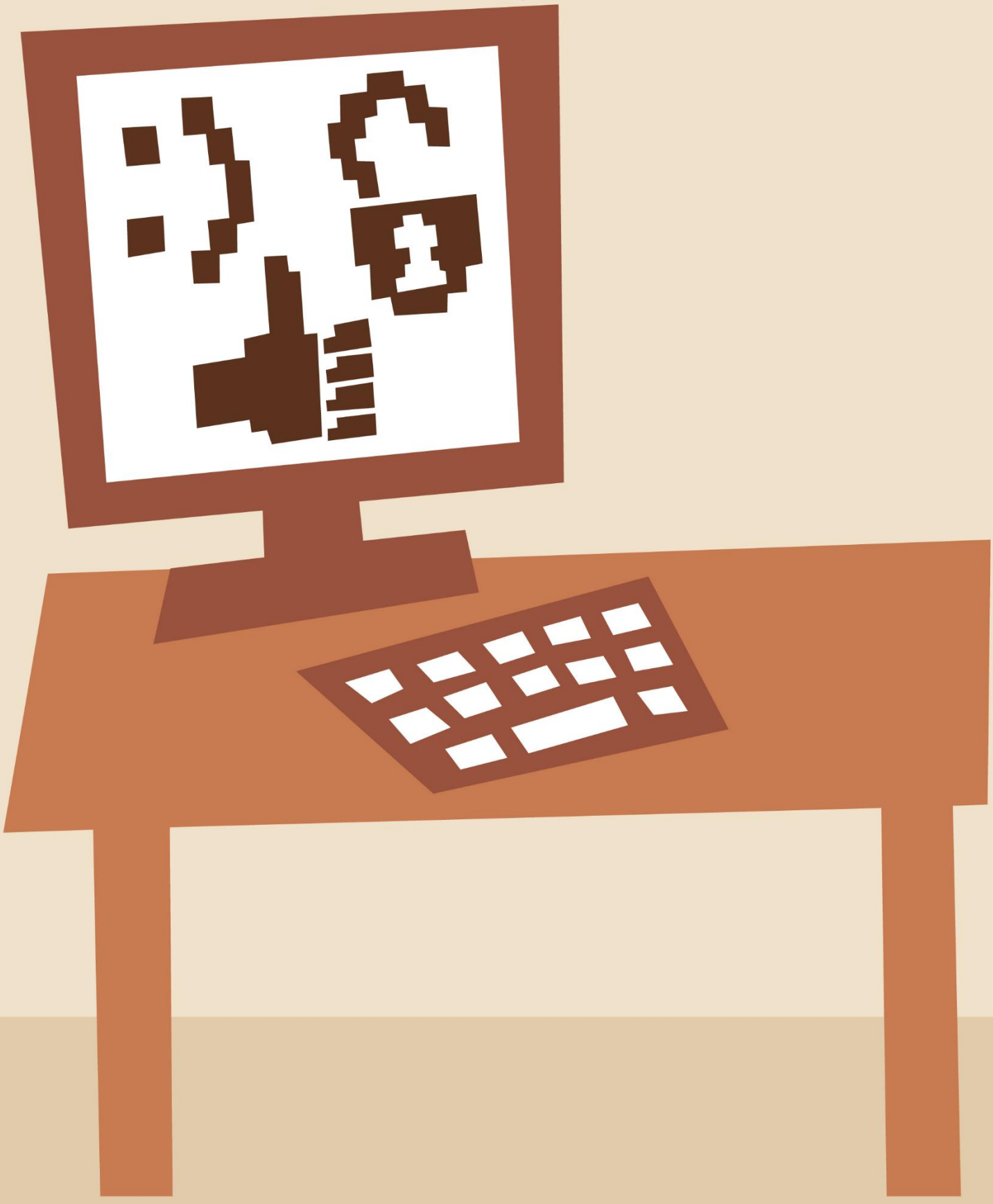
Isabel Mager will show us on 25 May how recruitment algorithms categorise and appraise job candidates during their video interviews. How do algorithms analyse our personalities and can we turn this to our advantage during a job interview?

Transparency is the first step on the road to empowerment
Making algorithmic decision-making more transparent is the first step on the road to empowerment. The next step is to understand what we're seeing. The 'Civil Weapons of Math Retaliation' programme will offer society telling examples, designs, presentations and a vocabulary that makes algorithmic decision-making comprehensible for a wider audience.

After all, all of us – and not just technicians – need to be able to talk about algorithms and decide, along with others, how we're going to live with them.

22 See https://www.setup.nl/magazine/2018/06/betrokkenheid-op-de-werkvloer-meten-met-een-algoritme-goed-idee

3 How can we help IT professionals to work ethically?



In this chapter, the sector organization KNVI, academics and privacy experts write about the role of IT professionals in an ethical digital society.

3.1 Let IT professionals identify violations of fundamental rights

By Leon Dohmen, Joan Baaijens and Liesbeth Ruoff, Board Members for Research and Training at the Royal Netherlands Association of Information Professionals.[23]

We know that digitisation is putting pressure on public values and fundamental rights such as privacy, justice and security. We also know that there are a vast number of companies, institutions and people involved in building the digital society, so we cannot single out one person, business or institution as the villain or the hero. If only it were that easy. Everyone has a part to play in keeping digitisation on the right track and ensuring that respect for fundamental rights remains intact.

That was one of the conclusions of a round-table meeting on digitisation and fundamental rights organised recently by the Royal Netherlands Association of Information Professionals (KNVI). Despite that conclusion, there is no denying that IT professionals play a crucial role. Bear in mind that it is these professionals – the product managers, functional managers, project coordinators, software architects, programmers and testers – who build the digital applications that are transforming society.

We think that they should be more conscious of the dilemmas that arise between digitisation and fundamental rights. Fundamental human rights take precedence over commerce and digitisation. Businesses, institutions and government organisations should create work environments where it goes without saying that IT professionals ask critical questions if they sense that fundamental rights are at risk.

Their input may not be welcome. IT professionals work in organisations where other, often commercial, interests prevail. And those interests may clash with their ethical and professional standards. In other words, there may not be any occasion at which they can raise their hands and object. It's vital that their workplace offers them the opportunity to do.

It's also vital to set up project operational structures to escalate alerts and findings to the appropriate level of authority. For example, a client and a project coordinator

23 This paragraph is published as a blog on February 19, 2018 on https://www.rathenau.nl/en/digital-society/knvi-let-it-professionals-identify-violations-fundamental-rights

can encourage their project team to speak up if they feel that an IT solution (under development) could be a threat to fundamental human rights. That would give IT professionals the chance to speak up as soon as they detect a risk. They should also be able to broach this subject with the product owners and/or management. In real life, that is seldom – if ever – the case.

The best way for IT professionals to draw attention to fundamental rights is by asking the right questions at regular intervals and in their everyday work. For example:

- Who will win and who will lose with this technology?
- Who is most likely to be hurt by this technology?
- What unwanted side-effects might this technology have?

IT professionals can ask these questions at regular intervals and at different points in time, in specific situations.

- For example, they can embed them in the popular ‘Scrum’ agile process.
- They can incorporate them into the product backlog as non-functional questions or standard ‘stories’. That ensures that both the development team and the product owner never lose sight of them.
- They can also make the questions part of their sprint review, when they demonstrate a tested, operational IT solution to stakeholders or to the people who will be working with the technology and in turn get feedback from them. The feedback round is another opportunity to ask the foregoing questions.

Businesses and government have a duty to protect

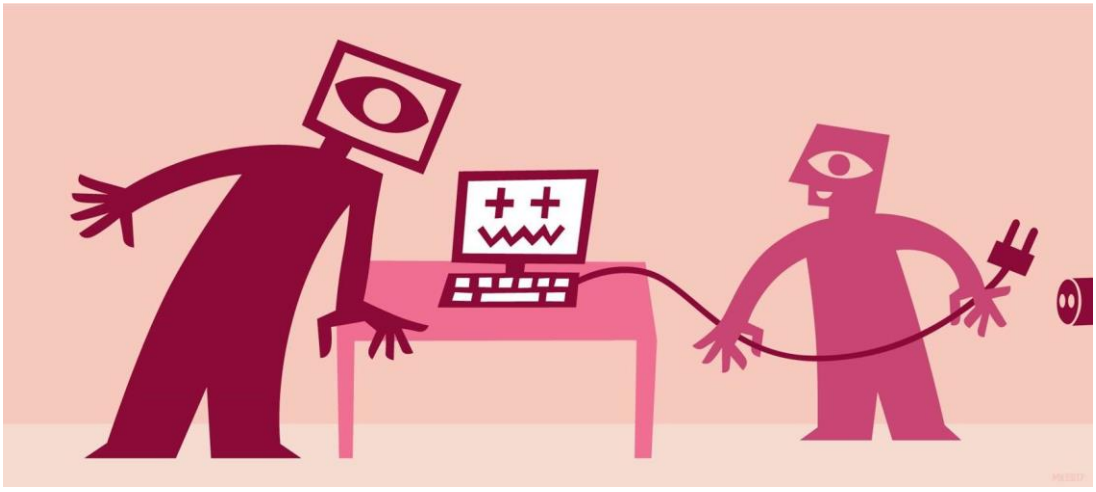
Businesses and government have a duty to protect fundamental human rights as digitisation proceeds. They must not permit these rights to be tampered with in the digital society. And as they are the actual builders of the digital society, IT professionals implicitly accept the same duty.

3.2 Programmers, embrace the responsibility befitting to your position

By Frans Stafleu, assistant professor of Ethics at Utrecht University & Linda Kool, senior researcher at the Rathenau Instituut.[24]

Software programmers have become so crucial to our society that we must regard their work as a profession –one whose conduct influences important public services and that requires not only technical expertise but also, and above all, sound ethical judgement. Programmers must also be able to act autonomously to produce effective work.

The traditional professions are those of doctor, lawyer and minister. Today, we must add programmers to that list, a move that naturally imposes a whole new set of responsibilities on them. They can either shoulder those responsibilities or accept that government will increasingly curtail their freedom to act.



Why have programmers become so important?

Now that digitisation is trickling into the very capillaries of society, the ethical aspects of programming are becoming increasingly prominent. Programmers provide the building blocks for many key public services, from self-driving cars to robot carers.

The digital and physical world are often closely entwined in those services. In that sense, a software program doesn't just perform a series of actions in the virtual world but often has a direct impact on the 'real', physical world. That means that a

24 This paragraph is published as a blog on November 29, 2017 on https://www.rathenau.nl/en/digital-society/ethicist-frans-stafleu-programmers-embrace-responsibility-befitting-your-position

tiny error in a software code can suddenly become a matter of life or death, for example if the wrong instructions are sent to an insulin pump.

The latest advances in artificial intelligence and autonomous systems are also raising new ethical questions in this context. The mobile phone, social media and smart assistants such as Alexa and Siri are changing relationships between people and between people and their devices. Programmers and businesses are suddenly facing the ethical implications of their work and the choices that society has scarcely considered, if at all.

For example, can you still be your uncensored self in your own home when all sorts of smart devices are monitoring your every move? Toy manufacturer Mattel recently scrapped plans to develop a virtual assistant for children, stating that it would be contrary to its corporate philosophy. In other words, programmers themselves are reinterpreting such ethical concepts as ‘privacy’.

Those who practise a profession must accept that they have a certain responsibility not only to protect the interests of society, but also because their professional conduct is murky and unintelligible to most clients, managers and policymakers. The latter must be able to *trust* that the professionals work ethically. Of course, that trust isn’t always justified, as the ‘diesel dupe’ software scandal at Volkswagen recently revealed.

Reality is so complex that it cannot easily be captured in a set of rules

This brings us to a critical dilemma. On the one hand, society wants the programming profession to be more heavily regulated and supervised, given how important software has become. On the other hand, the programmers themselves need to be free to act. After all, reality is so complex that it cannot easily be captured in a set of rules; each new situation requires the expert opinion and ethical judgement of the professional.

The dynamic relationship between society and programmer is clear: the more programmers act responsibly, the less government will need to intervene on society’s behalf. It’s up to the programmers, then. Their professional autonomy is at stake.

Ethical programming in two steps

Programmers can take the first step towards acknowledging their responsibility by drawing up their own code of ethical conduct. Codes of this kind are naturally more effective if they are compulsory. Enforcement is therefore the second step.

When a lawyer violates the code of conduct for the legal profession, he or she can be disbarred in accordance with standard review and complaint procedures. A similar system can be imagined for programmers.

In addition to codes, society can also rig up an enforcement structure. In exchange for codes and enforcement, it can allow the profession the freedom to take decisions based on expertise, experience and professional ethics, naturally within a certain statutory framework.

Various IT-related occupational groups have already started drawing up codes of ethics. The Association for Computer Machinery (ACM), for example, has had a Code of Ethics and Professional Conduct since 1999. The code states that members will:

- contribute to society and human well-being
- avoid harm to others
- take action not to discriminate, and
- respect the privacy of others.

Adherence to the code is voluntary, however. The ACM plans to issue a revised code in 2018.

International organisations such as the Institute for Electrical and Electronic Engineers (IEEE) and the International Federation for Information Processing (IFIP) also have or are involved in developing professional codes for programmers.

Pressure by lawmakers

At the moment, these codes are voluntary. It appears, however, that society will not be satisfied with general and non-committal initiatives. The European Parliament, for example, has called for a dedicated code of ethical conduct for robotics engineers, and the German Transport Ministry’s ethics committee has taken charge by becoming the first in the world to draft a set of ethical guidelines for self-driving cars.

Programmers are therefore under growing pressure to develop a mature professional culture that provides clear guarantees for ethical programming. How the scales tip between government regulation and professional self-regulation will be determined in the years ahead.

So it’s high time for Dutch programmers to get to work. Embrace the responsibility befitting your position in society. Being a professional is a burden, but also an honour. Accept it with verve!

3.3 We need technologies of humility

By Sheila Jasanoff, Professor of Science and Technology Studies at Harvard Kennedy School.[25]

Disruptive innovations are innovations that cause upheaval in society. They change our lives radically. For many people, disruptive innovations come as a surprise. That's odd, because science fiction films show that we are very good at imagining what happens when new technologies take over the world.

In the 1956 film Forbidden Planet, for example, human explorers on a distant planet have evidently been wiped out by a malign, superior intelligence; only two people and an enormous technological complex survives. In 2001: A Space Odyssey, released in 1968, one of the main characters is a clever supercomputer that can read lips – something that has become possible in the meantime. These films show us that humans have the imagination to think about the social implications of new technology. And that we're also capable of preparing ourselves for disruptive innovations.

Silicon Valley's 'every user for himself' ethos

The smartphone is an example of a disruptive innovation. From our social lives to our consumption habits, and from data security to mobility, smartphones are changing our behavior in unprecedented ways. The consequences are both positive and negative.

25 This paragraph is based on prof. Jasanoff's presentation on the ethics of invention, at an event of the Rathenau Instituut, and published as a blog on January 10, 2018 on https://www.rathenau.nl/en/digital-society/sheila-jasanoff-we-need-technologies-humility

What strikes me about the digital technology in smartphones and elsewhere is that it promotes the ‘every user for himself’ ethos of Silicon Valley. Take the payment app Venmo, which is very popular in the United States. When you dine out with friends, it will tell you precisely what each person owes. No one pays for a round of drinks anymore, or lends money trusting that good friends will always pay each other back. In other words, although it makes such transactions easier, it may also undermine long-cherished values like generosity and taking care of one another in everyday life.

Fortunately, we can tame new technology in all sorts of ways: the government can enact legislation, consumer preferences can regulate the market, and ethics can steer trends away from effects many see as harmful. But all these have their limitations.

First of all, two governance paradigms influence how we think about technology: the paradigm of risks and the paradigm of rights.

Why regulating technology is not enough

If we focus solely on risks, then we try to reduce the damage that technology can cause as much as possible. We dive into statistics and study complex expert reports. It’s a valuable strategy, but limited: in risk analyses, we almost always accept new technology without questioning why we need it in the first place. And there is limited public participation, because we let experts do much of the analysing and decision-making for us.

If we focus on rights, we ask how well technology actually reflects the rights and freedoms that we have enshrined in laws. This legal perspective usefully complements risk analysis. In the United States, for example, the courts moved to protect privacy in telephone booths and on cellphones at critical points on the ground that they carry the same expectations of privacy that people once attached to their homes and their thoughts.

Legal standards are not enough, however. Government regulation is often slow-moving and tends to follow market trends instead of leading them. And since regulation follows the initial design phase of technological systems, it often takes the form of damage control rather than social shaping.

The market is more immediately responsive to consumer preferences. However, the market too is an inadequate regulatory mechanism because of lock-ins already in place. It turns out, for example, that the new economy for sectors such as biotechnology isn’t actually creating a competitive and innovative market; instead, it is dominated by a few giants who bend innovation to protect their existing market

share. In addition, the environment too often loses out to the demand for short-term profits.

Even ethics is not enough

This brings us to ethics. Can greater ethical expertise convince governments to spur businesses to act responsibly, especially toward excluded or marginalized groups? Unfortunately, even ethics is just one piece of the puzzle. All too often, ethical committees emphasise individualistic values, for example bodily integrity, above collective values such as equality. Ultimately, moreover, the point is to encourage ethical reflection in every person instead of outsourcing it to groups of experts selected through opaque, possibly undemocratic processes.

So how should we deal with new technology?

We shouldn't be discouraged by all these critical remarks. Risk analyses, regulations, market instruments, and ethics all give us useful ways to shape the introduction of a new technology, but no mechanism is enough all by itself. For every new technology, we must leave ourselves time to stop and consider how to engage a wider range of social perspectives. And we should try to answer the following four questions:

1. Is there another way to evaluate the need that this technology is addressing?
2. Who is most likely to be hurt by this technology?
3. Who will win and who will lose with the adoption of this technology?
4. How can we learn and improve our understanding of this technology?

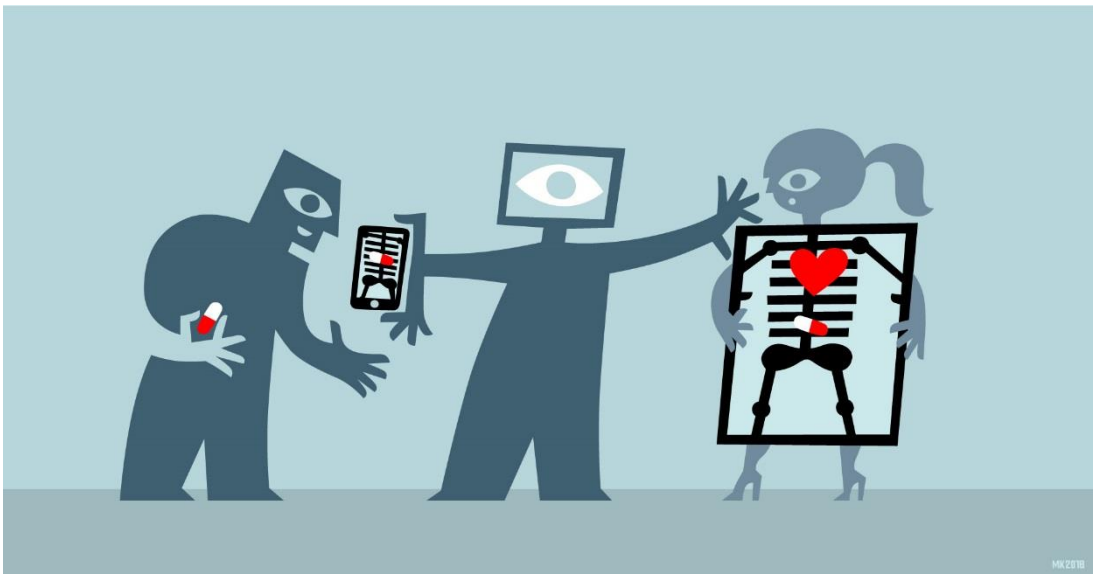
These are the technologies of humility that will help repair and strengthen social relationships against disruptions caused by new and emerging technologies. If we keep the negative distributive impacts under control, and consider lower-impact alternatives as needed, then we can use technology not to harm or destroy the world but to make it a truly better place.

3.4 Engineers, see that we can share the right data

By M. Birna van Riemsdijk, Assistant Professor of Intimate Computing at Delft University of Technology.[26]

'Germany bans children's "smart" watches over surveillance concerns.' [27] 'First Digital Pill Approved Leads to Worries About Biomedical "Big Brother".' [28] These two recent newspaper articles give examples of how digital technology is getting under our skin – both figuratively and literally.

Intimate technology of this kind allows us to collect and share personal and intimate data in all sorts of ways. That can be very useful, for example a 'digital pill' that reminds patients to take their medication. But intimate technology can also infringe our privacy, or diminish our sense of responsibility, when we share it with others because someone is always monitoring our behaviour and ready to intervene.



We must learn to develop tailor-made, context-sensitive technology. Today's technology is often designed to share all of the user's data. For example, digital pills share all the data showing the date and time of ingestion with the patient's doctor. Patients can withdraw their consent at any time, but they then share no data whatsoever. It's all or nothing.

26 This paragraph is published as blog on January 29, 2018, on https://www.rathenau.nl/en/digital-society/computer-scientist-tu-delft-engineers-see-we-can-share-right-data
27 See https://www.theguardian.com/technology/2017/nov/18/germany-bans-childrens-smart-watches-over-surveillance-concerns
28 See https://www.nytimes.com/2017/11/13/health/digital-pill-fda.html

I believe that there's another solution: a happy medium of flexible technology.

Design flexible software
Let's take the digital pill as an example. A patient who only occasionally forgets to take his medication doesn't need to share all his data with his doctor or family members. All he needs is for the technology to alert him directly. But there are some patients who constantly forget. In their case, data-sharing is important to give them the help that they need. The situation differs from one person to the next – and the technology should adapt accordingly.

The first step in developing this new type of personal and intimate technology is to redefine how we view technology: it is not there merely to collect and share data but should also help us do so responsibly. We can redefine that view by getting engineers to work with philosophers, for example in research teams.

These teams can apply the theory of technological mediation, which advises us to reframe the human-machine interface in terms of freedom rather than autonomy. Technology influences our behaviour and that means that our actions are never entirely autonomous, but we can exercise our freedom by being conscious of how we are using technology. Personal and intimate technology should support users in that respect.

We need software that knows what patients can do themselves
To ensure that technology provides this support, we need software models that allow users to agree on data-sharing protocols. For example, a patient and her family can agree that she takes her medication every day at 6 p.m. and that if she doesn't, the software will alert her family.

The software must also be capable of interpreting the agreements properly. What if it's 6.01 p.m. and the patient hasn't taken her medication yet? Should it alert the family immediately? Should it wait another 30 minutes? The right response depends on the situation.

Technology is not value-free
It should be up to users to decide how to share their data with others. This is critical. Technology is never value-free and all too often it lumps everyone into the same category. In the end, the point is to make our own, individual choices: how can technology support me in my chosen lifestyle? And in the way that I wish to share my life with others? Sharing personal data should no longer be a question of all or nothing, in other words. It's time for the happy medium.

3.5 Use open standards to break up monopolies

By Jaap-Henk Hoepman, director of the Privacy & Identity Lab at Radboud University.[29]

E-mail is one of the oldest internet applications still around, and it's fantastic. The only thing you need is an e-mail program and an e-mail address to which to send your message. E-mail is a very open, egalitarian application, available to everyone. The program you use to send your message is entirely up to you, whether that's Outlook, Gmail, or an app on your smartphone. The same goes for the recipient. Thanks to e-mail, everyone with an internet connection can communicate with everyone else.

That is precisely what the internet was meant for, and how it once was, at the beginning: open. And it sets an example for how the rest of the internet ought to be: based on open standards, interconnected, and with no one minding the gate and excluding certain users or applications.

That openness bears little resemblance to more recent internet applications such as social networks or messaging services. If I want to send a WhatsApp user a message, I need his or her telephone number and I have to have installed WhatsApp on my own phone. Apple's iMessage only works between iPhones. And if I have friends and colleagues who use Skype... well, as you might have guessed, I need to have a huge number of apps on my smartphone.

29 This paragraph is published as a blog on December 8, 2017 on https://www.rathenau.nl/en/digital-society/privacy-expert-jaap-henk-hoepman-use-open-standards-break-monopolies

The same is true of Twitter, Facebook, LinkedIn and Instagram. They are similar networks but they are not connected with one another. And that's just crazy. It's as if e-mails sent to Outlook users always had to be composed in Outlook. Or as if someone with a Nokia telephone could only receive text messages from another Nokia owner, and only if both parties had a contract with the same mobile network operator.

The Big Five killed the internet dream

The open internet of yore is now dominated by five big companies: Apple, Microsoft, Google, Amazon and Facebook. These 'Big Five' killed the original internet dream, each in its own way.

They did so because the services that they provide are monopolistic in nature. Or perhaps I should say: because we think that these services are monopolistic?

The idea seems logical at first glance: the more people using Facebook or WhatsApp, the more appealing it is to use Facebook and WhatsApp. After all, all your friends, acquaintances and colleagues already do. Thanks to this network effect, the value of the service rises exponentially with the number of users, making a monopoly seem almost inevitable.

But the same argument should also apply, say, for word processing programs. If, at a given moment, the vast majority of computer users use a certain word processing program tied to a certain document format, then it becomes almost impossible to work with others if you don't all use the same software.

And yet, it is possible to survive without Microsoft Word, the dominant word processing program. We can open Word documents in other applications because the document formats are 'open'. After long resistance, Microsoft has made it possible for us to work with Word users without having to purchase Word ourselves.

A closed format makes that impossible, because:

- it's hard to figure out everything that a document might contain and how it's all coded, and
- the software manufacturer can decide to change everything at any given moment.

We can break up the internet service monopolies by doing something similar: forcing the Big Five to use open standards and an open Application Programming Interface or API. The API for an internet service describes which commands can be sent to that service, how they must be sent, and what result that will produce. In the

case of e-mail, for example, the command is ‘send this message to this e-mail address’, the expectation being that this will happen as described.

We can compare an API to filling in and sending off a standard form to a government organisation, for example to request a parking permit or to report a change of address. All of the popular internet services – Facebook, Twitter, etc. – have an API. They allow your browser or the app on your smartphone to make use of their service.

But in many cases that service is not open, because there is no description of how to use the API (the ‘form’ has a secret format) or because a special key is needed to use the API (only authenticated ‘forms’ will be considered). When an API is open, third-party services or smartphone applications can use it too, and thus also make use of the service.

Stop dividing up the internet

If the API for WhatsApp were open, for example, then your iMessage would know how to send a message to a WhatsApp user. iMessage users would then have no trouble sending instant messages to WhatsApp users. In fact, we wouldn’t even need to know which app the recipient is using.

That would be a real blessing. Not only would it stop the division of the internet but it would also vastly improve the user experience of many services because people could continue using their favourite social network app or messaging app without excluding some of their friends.

The indirect praise I’m lavishing on e-mail isn’t entirely justified. E-mail is unbelievably user-unfriendly and an old-fashioned way of communicating. But the basic principles underpinning its design are timeless and invaluable. It’s time to apply the same principles to other internet services.

3.6 EU advances data dialogue

By Iris Huis in ‘t Veld and Arnold Roosendaal of Privacy Company, a team of consultants who help businesses and governments comply with privacy rules.[30]

The European Union has given us an important tool for creating the digital society that we desire: the General Data Protection Regulation (GDPR). Prior EU privacy

30 This paragraph is published as a blog on January 18, 2018 on https://www.rathenau.nl/en/digital-society/privacy-company-eu-advances-data-dialogue

legislation dates from 1995. In a society in which more data is available now than ever before, that legislation no longer adequately protects our right to privacy. The GDPR will go into effect on 25 May. The GDPR will bring about three major changes:

1. privacy supervisory authorities will be authorised to impose stiff fines;
2. there will be more rules for organisations that process personal data, and
3. citizens and consumers will have more and stronger rights.

Legislation is only one of many ways to influence the shape of society. Bottom-up initiatives can also make a difference. Privacy legislation is also often perceived as time-consuming and intimidating. That is in fact true: companies will have to set aside time to amend their practices to comply with the GDPR, which is more than 200 pages long. And a fine of up to 20 million euros is not to be sneezed at.

The GDPR is a stepping stone for ethical discussions

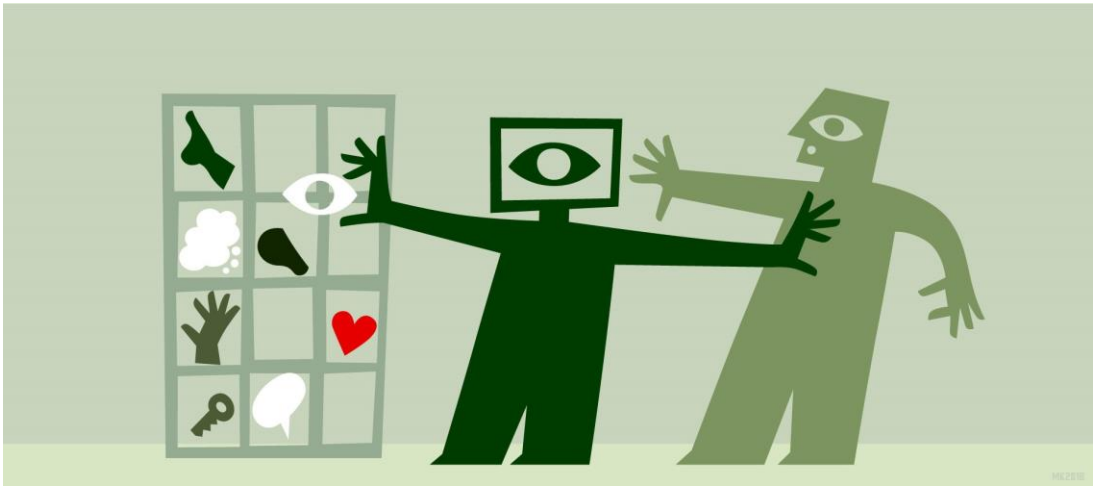
Even so, this new EU law deserves more praise. The GDPR has already raised the bar for ethical discussions about privacy. We notice that organisations are using the GDPR as a stepping stone for a serious dialogue about data. They are more likely now to ask themselves who their clients are, what they expect, and how their products and services can meet those expectations.

The GDPR will extend the rights of citizens and consumers. For example, someone who is significantly disadvantaged by automated decision-making can now question and fight that decision. ‘Computer says no’ is no longer an acceptable outcome, in other words.

This means that organisations must be more transparent in their use of artificial intelligence; they must be able to explain in clear and comprehensible terms how their algorithm works and how they reach their decisions. They must also introduce procedures that allow the decision-making process to be repeated without using the algorithm and with human intervention. So if a government agency refuses to pay out a benefit based on an algorithm, the relevant citizen can now force the agency to repeat the review processes without resorting to the algorithm.

When an organisation begins processing a new set of personal data, it will be obliged in some cases to conduct a – wait for it – ‘data protection impact assessment’. That will be the case if crime data are being processed, for example, or if public spaces are being monitored. The procedure consists of a risk assessment and a list of risk mitigation measures.

The risk assessment itself is extremely valuable. In our practice, we also often see organisations assessing ethical factors and societal risks along with the necessary legal risks.



‘Privacy by design’ will become standard
The GDPR will not only change procedures, then, but also, and most importantly, the mindset of organisations. They are already taking on board the principle of ‘privacy by design’: designing products and services in a way that anticipates privacy-related problems. For example, they can minimise data collection from the very start, choose to anonymise or ‘pseudononymise’ personal data, and invest in encryption and other data security measures.

Privacy by design could become an all-encompassing design philosophy, with programmers learning to consider ethical frameworks and with public values underpinning design choices.

All this will lead not only to corporate social responsibility; products and services that reflect public values will also cause the market to pick up. People are increasingly insisting on privacy-friendly products and services. For example, chat apps that use end-to-end encryption, such as Signal, are growing in popularity and more and more people are turning their backs on Google and using alternative search engines. A concern for public values also gives companies a competitive advantage, in other words.

The arrival of the GDPR gives us every reason to grasp these opportunities. The successful 21st-century organisation is an organisation that prioritises the interests of society and public values.

4 How can we protect children?

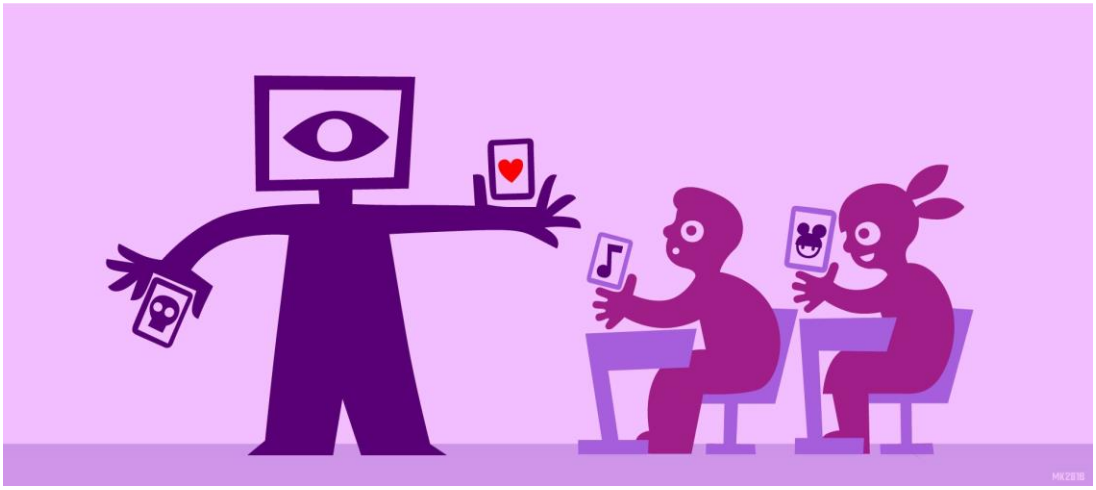
This chapter discusses how we can protect children online; with contributions from eLaw, Kennisnet and the Youth & Media Agency.

4.1 Schools need help in the battle for digital literacy

By strategic consultant Remco Pijpers and Kennisnet director Toine Maes.[31]

We all agree that we must go beyond teaching pupils 'regular' reading and writing. We also have to ensure that they become digitally literate and teach them to make safe and effective use of digital applications. In addition, we must prepare them for their digital future: throughout the rest of their education, in their working lives, as consumers, in social transactions, and in their dealings with government.

But what do we do about children who are at risk of missing the e-boat?



We used to worry about the gap between rich children and poor. Now, there's another worry: the gap between children who have mastered digital skills and those who have not. That gap will lead to more inequality in the job market, as noted by the Netherlands Institute for Social Research its report De toekomst tegemoet.[32]

Numerous reports emphasise how worried both pupils and teachers are about the potential losers of the information society. Kennisnet's survey of Youth and Media 2017[33] reveals that teenagers do not have the necessary digital skills, unless they are enrolled in pre-university programmes and have well-educated parents. Fortunately, things are set to change.

31 This paragraph is published as a blog on March 7, 2018 on https://www.rathenau.nl/en/digital-society/kennisnet-schools-need-help-battle-digital-literacy
32 See https://www.scp.nl/Publicaties/Alle_publicaties/Publicaties_2016/De_toekomst_tegemoet
33 See kennisnet.nl/fileadmin/kennisnet/publicatie/jeugd_media/Kennisnet_Monitor_Jeugd_en_Media_2017.pdf

- Curriculum.nu, a broad coalition of stakeholders in education, is developing ‘building blocks for digital literacy’. The Ministry of Education, Culture and Science and the Netherlands Institute for Curriculum Development (SLO) will use these building blocks to update the learning objectives and attainment aims in Dutch primary and secondary education respectively.
- The new objectives and aims are expected to be introduced in 2021. Primary and secondary schools will be working with them as of that year and digital literacy will become an integral part of the school curriculum. Children will then have to satisfy minimum requirements in terms of their digital theoretical knowledge and practical skills. All children will receive instruction in digital literacy, even those who are less academically inclined or who cannot depend on assistance at home.

Being attentive to digital literacy: three recommendations

The introduction of a new curriculum will not solve every problem straight away. The new objectives and aims introduced in 2021 are sure to make a difference in the long run, but more is required. There are three objections, for which we have three recommendations.

1. **Objection: Lack of evidence**
   As yet, we do not know to what extent digital literacy lessons will produce practical results for all pupils. That’s because we do not yet know precisely how children acquire digital skills. We are not really sure how to allow for differences in pupils’ digital skill sets.

   Recommendation: Encourage researchers to study pupil differences in digital skills and what method of instruction allows for those differences best.

2. **Objection: The new curriculum neglects the short term**
   The immediate, short-term problem is that children who are not encouraged to develop their digital skills at home risk falling behind even more. There is no way that schools can close that gap in the next few years. That’s why it’s important to invest now in extracurricular instruction. Fortunately this option is growing, but the relevant courses and programmes tend to emphasise programming skills, as an element of ‘computational thinking’. And it is precisely those skills that children who haven’t progressed beyond basic maths have trouble grasping.
   Recommendation: Extend extracurricular instruction in basic digital skills and in digital information skills to include courses and programmes suitable for vulnerable children from low-literacy homes.

3. Objection: Focusing on a qualification alone is not enough

What happens to children who are offered 'equal opportunities' but 'ignore' them? School managers and teachers at schools for children with severe learning difficulties are very worried. Despite all the tutoring and instruction, almost all their pupils end up in trouble and are seldom capable of thinking clearly about their behaviour and the behaviour of others on social media. For these vulnerable pupils in particular, it's important to move away from a unilateral emphasis on obtaining a qualification, with strict, quantifiable goals for digital literacy. Instead, we should talk to them about social conventions online, ensuring that they are 'heard' and that they feel comfortable and safe, including – and especially – in a digital environment. That doesn't happen often enough at the moment. Schools cannot create a safe digital context for vulnerable pupils by themselves, however. They need external help to do that.

Recommendation: Pay more attention to teaching vulnerable pupils safe online behaviour. Invest in special education. Have government, businesses and civil society organisations develop effective instruction programmes especially for these groups.

There ought to be a 'schoolspace' surrounding the cyberspace of children, one that is attentive to digital literacy and differences in digital skills, and that keeps close watch on pupils' safety online. But schools cannot create this 'space' by themselves; we must all act together to adopt the above recommendations.

4.2 We need leadership to battle cyberbullying

By Justine Pardoen, Founder of the Youth & Media Bureau / Parents Online.[34]

Children get bullied most between the ages of 10 and 15. That's when they slowly become more independent in their thinking, but they can also get caught up in group dynamics. Teasing – bullying – is part of growing up. And however optimistic parents and teachers may be, it really does happen everywhere –even online, for example when children send each other mean texts in group messaging apps or share photos that make other children look foolish.

Cyberbullying may be a natural part of growing up then, but it can be very painful for children and damage them for life. Bullying is ubiquitous and we must always try to stop it. Teachers play a crucial role in this. That's because their work gives them

34 This paragraph is published as a blog on March 27, 2018 on https://www.rathenau.nl/en/digital-society/youth-media-bureau-we-need-leadership-battle-cyberbullying

the best vantage point for seeing how children treat each other in a group. They have the children in their classroom and see them make friends and exclude others. Parents often do not have that overview. Teachers should therefore assume the role of leader and point the group in the right direction. They should not merely coach pupils by offering occasional advice; they must be strong women and men who set boundaries –and not only during school hours, but beyond as well.

Fear has us at a disadvantage

After all, it's precisely outside of school hours that things tend to go wrong. There are teachers who say 'I've got a private life too. Parents are responsible for what happens beyond the school gates.' But teachers cannot simply withdraw from the group process. They must remain available to children and engage in continuous dialogue with them. That is the best medicine against bullying.

Antibullying legislation and resilience training can never replace genuine personal engagement. In fact, governments, experts, parents and teachers all have a tendency to hide behind the rules, methods and advice. Fear has us at a disadvantage: the fear of actually engaging in dialogue with youngsters, and the fear of giving teachers the opportunity to do so.

Use new technology in the teacher-pupil relationship

Those teachers who remain engaged after school and, for example, spend an hour in the evening texting with their pupils about homework are often reprimanded. The Education Inspectorate warns teachers not to get too chummy with their pupils. In fact, teachers can improve their teacher-pupil relationships precisely by using the new technology.

Go ahead and tell your pupils that they can always text you if they really need to, 24/7. Get a second phone if you don't want them messaging you privately. It's

wonderful to have them see you as a confidante. You'll be the first to know when something's wrong, and you can take action. At the moment, school concierges often play that role. They receive a text message or tweet when a fight breaks out in the school playground and the teachers are all inside. Not many pupils feel called upon to be heroes, and they are relieved when someone steps in to stop bullying.

Prepare children for the future
Children will not ask other children in a group messaging app to stop bullying them, but they often do want to prevent things from going wrong. Make yourself available and join the group messaging app so that you have a powerful influence on the group process.

Teachers who are engaged can not only protect children against bullying but also prepare them for a digital world full of risks. Online gambling, 'shame texting', stalking – these are all things that children may come across. It is a tremendous help to them to be media literate, educated by an engaged teacher who knows the score.

It's a delight and a privilege to work with children. So teachers: show leadership and be a credit to your profession.

4.3 Protect kids online, but don't deprive them of their rights and freedoms

By Simone van der Hof, Professor of Law and Information Society at eLaw, Centre for Law and Digital Technologies, Leiden University.[35]

Imagine that your five-year-old daughter is playing football with a friend at a local playground. They're surrounded by a group of people who are writing down everything the two children do and don't do – are they being nice to each other, are they talented players? These people are always there, but no one knows precisely who they are and what they're doing with the information they're collecting.

Would you go along with this situation, as a parent? Of course not. And yet, in the digital world, it's become standard practice to continuously track, quantify and analyse children's behaviour. Fortunately, there is growing awareness that we have to put a stop to that. Rules are being drawn up and policies introduced to protect children's privacy. But that is precisely why we must be especially vigilant now: in

35 This paragraph is published as a blog on February 13, 2018 on https://www.rathenau.nl/en/digital-society/elaw-professor-protect-kids-online-dont-deprive-them-their-rights-and-freedoms

our eagerness to protect our children, we must not take away their freedom to develop.

Two documents are critically important for safeguarding children's rights. They are the EU's new General Data Protection Regulation (GDPR) and the United Nations' Convention on the Rights of the Child (UNCRC). But these two disagree on certain points.

Let's begin with the GDPR, effective 25 May 2018, which aims to improve consumer data protection and which takes a special interest in children, who are often unaware of the risks that personal data processing poses. For example, under the GDPR online service providers must have parents' consent before they can process the personal data of children under the age of 16. The overriding aim of the GDPR is to protect children.

The other document, the UNCRC, requires that in every decision by public and private parties concerning children, the best interests of the child must be a primary consideration. In other words, we must think of the children first. We must also consider children's rights in their totality. All of their rights are relevant, and not just their right to have their privacy protected. It is precisely this principle that may clash with the GDPR.

Protection of privacy at the expense of privacy

Let's take the GDPR's parental consent rule as an example. It could very well have a negative impact on the rights of children. Specifically, children will need a parent's consent for many of their online activities. Teenagers understandably don't always want their parents looking over their shoulder. That becomes problematical if

service providers are strict about applying the rule, since parents will be obliged to monitor their teenager's online activities.

Interestingly enough, this rule is at loggerheads with the notion that parents too must respect children's right to privacy. After all, children have the right to discuss sensitive topics with other children away from prying eyes and ears. Privacy is enormously important for children of any age.

At the same time, some companies are excluding children from their platforms. Google services such as Gmail block users who turn out to be younger than 16. Many schoolchildren make use of Gmail and get into trouble when they suddenly can't access their e-mail – and perhaps their homework.

Google is simply adhering to privacy law, but if the more stringent GDPR means that more companies will tighten the reins and exclude children from their services, then children's right to certain freedoms and to development is impacted directly: the right to obtain information and to express themselves freely, the right to access media, the right to privacy and freedom of association, the right to engage in play, and the right to an education. Unilateral protection rules can therefore have negative consequences.
In addition, it is doubtful that parental consent will actually offer much protection. It's an illusion to think that we as individuals control our personal data and that we can choose, or at least know, what happens to that data. We don't have that control and it is entirely unclear how personal data is processed in the inner workings of the internet.

Choose 'privacy by design'
But here too, there are solutions to hand. The principle of 'privacy by design' introduced in the GDPR makes it possible to use innovative means to build a child-friendly digital world. Creative app designers could turn their hand to making data practices in apps transparent in a manner that children of all ages can understand.

Even better would be to change the 'standard' and stop automatically observing and analysing children's online behaviour ('privacy by default') – or to anonymise their personal data immediately. Parental consent would be unnecessary then, and we would be safeguarding the rights of children.

Whatever choices we make in our eagerness to protect children, let's make sure that their rights and freedoms remain intact. Because that is ultimately in the best interest of every child.

Conclusion

We started this blog series last year in September. We called in experts from a wide variety of disciplines to show how we can bring decency to our digital society and keep it there. We threw down the gauntlet and saw that, in the main, government institutions, civil society organisations and researchers rose to the challenge. They shared their solutions in 17 separate blogs. In this concluding blog, we look at where we now stand.

Over the course of the year, we divided the blog series into various topics, for example ‘Ethical IT professionals’ and ‘Digital child-rearing’. The insights generated by the series transcend their specific context, however. Those insights can be described in terms of four virtues that can help us deal decently with digital technology:

1. personalisation
2. modesty
3. transparency; and
4. responsibility.

Together, these virtues reveal how politicians, policymakers and IT professionals can uphold public values such as fairness and autonomy in a digitising world. We examine each one below.

Personalisation: not everyone wants the same thing

The blogs repeatedly raise the point that people can’t all be lumped into the same category. For example, the National Ombudsman of the Netherlands comments that many people lack digital skills and lose their way in the government’s digital infrastructure. At the same time, there are large groups of people who have no trouble filing their tax returns or booking their wedding at city hall online. The message is that service providers must be sensitive to the differences between people and develop services that will allow for those differences. Or, as ICTU writes: ‘Maybe there’s no such thing as digital illiteracy. At most, there are “people-illiterate” systems.’

Digital personalisation is therefore a must, but it will require adaptability within digital systems themselves. Computer scientist Birna van Riemsdijk, for example, advocates digital pills that can share data in various different ways. After all, sometimes only the patient needs to know the data; in other cases, for example when a patient has dementia, it makes more sense to share the data with informal care-givers and doctors too. The next step is to talk to users about how they would

like to use digital technology. That will also help build support for digital innovation. Nictiz's blog, for example, shows that patients can only take charge of their own health when they receive personalised information and advice, and when companies involve them in developing e-health applications.

Personalisation also requires closer coordination between digital systems. In his blog, researcher Jaap-Henk Hoepman argues in favour of open systems, so that users are not locked into the technology of a specific provider. We should, for example, be able to send an iMessage to a WhatsApp account. Hoepman criticises the status quo, which is the very opposite: companies isolate their products from those of other providers and resist the introduction of uniform standards. That is bad for users' freedom of choice and thus for their ability to find a service that best suits their needs.

Modesty: know the limits of digital technology

To personalise their services, organisations must let go of the notion of digital absolutism. Not everything can or should be arranged digitally. Sometimes it makes more sense to reverse a decision to operate a wholly digital environment and leave an analogue channel open, as the UWV Employee Insurance Agency has done. Whether the issue is benefits, municipal bylaws or a child's living environment, the human world is rich and complex and not easily captured in algorithms.

That is why e-Law professor Simone van der Hof warns us that we should not lose sight of important human values when we consider the impact of digitisation on children. It is not in children's best interests to protect them at all costs, but neither should they be given complete and utter freedom. Only a nuanced approach can offer children a safe, private environment in which they are allowed to make mistakes too.

Or as Sheila Jasanoff puts it: humility is essential. Because let's be honest: the digitisation projects of the past ten years haven't all been winners. Of course there have been successes in medical diagnostics and the digitisation of cars, but for each and every success we can also point out a crisis – and successes often give rise to new risks.

Just think of the many major IT projects that ended up being more expensive than anticipated. Digitisation is seldom easy and involves much more than a simple, straightforward efficiency operation. That is something that organisations should realise from the very start. It is therefore laudable that the Dutch Police insists on linking experiments with algorithms that advise on policing to the scrupulous protection of democratic rights.

Transparency: watch out for an algorithmic ‘black box’
Transparency is a key requirement for personalisation and the targeted use of digitisation: people must know enough about technology to say what they actually want, and policymakers need the right information to recognise opportunities and threats. Unfortunately, it is precisely transparency that sometimes goes missing.

For example, Marlies van Eck writes that automated chain decisions by government are anything but transparent for the public or even civil servants. They do not understand how decisions about benefits or tax assessments come about and are powerless to set things straight in individual cases. That undermines the public’s legal protections.

Medialab SETUP and Amnesty International Netherlands are also worried about the algorithmic ‘black box’ that takes in data and spits out decisions. Algorithms are coded by fallible human beings, who can make programming mistakes or input substandard datasets. Algorithms that have not proved themselves beyond a doubt are nevertheless being used in all sorts of ways, for example in employee recruitment procedures. The lack of transparency is also a concern for democracy. When all is said and done, the Netherlands is a country where politics is meant to respond to the worries and wishes of citizens – but without proper information, how can we adequately express those wishes in the first place?

The challenge, then, is to educate the public and policymakers and offer them a better understanding of how algorithms work. That is precisely where technology itself can play a constructive role, by creating applications that explain things like automated chain decisions in an entertaining and comprehensible manner. But once again, we must respect the limits of the possible. Digital technology is growing increasingly complex, certainly when it comes to deep learning systems that use a huge number of variables in their calculations. Even programmers do not always understand these systems. That's why it is not enough to call on the public, politicians and civil servants to learn the skills needed to control technological innovation; we also need to ensure that the right parties are charged with the right responsibilities.

Responsibility: dare to take the plunge
The blogs offer numerous suggestions for how to do this. To begin with, Linda Kool and Frans Stafleu argue that as a group, programmers – like doctors and lawyers – practise a profession that impacts society, one that requires sound ethical judgement. Programmers need to acknowledge their special responsibility and understand how their products and services are changing the way people live.

The argument put forward by the Royal Netherlands Association of Information Professionals (KNVI) is entirely in line with this idea. They too believe that information professionals need to bear in mind fundamental rights and freedoms and public values; perhaps even more importantly, their workplace should give them the opportunity to ask ethical questions and to alter plans where necessary.

Other parties also have certain special responsibilities. In the educational context, Justine Pardoen zeroes in on teachers: they must show leadership in guiding their pupils through the digital world and teaching them how to respect others and navigate safely online. Kennisnet offers a broader view; it recommends supporting schools with extracurricular instruction, auxiliary programmes and research.

The way ahead is, in any event, clear: decide who is responsible for what. Only then will society move forward. The recent introduction of the EU's General Data Protection Regulation makes this clear. Privacy Company writes enthusiastically that many companies and other organisations are using the GDPR as a stepping stone for a serious dialogue about data collection and processing. This offers proof that a growing number of people are aware of the challenges of digitisation and courageous enough to acknowledge their responsibilities in that regard.

Decent Digitisation? We've only just begun

The Rathenau Instituut is pleased with this intriguing blog series. Our authors have shared inspiring insights with us and helped us to see the practical side of vital ideals. There is no doubt that we need their inspiration. Because although the Netherlands is more aware of the implications of digitisation than it was five years ago, has a better grasp of the ethical issues involved, and has shown more willingness to take responsibility, many questions remain unanswered. The virtues discussed above offer us all a good place to start, but they need to be incorporated into real solutions, such as technical applications, codes of conduct or statutory frameworks.

We will be keeping a very close eye on developments as they unfold. And while this particular blog series has come to an end, the Rathenau Instituut will continue publishing on this topic and asking stakeholders in society what they think. Decent digitisation? We've only just begun.

Open Access
The Rathenau Instituut has an Open Access policy. Reports and background studies, scientific articles and software are published publicly and free of charge. Research data are made freely available, while respecting laws and ethical norms, copyrights, privacy and the rights of third parties.

Contact
Rathenau Instituut
Anna van Saksenlaan 51
P.O. Box 95366
2509 CJ The Hague
The Netherlands
+31 70 342 15 42
info@ Rathenau.nl
www.Rathenau.nl
Publisher: Rathenau Instituut

The Rathenau Instituut stimulates public and political opinion forming on social aspects of science and technology. We perform research and organise debate relating to science, innovation and new technologies.

Rathenau Instituut