Rathenau Instituut

Human rights in the robot age

Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality

Report

Parliamentary Assembly
Assemblée parlementaire

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Human rights in the robot age

Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality

Rinie van Est & Joost Gerritsen, with the assistance of Linda Kool

This report was commissioned and funded by the Parliamentary Assembly of the Council of Europe (PACE) in the framework of preparation of the PACE report on “Technological convergence, artificial intelligence and human rights” (Rapporteur for the PACE Committee on Culture, Science, Education and Media: Mr Jean-Yves Le Déaut, France, SOC) which was adopted by PACE on 28 April 2017.

Rathenau Instituut
Anna van Saksenlaan 51
P.O. Box 95366
2509 CJ The Hague
The Netherlands
Telephone: +31 70 342 1542
E-mail: info@rathenau.nl
Website: www.rathenau.nl
Publisher: Rathenau Instituut

Proof reader: Beverly Sykes
Design cover: Max Beinema Graphic Design
Layout: Rathenau Instituut
Print: Rathenau Instituut
Cover photo: iStock

Preferred citation:
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

Preface Rathenau Instituut

Smart devices surveilling our lives. Artificial intelligence technologies steering our behaviour. Care robots hindering human contact. Does this sound terrifying? Inevitable? It does not have to be. Time for a wake-up call.

The Rathenau Instituut was established more than thirty years ago. Its mission: to research the societal impact of new technologies and developments in science. Since then, our research has illustrated the notion of this convergence: the growing interaction between nanotechnology, biotechnology, information technology and cognitive technology. This report elaborates on NBIC convergence, with a special focus on the connection between human rights and technological convergence, in particular technologies concerning robotics, artificial intelligence, and virtual and augmented reality.

The report demonstrates that these technologies can have a positive or a negative impact on human rights. Regarding these rights, we focus on issues relating to the right to respect private life, human dignity, ownership, safety and liability, freedom of expression and the prohibition of discrimination as well as access to justice and the right to a fair trial.

The Rathenau Instituut conducted this research on the invitation of the Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe (PACE). Our research shows that the human rights framework forms a practical starting point for policy makers tasked with regulating robotics, artificial intelligence or similar technologies. However, in certain cases clarification on the rights is needed. We therefore argue in favour of two, novel, human rights: the right to not be measured, analysed or coached, and the right to meaningful human contact.

I would like to thank PACE, and Mr. Le Déaut in particular, for the invitation, enabling us to further elaborate on our body of work in order to explore emerging technologies and the challenges that arise from a human rights perspective. We hope that our report provides inspiration in future discussions.

The technologies described in this report can be of great benefit to us all. However, in order to maintain our human dignity and fundamental rights, we have to remain vigilant, remembering our values as laid down in the conventions and apply these in practice. Fortunately, robots or AI do not determine the rules, but society does. It is possible, if needed, to draft policies before technologies take over. The legislators of the Oviedo Convention on Human Rights and Biomedicine recognised this earlier. We therefore trust that our wake-up call will be carried on by the Council of Europe to also protect our human dignity in the digital age.

Melanie Peters
Director Rathenau Instituut

Preface Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe (PACE)

Science and technology are having an increasing impact on society. The new challenges of the digital age, synthetic biology, artificial intelligence and genome editing are leading to accelerated changes as their applications enter the market, but the understanding of them is incomplete.

These technological fields combine nanotechnology, biotechnology, information technology and cognitive technology (NBIC). They represent very powerful developments, often characterised by their irreversible and uncertain nature.

The boundaries between the medical and the non-medical and the non-living and the living are fading. We have moved on from a human being that is taken care of well to a healed person, and what is looming on the horizon now is an enhanced human being.

The Rathenau Instituut has written a high-quality report which analyses these new technological advancements against the background of bioethical principles.

The protection of personal data, the fair and lawful processing of big data and the Internet of Things all create challenges for the legislator, because there is no real transparency in relation to algorithms. The right to respect for private life is a concern too, since various IT applications aim to change people's attitudes or behaviour. Such persuasive activities may undermine people's autonomy and self-determination, and also their freedom of thought and conscience.

So-called electronic coaches allow a form of voluntary self-monitoring, but in reality the recorded data create digital representations of the self in an opaque manner.

Care robots have been equipped with artificial intelligence, but they could influence the quality of human relationships by keeping the individual in a virtual world.

This report analyses the safety of robots and artificial intelligence artefacts and the respective responsibilities of the designer, the operator and the user, as well as the consequences for human dignity, freedom of expression, ownership, the security of robots and artificial intelligence artefacts, discrimination and access to justice.

It is on the basis of this thorough and relevant analysis that I propose as rapporteur for the Parliamentary Assembly of the Council of Europe (PACE):

- to strengthen the legislation of the public authorities and equip individuals with legal means to resist pressures or constraints that would subject them to technologies which would enhance their performances,
- to ensure transparency and raise public awareness,
- to define the responsibilities of the actors involved in automatic processing aimed at the collection, use and treatment of personal data,

- to create a common normative framework for artificial intelligence artefacts,
- to require that any machine, robot or artificial intelligence artefact remains under human control,
- to establish a right to be let alone, that is to say a right to refuse to be subjected to profiling, to have one's location tracked or to be manipulated, and the right to meaningful human contact,
- to establish cooperation between the Council of Europe, the European Union and UNESCO to develop a harmonised legal framework and regulatory mechanisms at the international level.

Innovation is desirable if it provides a service to society. Progress is useful if it is controlled and shared. This report by the Rathenau Instituut and my parliamentary report that includes the recommendations of the Council of Europe both agree that we are working towards achieving a fine balance between artificial intelligence and human rights.

Jean-Yves Le Déaut
President of the Parliamentary Office for Scientific and Technological Assessment (OPECST),
General Rapporteur for Science and Technology Impact Assessment of the Parliamentary Assembly of the Council of Europe (2014–2017)

Contents

1 Introduction

Background

As the continent's leading human rights organisation, the Council of Europe has a long-standing history of anticipating and coping with the downsides of new technologies in the face of human rights and human dignity. For example, triggered by developments in the field of biotechnology, the Parliamentary Assembly advised the Council of Europe in 1991 to start preparing for a convention on bioethics. In 1997, this led to the European Convention on Human Rights and Biomedicine (Oviedo Convention). The purpose of this Oviedo Convention is laid down in article 1: 'Parties to this Convention shall protect the dignity and identity of all human beings and guarantee everyone, without discrimination, respect for their integrity and other rights and fundamental freedoms with regard to the application of biology and medicine.' Furthermore, article 2 of the Oviedo Convention clearly instructs that 'the interests and welfare of the human being shall prevail over the sole interest of society or science'.

Recently, there has been a growing awareness within the Council of Europe that a new wave of emerging technologies, enabled by technological convergence and including big data, robotics and artificial intelligence (AI), is raising all kinds of ethical and social issues that may be highly challenging in the light of current ethical frameworks and regulatory regimes. Prompted by this, the Committee on Bioethics of the Council of Europe (DH-BIO) in May 2015 organised The International Conference on Emerging Technologies and Human Rights.[1] DH-BIO concluded that 'there is a clear need to look into these new developments in order to be able to respond to the possible ethical and legal challenges raised by these new technologies and their convergence'. This challenge was picked up by the Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe (PACE). In June 2015, a motion was tabled that pleaded for 'a forward-looking debate by the Parliamentary Assembly'.[2] In September 2015, Mr. Le Déaut was appointed as rapporteur in order to write a report on 'Technological convergence, artificial intelligence and human rights'. This exercise is driven by the notion that it might be wise to apply some of the basic guiding principles of the Oviedo Convention – such as the protection of private life, respect for autonomy, the right to information and informed consent – beyond the biomedical field. Its aim is that the Council of Europe will come up with proposals for the governance of converging technologies in order to safeguard human rights, such as the right to bodily integrity, privacy and freedom of thought. In order to complete this report, PACE has looked for cooperation with various knowledge partners. It asked the Rathenau Instituut to write a concise, background expert report on the above-mentioned topic. The current paper is the result of that request.

On 22 March 2017, the Committee on Culture, Science, Education and Media discussed the draft recommendations made by the rapporteur. The draft recommendations were adopted unanimously.[3] On 28 April 2017, the Parliamentary Assembly unanimously adopted an amended version of the recommendation[4] based on the rapporteur's report.[5] See Box 1.1 for the full text of the recommendation from the Parliamentary Assembly.

[1] Council of Europe, 'Emerging technologies', http://www.coe.int/en/web/bioethics/emerging-technologies.

[2] Council of Europe – Parliamentary Assembly, 'Technological convergence, artificial intelligence and human rights', 24 June 2015, http://www.assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=21951&lang=en.

[3] Council of Europe – Parliamentary Assembly, 'Intelligent artefacts should not challenge different dimensions of human rights', 22 March 2017, http://assembly.coe.int/nw/xml/News/News-View-EN.asp?newsid=6556. Council of Europe – draft recommendation, 10 April 2017, http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23531&lang=en.

[4] Council of Europe – Parliamentary Assembly, Recommendation 2102 (2017) Provisional version, 28 April 2017, https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23726&lang=en.

Box 1.1 Overview of Recommendation adopted by PACE on 28 April 2017

Recommendation 2102 (2017) Provisional version
Technological convergence, artificial intelligence and human rights

1. *The convergence between nanotechnology, biotechnology, information technology and cognitive sciences and the speed at which the applications of new technologies are put on the market have consequences not only for human rights and the way they can be exercised, but also for the fundamental concept of what characterises a human being.*
2. *The pervasiveness of new technologies and their applications is blurring the boundaries between human and machine, between online and offline activities, between the physical and the virtual world, between the natural and the artificial, and between reality and virtuality. Humankind is increasing its abilities by boosting them with the help of machines, robots and software. Today it is possible to create functional brain-computer interfaces. A shift has been made from the "treated" human being to the "repaired" human being, and what is now looming on the horizon is the "augmented" human being.*
3. *The Parliamentary Assembly notes with concern that it is increasingly difficult for lawmakers to adapt to the speed at which science and technologies evolve and to draw up the required regulations and standards; it strongly believes that safeguarding human dignity in the 21st century implies developing new forms of governance, new forms of open, informed and adversarial public debate, new legislative mechanisms and above all the establishment of international co-operation making it possible to address these new challenges most effectively.*
4. *The Assembly recalls the principle enshrined in Article 2 of the Convention on Human Rights and Biomedicine (ETS No. 164, "Oviedo Convention") which affirms the primacy of the human being by stating that "the interests and welfare of the human being shall prevail over the sole interest of society or science".*
5. *In this regard, the Assembly welcomes the initiative of the Council of Europe Committee on Bioethics to organise, in October 2017 on the occasion of the 20th anniversary of the Council of Europe Convention on Human Rights and Biomedicine, an international conference to discuss the prospect of the emergence of these new technologies and their consequences for human rights, with a view to developing a strategic action plan during the next biennium 2018-19.*
6. *In addition, the Assembly considers that it is necessary to implement genuine world internet governance that is not dependent on private interest groups or just a handful of States.*
7. *The Assembly calls on the Committee of Ministers to:*
   - *7.1 finalise without further delay the modernisation of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) in order to have new provisions making it possible to put rapidly in place more appropriate protection;*
   - *7.2 define the framework for the use of care robots and assistive technologies in the Council of Europe Disability Strategy 2017-2023 in the framework of its objective to achieve equality, dignity and equal opportunities for people with disabilities.*
8. *In the light of the above, the Assembly urges the Committee of Ministers to instruct the relevant bodies of the Council of Europe to consider how intelligent artefacts and/or connected devices and, more generally, technological convergence and its social and ethical consequences related to the field of genetics and genomics, neurosciences and big data, challenge the different dimensions of*

[5] Council of Europe – Parliamentary Assembly, 'Intelligent artefacts should not challenge different dimensions of human rights', 28 April 2017, https://assembly.coe.int/nw/xml/News/News-View-EN.asp?newsid=6624&cat=8.

human rights.

9. *Moreover, the Assembly proposes that guidelines be drawn up on the following issues:*

   9.1 strengthening transparency, regulation by public authorities and operators' accountability concerning:

      9.1.1 the fact that responsibility and accountability lies with the human being, no matter the circumstances. References to "independent" decision making by artificial intelligence systems cannot exempt the creators, owners and managers of these systems from accountability for human rights violations committed with the use of these systems, even in cases where the action that caused the damage was not directly ordered by a responsible human commander or operator;

      9.1.2 automatic processing operations aimed at collecting, handling and using personal data;

      9.1.3 informing the public about the value of the data they generate, consent to the use of those data and the length of time they are to be stored;

      9.1.4 informing everyone about the processing of personal data which have originated from them and about the mathematical and statistical methods making profiling possible;

      9.1.5 the design and use of persuasion software and of information and communication technology (ICT) or artificial intelligence algorithms, that must fully respect the dignity and rights of all users and especially the most vulnerable, such as elderly people and people with disabilities;

   9.2 a common framework of standards to be complied with when a court uses artificial intelligence;

   9.3 the need for any machine, any robot or any artificial intelligence artefact to remain under human control; insofar as the machine in question is intelligent solely through its software, any power it is given must be able to be withdrawn from it;

   9.4 the recognition of new rights in terms of respect for private and family life, the ability to refuse to be subjected to profiling, to have one's location tracked, to be manipulated or influenced by a "coach" and the right to have the opportunity, in the context of care and assistance provided to elderly people and people with disabilities, to choose to have human contact rather than a robot.

10. *The Assembly reiterates its call made in Resolution 2051 (2015) "Drones and targeted killings: the need to uphold human rights and international law" on all member States and observer States, as well as States whose parliaments have observer status with the Assembly, to refrain from any automated (robotic) procedures for selecting individuals for targeted killings or any sort of injury based on communication patterns or other data collected through mass surveillance techniques. This should be true not only for drones but also for other combat equipment with artificial intelligence systems, as well as other equipment and/or software which might potentially inflict damage on people, property, personal data or information databases, or interfere with privacy, freedom of expression, or the right to equality and non-discrimination.*

11. *The Assembly calls for close co-operation with the institutions of the European Union and the United Nations Educational, Scientific and Cultural Organisation (UNESCO) to ensure a consistent legal framework and effective supervisory mechanisms at international level.*

Structure of the report

The invitation from PACE to the Rathenau Instituut was probably made because of earlier work done by the Rathenau Instituut that explored the societal meaning of so-called NBIC convergence, that is, the growing interaction between nanotechnology, biotechnology, information technology and cognitive technology (cf. Berloznik et al. 2006; Van Est & Stemerding 2012; Van Est 2014; Van Est et al. 2014; Kool et al. 2015; Royakkers & Van Est 2016; Van Est et al. 2016). This report will elaborate on this body

of work, with a special focus on the connection between human rights and technological convergence, on particular trends in robotics, AI, and virtual and augmented reality.

In chapter 2 we introduce the notion of NBIC convergence. We explain how technological convergence enables two engineering megatrends: 'biology is more and more becoming technology' and 'technology is increasingly becoming more biology' (Arthur 2009). Because of these trends we are now experiencing the historic tipping point at which the distance between technology and ourselves is rapidly decreasing. We have become very intimate with technology; in other words we have become human–machine mixtures, that is, cyborgs. Historically, the relationship between human rights and the 'human biology is becoming technology' trend has received considerable attention from a human rights perspective; see, for example, the Oviedo Convention. In contrast, the link between human rights and the 'technology is becoming biology' trend has received very little attention so far. To address that blind spot, this report focuses on that trend.

In chapter 3 we look at the 'technology is becoming biology' trend from a human rights perspective. To make that connection, in our research we looked at six specific technologies: self-driving cars, care robots, e-coaches, AI that is used for social sorting, judicial applications of AI, and virtual and augmented reality. For each of these cases we map the various social, legal and ethical issues that are already in play or might come into play and relate them to established human rights, for example the rights as set down in the Convention for the Protection of Human Rights and Fundamental Freedoms, also known as the European Convention on Human Rights (ECHR).[6] We illustrate how these six technologies might strengthen or challenge certain human rights. This has been organised as follows. After the introduction in section 3.1, we describe rights related to privacy in section 3.2, which includes the right to the protection of personal data, the right to respect for private life and the right to respect for family life. The next section describes how human dignity may be affected, especially in relation to the use of care robots. We then describe how ownership issues affect the notion of the right to property. Section 3.5 deals with safety, responsibility and liability (tort rights). The next three sections are dedicated to how automated decisions may affect freedom of expression, the prohibition of discrimination, access to justice and the right to a fair trial (sections 3.6, 3.7 and 3.8). The last section (3.9) proposes two 'novel' human rights: the right to not be measured, analysed or coached and the right to meaningful human contact.

In chapter 4 we reach our conclusions and set out a list of recommendations which the Council of Europe could take into account.

Note on our methodology

The source material of international organisations – such as the Council of Europe and the European Commission – has been used as the primary source for the report's background investigation. Owing to the broad nature of the 'technology is becoming biology' trend that is part of NBIC convergence, the scope of this investigation has been limited to the above-mentioned technologies (self-driving cars, care robots, e-coaches, AI, and virtual and augmented reality). This approach shows the very diverse set of human rights implications of these technologies. However, this report neither provides a complete set of emerging technologies that are part of NBIC convergence nor an exhaustive list of possible human rights challenges. The research was conducted in the period July 2016 to April 2017. The terminology used in this report builds on the body of work from the Rathenau Instituut.

[6] The ECHR is available at: http://www.echr.coe.int/Documents/Convention_ENG.pdf. The protocols to the ECHR are available at: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/results/subject/3.

This report pays special attention to the report entitled 'Civil Law rules on Robotics' of the Committee on Legal Affairs (JURI Committee) of the European Parliament, chaired by MEP Mady Delvaux.[7] The JURI Committee adopted its report, which included recommendations for the Commission, in January 2017 as part of a motion for a resolution. It calls on the Commission to propose legislation regarding smart robots. It also suggests a system of registration of advanced robots, to be managed by an EU Agency for Robotics and AI. The report also provides suggestions on how to deal with liability for damage caused by robots. As an annex to the resolution, the report contains a Code of Ethical Conduct for Robotics Engineers (which contains ethical principles for robotics engineering) and a Code for Research Ethics Committees.

With regard to the notion of human rights, the authors stayed as close as possible to the rights and freedoms as laid down in the ECHR and – when data qualify as personal data – Convention 108 and its Protocol.[8] Where appropriate the report refers to EU legislation, most notably the Charter of Fundamental Rights of the European Union, the General Data Protection Regulation and the e-Privacy Directive (to be repealed by the e-Privacy Regulation).

[7] European Parliament News, 'Robots and artificial intelligence: MEPs call for EU-wide liability rules', 16 February 2017, http://www.europarl.europa.eu/news/en/news-room/20170210IPR61808/robots-and-artificial-intelligence-meps-call-for-eu-wide-liability-rules.

[8] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and its Additional Protocol regarding supervisory authorities and transborder data flows are available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

2 Converging technologies converging with humans

Technology becoming biology and vice versa

Technological innovation often results from combining different technologies, so-called technological convergence. Currently, such convergence is taking place on a massive scale, since four technological revolutions are propelling each other, being the nano-, bio-, information and cognitive technologies. This dynamic quartet is known as NBIC convergence. NBIC convergence signifies an increasing interaction between the life sciences, which have traditionally studied living organisms, and the natural or engineering sciences, which have traditionally studied and built non-living systems. This merger is reflected in two bioengineering megatrends: 'biology is becoming technology' and 'technology is becoming biology' (Arthur 2009; Van Est & Stemerding 2012).

The first trend implies the promise that in the future living systems, such as genes, cells, organs and brains, might be engineered in much the same way as non-living systems, such as bridges and electronic devices. This expectation is driven by the fact that the engineering sciences provide more and more ways to measure, analyse and intervene in living organisms. Genetically modified bulls, cloned sheep and dogs, cultured heart valves, bacteria with complete synthetic genomes, human germline editing, deep brain stimulation and persuasive technologies illustrate this trend. The trend of 'technology becoming biology' refers to the ambition of engineering properties we associate with living organisms, such as self-assembly, self-healing, reproduction, intelligent behaviour and autonomy into man-made technology. This trend thus embodies a (future) increase in artefacts that are inspired by biological, cognitive and sociocultural systems. Examples of bio-inspired artefacts are engineered stem cells and 3D-printed artificial blood vessels. Humanoid or android robots, avatars and AI are examples of cogno- and socio-inspired artefacts.

Technology in and close to us, between us, about us and just like us

When we look at our own techno-human condition, the two engineering megatrends support the notion that humans are becoming more and more intimate with technology (Van Est 2014). We let technology nestle itself within us, close to us and between us. And as a result, this technology can be used to collect a huge amount of data about us and mimic facets of our human characteristics.

First, technology is nestling itself within us or very close to us. Besides biological techniques, such as pharmaceutical pills or gene therapy, numerous IT-based interventions are also emerging, such as RFID chips, electronic pills, cochlear implants, artificial balance organs and artificial retina. Technology can thus become part of our body and sometimes even our brains, and therefore our identity. Technology also comes between us, on a large scale. Think of smart phones, activity trackers, social media, massively multiplayer online games and augmented reality glasses. These digital machines penetrate our private and social life and increasingly influence how humans interact.

Because we accept that these machines nestle themselves within us, close to us and between us, they can be used to collect a lot of information about us. Through our interactions with the machines that surround us – such as cameras, GPS, smart shoes, DNA chips, face-recognition technologies, Internet search engines and smart cars – we are being digitally measured. Think about digital data on our genetic make-up, health, thoughts, feelings, preferences, conversations and whereabouts. These data are not gathered without a purpose, but are often used to profile human beings in all kinds of ways with the explicit goal of intervening in human processes. These three steps in the digitisation of human life –

measuring, profiling and intervening – link directly to the three general processes that make up the value chain of big data: collection, analysis and application (cf. Roosendaal et al. 2014). The three processes together create a *cybernetic feedback loop*.

Finally, some technologies get more and more human-like features. Machines can have human traits and we can be touched by their outward appearance, and how they mimic human activities, such as driving a car, exhibit intelligent behaviour or even show emotions. Think, for example, of self-driving cars, social robots, digital assistants, chatbots, Google Translate and IBM Watson Health, this last functioning like a clinical decision support system for use by medical professionals. It is important to note that the ability of these machines to mimic human features or activities is often enabled by the fact that a lot of digital data exists about these human activities. Google uses the digitised data of human translation, for example data generated by human translators within the European Parliament, to train its algorithms. Thus, gathering a lot of digital data about us enables engineers to create artefacts that behave just like us, and this can therefore even increase the interaction between humans and machines.

We may conclude that in this digital age we are experiencing an ongoing merger between humans and machines. To put it more bluntly, we have become techno-humans, mixtures of humans and machines, that is, cyborgs. In this report we want to study this intimate interaction between technology and humans from a human rights perspective.

Studying the merger between humans and machines

So far, the bulk of the bioethical debate and related human rights treaties has focused on invasive biomedical technologies that work inside the body, or 'technologies within us'. It has been commonly recognised that there is a strong connection between biomedical technologies and human rights. The Oviedo Convention is shaped around this premise, and created common guiding principles – such as the protection of private life, respect for autonomy, the right to information and informed consent – to preserve human dignity in the way humans apply innovations in biomedicine. Above it was outlined that in the meanwhile there exists a broad range of technologies that work outside the body but still impact the bodily, mental and social performance of human beings. Like biomedical technologies, these new, emerging ICT-based technologies also raise all kinds of ethical, social and human rights issues (cf. Stahl et al. 2016). Safeguarding human dignity in the 21st century, therefore, forces us to look at all kinds of intimate technologies, that is, technologies inside us (such as deep brain stimulation), but also technologies close to us (such as EEG neuromodulation) and between us (such as social media), technologies that gather a lot of information about us (big data) and technologies that behave just like us (for example robots and smart environments). This report aims to address the relationship between a broad range of intimate technologies and human rights. Since the link between intimate technologies within us and human rights has been widely studied, debated and regulated, this report focuses on human rights issues related to non-invasive intimate technologies: technology close to us, between us, about us and just like us.

To indicate this cluster of technologies, the term the Internet of Things (IoT) is often used. The Internet has penetrated the whole of society since it has become available in ever more places, especially through the smartphone. Modern robotics is based on these existing networks and consequently changes the nature of these networks. Through robotics the Internet is given 'senses' by means of sensors, and 'hands and feet' by means of actuators. In this manner, an Internet of Robotic Things is being shaped. A broad set of emerging ICTs, such as sensor networks, the Internet, big data, AI and robotics, is playing a role in this development. The pervasiveness of these ICTs is ever increasing and leads to a blurring of the distinctions between humans and machines, between our online and offline activities, between the physical and the virtual world and between reality and virtual or augmented reality (cf. Floridi 2015). To indicate this human condition, the term *onlife* has been used (ibid.).

In this onlife world we interact with all sorts of intelligent or digitally coded artefacts. We name four characteristics of these intelligent artefacts to illustrate the many ways in which we interact with them. The first characteristic concerns the environments that artefacts inhabit. Some intelligent artefacts can only thrive in a digital environment. These intelligent artefacts are called software agents or softbots. Intelligent artefacts that can thrive in the physical world are physical robots. Physical robots can be seen as physically embodied AI. Secondly, intelligent artefacts can have a certain degree of autonomy. When a human is in control of what the machine does, the human is said to be 'in the loop'. When a human is in the loop, the location of the operator and the machine may be different. This makes it possible for people to act remotely. When the machine acts autonomously, the human is said to be 'out of the loop'. When the human and machine are both partly in control, the human is said to be 'on the loop'. Thirdly, the interaction between humans and these intelligent artefacts is also shaped by their appearance. If the soft or physical robots look like machines, one speaks of mechanoids. Animal-like and human-like robots are called humanoids. Humanoid robots that are built to aesthetically resemble humans are called androids. Finally, the way we perceive the world can be mediated in various ways by intelligent artefacts – think of virtual or augmented reality.

Each type of interaction between humans and intelligent artefacts can raise various human rights issues. This report cannot provide a complete picture. We investigate six specific technologies: self-driving cars, care robots, e-coaches, artificial intelligence (AI) that is used for social sorting, judicial applications of AI, and virtual and augmented reality. The selection of these six cases has been guided by the four characteristics of intelligent artefacts that are described above. As a result we expect that our study will provide a sufficiently broad overview of the human rights issues that relate to converging technologies, in particular robotics and AI.

3 Human rights related to intelligent artefacts

3.1 Introduction

This chapter examines how six different types of intelligent artefacts – self-driving cars, care robots, e-coaches, AI that is used for social sorting, judicial applications of AI, and virtual and augmented reality – may strengthen, challenge or infringe our human rights. With respect to the impact of technology on human rights, we adhere to Kranzberg's adage: 'Technology is neither good nor bad; nor is it neutral' (Kranzberg 1986). This implies that technology can have a diverse set of social and ethical consequences, but that we should be aware of the fact that these impacts can vary significantly according to how and the contexts within which the technology is used. Because the design of technology plays an important role in how technology impacts human lives and fundamental rights, design choice is a recurring theme within this chapter.

Intelligent artefacts may challenge different dimensions of human rights, for example in terms of freedoms (privacy and data protection, ownership, autonomy, personality), equality (more specifically, non-discrimination) and justice (fair trial, access to justice). Regarding human rights, we primarily refer to the principles laid down in the treaties, charters and documents of the Council of Europe or, where appropriate, the principles as set out in the Charter of Fundamental Rights of the European Union. Thus, the impact of intelligent artefacts is first discussed in the context of seven existing human rights: the right to respect for private and family life (3.2), the right to human dignity (3.3), the right to the peaceful enjoyment of possessions (3.4), tort rights and safety (3.5), the right to freedom of expression as well as the freedom of thought, conscience and religion (3.6), the prohibition of discrimination (3.7) and access to justice as well as the right to a fair trial (3.8).

In addition, section 3.9 elaborates on two potential 'novel' rights: 1) the right to not be measured, analysed or e-coached, and 2) the right to meaningful human contact. These two novel rights are indirectly related to, and aim to elaborate on, existing human rights, such as, respectively, the classic privacy right to be let alone[9] and the right to respect for family life. These rights might be needed to protect humans' interests in a society where not only have 'machines' been put into humans – which is (in part) covered by the Oviedo Convention – but also where humans are becoming more and more part of 'machines', that is, the Internet of Robotic Things.

The preceding chapter introduced the value chain of big data, which consists of collection, analysis and application of data. This chapter will reflect on how different types of value chains challenge different human rights. The Internet has proved itself to be a powerful tool for collecting, analysing and applying data. The Internet has also enabled the arrival of *surveillance capitalism*, which is characterised by massive data collection and analysis, psychological experimentation and personalised persuasion (Zuboff 2015). We are now witnessing the rise of the Internet of Robotic Things, which, as explained in chapter 2, gives the Internet 'senses' and 'hand and feet', and thus provides, compared to the Internet, numerous new ways to gather data and intervene in our daily lives. With regard to the Internet, the actions are initiated by software bots – or softbots – and with regard to the Internet of Robotic Things

[9] As advocated by Warren and Brandeis (1890). These authors created this concept that aims to protect an individual's sphere of confidentiality against public or private interferences.

these are robots with a physical appearance ranging from a utensil to an almost human-like robot. To a certain extent, human rights issues that have been identified and that relate to the virtual world of the Internet also apply to the mixed virtual and physical world of the Internet of Things. However, in certain cases, emerging robot technologies impact human rights in a different manner. This chapter aims to clarify these similarities and distinctions between the Internet and softbots and the Internet of Things and physical robots.

3.2 The right to respect for privacy

The right to respect for privacy

Never in our history has there been so much data collected about so many individuals, stored in so many places and analysed and used. Strand and Kaiser (2015, 13) argue that there is 'considerable uncertainty about how this development may affect the right to privacy as a basic element in the human condition for personality development'. In fact, they comment that this uncertainty in itself is a major concern. This section explores to what extent physical robots or softbots challenge the right to respect for privacy by looking at various application contexts.

When referring to 'the right to the respect for privacy', we refer to the right to the protection of personal data as explicitly mentioned in article 8(1) of the Charter of Fundamental Rights of the European Union and as laid down in Convention 108 as well as to the right to respect for private life as laid down in article 7 of the Charter of Fundamental Rights of the European Union and article 8 ECHR.[10]

We first investigate how the protection of personal data is challenged by softbots that operate via the Internet, mostly via the World Wide Web, and how the right to personal data protection is impacted by physical robots, as part of the Internet of Robotic Things. We then focus on how, respectively, softbots and physical robots might affect the right to respect for private life, both in the virtual (Internet) world and in the physical environment. Lastly, we describe how physical robots may interfere with the right to establish and develop relationships with other human beings.

3.2.1 Protection of personal data

Protection of personal data and regulations

The primary business model of the Internet is built on mass surveillance (Schneier 2013). For instance, Facebook processes data about its 1.86 billion members who are active each month,[11] and sometimes about people who are not a member of this social media website (Roosendaal 2012; Van Alsenoy et al. 2015).[12] Kosinski et al. (2013) claim that the surfing behaviour of Facebook users (for example their number of 'likes') may reveal a lot of sensitive personal information about these users' lives, such as their age, gender, sexual orientation, ethnicity, religious and political views, personality traits, level of

[10] See also, with regard to the right to privacy, article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights. Because of the scope of this report, the human rights impact of the investigated technologies have not been tested against these provisions.

[11] CNN tech, 'Facebook is closing in on 2 billion users', 1 February 2017, https://money.cnn.com/2017/02/01/technology/facebook-earnings/.

[12] Currently, the Belgian Data Protection Authority is involved in legal proceedings on the merits against Facebook about the tracking of non-users via its datr-cookie and social plugins. See: Belgian Commission for the Protection of Privacy, 'Hof van Beroep wijst eis tegen Facebook af', 30 June 2016, https://www.privacycommission.be/nl/nieuws/hof-van-beroep-wijst-eis-tegen-facebook-af (Dutch). Prior to these legal proceedings, *The Guardian* reported that Facebook has admitted that it tracked non-members, but it stated that the tracking only happened because of a bug that is now being fixed; see: S. Gibbs, 'Facebook admits it tracks non-users, but denies claims it breaches EU privacy law', *The Guardian*, 10 April 2015, https://www.theguardian.com/technology/2015/apr/10/facebook-admits-it-tracks-non-users-but-denies-claims-it-breaches-eu-privacy-law. From May 2016, Facebook has indicated that it will deliver 'better ads' to everyone, 'including those who don't use or aren't connected to Facebook'. See: Facebook Newsroom, 'Bringing people better ads', 26 May 2016, https://newsroom.fb.com/news/2016/05/bringing-people-better-ads/. See also: The Wall Street Journal, 'Facebook Wants to Help Sell Every Ad on the Web', 27 May 2016, https://www.wsj.com/articles/facebook-wants-to-help-sell-every-ad-on-the-web-1464321603.

intelligence, level of happiness, whether they use addictive substances and whether their parents are divorced.

Data protection regulations apply to the processing of personal data. For example, as adopted by the Council of Europe in 1981, Convention 108 contains the principles for fair and lawful collection and automatic processing of personal data. The Convention also provides measures of control for individuals, such as the right to obtain confirmation of whether their personal data are stored as well as the right to obtain rectification of such data.[13] On the level of the European Union, great efforts have been made to 'make Europe fit for the digital age' by establishing the General Data Protection Regulation (GDPR), which will apply from 25 May 2018.[14] In addition to this, the e-Privacy Directive,[15] which covers various topics, such as the requirement to ask for a user's consent before, for example, cookies are stored on his or her device, will be repealed by a e-Privacy Regulation.[16]

Internet

The Internet and personal data processing go hand in hand, considering the broad definition of personal data.[17] Even the processing of an IP address, used to identify a device connected to the Internet, can activate the applicability of data protection regulations.[18] The data protection issues that arise from processing activities via the Internet have been described in great length. With regard to *big data analytics*, for example, the use of data for new or incompatible purposes, data maximisation, lack of transparency, the possibility of uncovering sensitive information, the risk of re-identification, security implications and incorrect data are all issues that pose challenges to personal data protection (Berlin Telecom Group 2014). Other implications of (big) data analysis that relate to *behavioural targeting* are, for instance, take-it-or-leave-it choices, for example the use of 'cookie walls' that deny people's access to a website unless they consent to the website owner tracking their activities (Zuiderveen Borgesius 2014).

The Council of Europe has addressed numerous of these 'big data' issues; see, for example, Korff (2013) in the report entitled 'The use of the Internet & related services, private life & data protection', and Rouvroy (2016) regarding fundamental rights and freedoms in a world of big data. Indeed, Convention 108 is currently being modernised with the aim of addressing the challenges for privacy resulting from the use of new ICTs,[19] and in January 2017 guidelines on big data were adopted by the Consultative Committee of Convention 108.[20] In relation to the issues that arise when data are used for automated decisions, including *profiling*, we refer to subsections 3.6 (freedom of expression) and 3.7 (prohibition of discrimination).

Internet of Things

Most of the data protection challenges that arise with regard to Internet services also apply to the Internet of Things. Similar to websites and apps that operate via the Internet, machines within the Internet of

[13] Article 8 Convention 108.

[14] The General Data Protection Regulation's predecessor, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, will be repealed on the same date.

[15] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directives 2006/24/EC and 2009/136/EC.

[16] European Commission, 'Proposal for an e-Privacy Regulation', https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

[17] Article 2(a) Convention 108 defines 'personal data' as any information relating to an identified or identifiable individual. See also: article 2(a) General Data Protection Directive 95/46/EC and article 4(1) General Data Protection Regulation.

[18] Court of Justice of the European Union 19 October 2016, C-582/14 (*Breyer*) and Court of Justice of the European Union 24 November 2011, C-70/10 (*Scarlet/SABAM*), paragraph 51.

[19] Council of Europe, 'Modernisation of the Data Protection "Convention 108"', 28 January 2016, https://www.coe.int/nl/web/portal/28-january-data-protection-day-factsheet.

[20] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 January 2017', Strasbourg, 23 January 2017 T-PD(2017)01.

Things can be used to collect data. Think of a car robot that registers its surroundings or monitors its travel route (location data) or a care robot that tracks an elderly person's face or emotion (biometric data). Shop owners already use technologies to track their customers within their shop, or even monitor people who pass by their shop.[21] Tech companies such as Google, Amazon, Apple and Microsoft have developed business strategies to gather data in and around the home.[22] As a result, one's home – which used to be his or hers castle – has become a place where a person's movements or behaviour is continuously being 'watched', e.g. via a smartphone, smart meter or smart television. The data collection via the Internet of Things enables these companies to gain a detailed insight into the behaviour and lives of millions of people. Sometimes data collection results from legislation, e.g. the use of smart meters[23] or event data recorders for eCall systems used in cars.[24]

The rise of the Internet of Things raises issues about the transparency of data processing and how the individual is able to exercise his or her rights as set out in Convention 108 or the General Data Protection Regulation (GDPR). One of the main pillars of legitimate data processing – the individual's informed consent to the proposed processing activity – will continue to be put under pressure (see, for example, Eskens et al. 2016). The more 'smart' devices surround people, the more difficult it becomes for individuals to exert control over the data processing activities of all these devices. To a certain extent, the processing of these data is covered by data protection regulations, offering the individual certain rights and safeguards. However, the data can be analysed and used in a way that affects human rights, most notably the right to respect for private life in the sense of article 8 ECHR, which protects an individual's autonomy, informational privacy and self-determination, among other things. As a consequence, there might still be an interference with the right to respect for private life, even if the party that processes the personal data – for example a state or a company – complies with all obligations as stipulated by the data protection regulations.

Recommendation

Modern-day surveillance via the Internet or the Internet of Things, performed by states or companies, inherently involves the processing of personal data. Researchers are still trying to grasp the full extent of the harmful effects on the lives of individuals caused by such surveillance. The known effects are not comforting. Not only does surveillance have a chilling effect on speech (affecting the freedom of expression, for example by preventing journalists from doing their job properly), but it also leads to behavioural effects. For instance, as a result of surveillance, individuals conform to perceived group norms. This conforming effect occurs even when people are unaware that they are conforming (Kaminski & Witnov 2015). Both states and companies reinforce each other in their surveillance activities, as part of the *surveillance-innovation complex* (Cohen 2016).

Ubiquitous and massive collection of data by *governments* has been possible with little fundamental political and public debate so far, although some institutions, such as (inter)national courts, have expressed their worries about these matters. For instance, on an international level, both the European Court of Human Rights and the Court of Justice of the European Union have voiced their concerns on numerous occasions regarding state surveillance activities and the impact on privacy rights.[25] For

[21] The Dutch Data Protection Authority imposed penalty payments on a company that could not demonstrate that Wi-Fi tracking in public spaces was necessary for a legitimate purpose. See also: Autoriteit Persoonsgegevens, 'Dutch DPA investigates WiFi tracking in and around shops', 1 December 2015, https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-investigates-wifi-tracking-and-around-shops.

[22] Google's Internet of Things Solutions, https://developers.google.com/iot; AWS IoT - Amazon Web Services, https://aws.amazon.com/iot/; HomeKit - Apple Developer, https://developer.apple.com/homekit/; Internet of Things (IoT) | Microsoft, https://www.microsoft.com/en-us/internet-of-things.

[23] European Commission, 'Smart grids and meters', https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters.

[24] European Commission, 'eCall in all new cars from April 2018', 28 April 2015, https://ec.europa.eu/digital-single-market/en/news/ecall-all-new-cars-april-2018.

[25] For an overview of (a selection of) these cases, see Annex I of: Article 29 Data Protection Working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 13 April 2016.

instance when the EU Court of Justice declared the Data Retention Directive to be invalid.[26] On a national level, the British Investigatory Powers Tribunal, for instance, ruled that during a time span of more than a decade, the British intelligence agencies illegally collected data about innocent citizens and illegally tracked their phone and web use.[27]

With regard to surveillance enacted by *companies*, the European Commission proposed the reform of EU data protection regulations, which ultimately led to the General Data Protection Regulation. In addition to this, the e-Privacy Regulation has been proposed, which will replace the e-Privacy Directive.

Court rulings[28] as well as decisions[29] and concerns[30] voiced by regulators show that companies and states often interfere with an individual's right to personal data protection. According to Georgetown University law professor Julie E. Cohen, '[W]e the citizens have been reduced to raw material – sourced, bartered and mined in a curiously fabricated "privatised commons" of data and surveillance'.[31] She concludes that the future of society is dependent on ensuring that our system counters – rather than reinforces – power asymmetries, 'allowing all of us to be treated as citizens, not as raw material'.[32]

In the light of the above, we recommend that the Council of Europe takes a stance with regard to the ubiquitous and massive personal data processing of the modern era, reinforcing the human rights principles as enshrined in the conventions.

[26] The EU Data Retention Directive 2006/24/EC deals primarily with the retention of certain data which are generated or processed by providers of publicly available electronic communications services or of public communications networks. Court of Justice of the European Union 8 April 2014, Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland and Seitlinger and Others*). See also: Court of Justice of the European Union 21 December 2016, Joined Cases C-203/15 (*Tele2 Sverige AB v Post-och telestyrelsen*) and C-698/15 (*Secretary of State for the Home Department v Tom Watson and Others*).

[27] The Investigatory Powers Tribunal 17 October 2016, [2016] UKIPTrib 15_110-CH, http://www.ipt-uk.com/judgments.asp?id=35. See also: The Guardian, 'UK security agencies unlawfully collected data for 17 years, court rules', 17 October 2016, https://www.theguardian.com/world/2016/oct/17/uk-security-agencies-unlawfully-collected-data-for-decade.

[28] For an overview of (a selection of) Court of Justice of the European Union and European Court of Human Rights cases, see Annex I of Article 29 Data Protection Working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 13 April 2016. In addition, with regard to decisions of the Court of Justice of the European Union concerning data protection, see: L. Laudati (OLAF Data Protection Officer), Summaries of EU Court decisions relating to data protection 2000–2015, https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf.

[29] Fines and warnings have been issued by regulators, for instance in Italy: R. Panetta, 'Garante issues highest EU sanction on record', *IAPP*, 15 March 2017, https://iapp.org/news/a/garante-issues-highest-eu-sanction-on-record/ and Reuters, 'Google pays $1.4 million fine in Italy over StreetView concerns', 3 April 2014, www.reuters.com/article/us-italy-google-privacy-idUSBREA3226A20140403; Germany: Reuters, 'German privacy regulator fines three firms over U.S. data transfers', 6 June 2016, www.reuters.com/article/us-germany-dataprotection-usa-idUSKCN0YS23H; Spain: Reuters, 'Spain privacy watchdog fines Google for breaking data law', 19 December 2013, www.reuters.com/article/us-spain-google-privacy-idUSBRE9BI12Z20131219; France: Reuters, 'France fines Google over data privacy', 8 January 2014, www.reuters.com/article/us-france-google-fine-idUSBREA0719U20140108 and Reuters, 'French data privacy regulator cracks down on Facebook', 8 February 2016, www.reuters.com/article/us-facebook-france-privacy-idUSKCN0VH1U1.

[30] See, for instance, the concerns as expressed by the Article 29 Data Protection Working Party as laid down in its letters to companies such as WhatsApp (regarding its Terms of Service and Privacy Policy), Yahoo (regarding stolen user data) and Google (regarding its Privacy Policy and Google Glass). These letters are available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm. More recent letters are available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[31] The London School of Economics and Political Science, 'Code and Law between Truth and Power', 11 March 2015, www.lse.ac.uk/newsAndMedia/videoAndAudio/channels/publicLecturesAndEvents/player.aspx?id=2972. For a summary of Julie E. Cohen's lecture, see: The Guardian, 'We are citizens, not mere physical masses of data for harvesting', 11 March 2015, https://www.theguardian.com/technology/2015/mar/11/we-are-citizens-not-mere-physical-masses-of-data-for-harvesting.

[32] The Guardian, 'We are citizens, not mere physical masses of data for harvesting', 11 March 2015, https://www.theguardian.com/technology/2015/mar/11/we-are-citizens-not-mere-physical-masses-of-data-for-harvesting.

3.2.2 Right to respect for private life

Right to respect for private life

Over time, the European Court of Human Rights (ECtHR) has interpreted 'the right to respect for private life' as laid down in article 8 ECHR, explaining that this right is a broad term which is not susceptible to an exhaustive definition. The right to respect for private life is not restricted to an individual's home but is also applicable to other places, such as the workplace. Moreover, with regard to the right to respect for private life as protected by article 8 ECHR, the ECtHR not only focuses on negative freedoms,[33] human dignity and individual autonomy but also on self-expression, personal development and human flourishing (Van der Sloot 2014).

From a technological perspective this subsection focuses on 'computers as persuasive technologies', which is usually abbreviated to captology. Captology includes the design and analysis of and research on interactive computing products (computers, mobile phones, websites, wireless technologies, mobile applications, video games, etc.) created for the purpose of changing people's attitudes or behaviours.[34] Persuasive technologies rely on data-gathering, analysis via AI and smart interfaces. First we address the massive covert use of persuasive technologies on the Internet and its influence on humans and their right to respect for private life. Subsequently we reflect on the voluntary use of self-surveillance, for example via smart wearables, and persuasion. We set out how people use *e-coaches* to (co)-steer their lives and how this impacts their autonomy and self-determination – either positively or negatively – as part of the right to respect for private life. Lastly, we describe how persuasive care robots may potentially interfere with or enhance the right to respect for private life.

Massive psychological experimentation and persuasion on the Internet

Persuasive technologies have been in use for several decades in the gambling industry, in particular in computerised slot machines (Schüll 2013). By means of compelling digital and video technology, these slot machines pull players into a trance-like state, which players call the 'machine zone', in which their daily worries, bodily awareness and even their sense of self fade away. Once in the 'zone', gambling addicts play not to win, but simply to keep playing. They are merging with the machine, or in other words, they are caught in the loop of the machine that is designed to entrance them. According to Schüll (2016), these types of small, repetitive feedback loops of stimulus and response, so-called compulsion loops, which are very absorbing, are used more and more in the world at large, especially in online gamification.

Virtual environments, like the Internet, are to psychology what cyclotrons are to physics: living laboratories (cf. Biocca 2003; Pentland 2014). Smartphone apps or websites, for instance, measure how people interact with these applications. In this way millions of people are tested on the Internet each day. Schutz (2016) speaks about the 'biggest psychological experiment in history'. Via A/B testing – a randomised experiment with two or more variables – knowledge is gathered about our behaviour and how our brain makes choices. Based on these measurements, the applications automatically adjust their content in order to test, for example, which colour scheme we think looks the best, but also to persuade the user to buy an article, click on a certain advertisement or extend his or her time using the application. Just as in the case of slot machines, the financial value of an app is mainly driven by the amount of time consumers use it for. In *Hooked: How to build habit-forming products*, Eyal (2014) explains that designers of apps apply basic slot machine psychology to hook users. For example, Facebook applies the psychological phenomenon of the fear of missing out (FOMO) to lure its users to spend time on Facebook. In his review of various books on how people interact with social and mobile media, Weisberg (2016, 9) draws a worrisome conclusion: '[T]he more you read about it, the more you may come to feel that we're in the middle of a new Opium War, in which marketers have adopted addiction as an explicit

[33] Such as the notion of 'the right to be let alone', as described by Warren and Brandeis (1890).
[34] Stanford Persuasive Technology Lab, 'What is captology?', http://captology.stanford.edu/about/what-is-captology.html.

commercial strategy. This time the pushers come bearing candy-colored apps.' In this respect this could also be a human rights issue with regard to the right to health.[35] Along the same lines, Jonathan Harris makes a comparison between software and medicine 'in their dual capacities to heal and hurt' (Harris 2012). Tristan Harris, co-founder of the advocacy group Time Well Spent, proposes that engineers should take a kind of Hippocratic oath which obliges them to develop software that respects people's agency (Bosker 2016). In medicine and biotechnology, it is common practice for companies to have an ethical board or an ethical review committee, and several pleas have been made to establish such committees for IT companies and IT research as well (KNAW 2016; Hern 2016).

Parties developing persuasive technologies apply knowledge derived from neuroscience and psychology. There are ethics codes for psychologists and for doing psychological research (see below). The question is whether parties use, and should use, persuasive technologies according to these codes of conduct. This is certainly not always the case. For example, in 2012 Facebook and academics from Cornell University tried to influence the emotions of almost 700,000 Facebook users via newsfeeds (Kramer et al. 2014), without the users' informed consent or the appropriate approval from an ethics committee.[36] The users had no idea that their emotions were being influenced via predominantly negative or positive newsfeeds. These influencing activities not only evidently interfere with an individual's autonomy and self-determination but also with the individual's freedom of thought, conscience and religion (Strand & Kaiser 2015). Another example is online dating service OkCupid, which conducted experiments designed to test which aspects of a member's profile had the most influence on attracting other members of the service (Grimmelmann 2015). OkCupid's co-founder told *The Guardian*: '[I]f you use the internet, you're the subject of hundreds of experiments at any given time, on every site. That's how websites work.'[37] How can people choose their own path if organisations, via websites or apps, nudge them towards certain emotions and choices? This question becomes especially urgent when people are not aware that they are being influenced, rendering them practically defenceless against these influencing activities.

Ethics codes for psychologists and the performance of psychological experiments

The potentially negative effects on humans of experimental, sometimes persuasive, conduct explain why psychologists and universities have developed their own codes of ethics, such as the Universal Declaration of Ethical Principles for Psychologists or – in Europe – the Meta-Code and the Model Code of the European Federation of Psychological Associations. These international principles and codes can provide models for national ones. For instance, the Netherlands Institute of Psychologists (NIP) developed the Code of Ethics for Psychologists 2015.[38] This Code explicitly refers to the ECHR as well as to the International Convention on the Rights of the Child. The obligations arising from these legal sources for psychologists have been included in the NIP Code insofar as possible.

The NIP Code deals with topics such as the responsibilities, integrity and expertise of the psychologist, as well as the respect they should have for their clients and includes a description of the complaints procedure. Article 12 of the NIP Code reads: 'Psychologists must respect the fundamental rights and

[35] See articles 11 and 13 of the Council of Europe's Revised Social Charter, for instance. For more information, see Resolution 1576 (2007) of the Parliamentary Assembly: https://tinyurl.com/hjj3b8e.

[36] On the matter of the appropriate, informed consent, see: J. Grimmelmann, 'As Flies to Wanton Boys', 28 June 2014, http://laboratorium.net/archive/2014/06/28/as_flies_to_wanton_boys (updated on 30 June 2014). See also: K. Hill, 'Facebook added "research" to user agreement 4 months after emotion manipulation study', *Forbes*, 30 June 2014, https://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/#1786ee0b7a62. With regard to the review procedure, see: M.N. Meyer, 'How an IRB Could Have Legitimately Approved the Facebook Experiment—and Why that May Be a Good Thing', 29 June 2014, http://www.thefacultylounge.org/2014/06/how-an-irb-could-have-legitimately-approved-the-facebook-experimentand-why-that-may-be-a-good-thing.html.

[37] A. Hem, 'OKCupid: we experiment on users. Everyone does', *The Guardian*, 29 July 2014, https://www.theguardian.com/technology/2014/jul/29/okcupid-experiment-human-beings-dating.

[38] Nederlands Instituut van Psychologen (NIP), *Code of Ethics for Psychologists 2015*, https://www.psynip.nl/en/dutch-association-psychologists/code-of-ethics/.

dignity of the Persons Involved. They must respect [their] right to privacy and confidentiality.' With regard to scientific research, article 85 of the NIP Code stipulates: 'The psychologist may, if so requested, provide Data to Third Parties for scientific research purposes. Those Data must be provided in such a way that they cannot be traced to the Client, unless that is impossible in light of the purpose of the research. In that case those Data may be provided only with the Client's consent.' Comparable to the Oviedo Convention, the NIP Code deems informed consent important in order to safeguard the client's rights and interests.

Even though the NIP Code is aimed at psychologists and not at technology companies developing robotics or AI, for instance, individuals should not have less protection merely because they are not in a traditional psychologist–client relationship with the entity that is performing the psychological experiment. It is quite remarkable that although such experiments are being conducted via the Internet (and the IoT) on a massive scale, the human subjects are unaware of this and have not given their consent to these experimental activities. The NIP Code provides for a complaints procedure, and if the complaint is successful, then a psychologist's NIP membership may be terminated. It may not always be clear to a citizen whether he or she has a right to file a complaint against experimental activities conducted by a website owner or app owner, and, if so, how this can be done, especially if he or she is unaware of the experiment and data protection regulations do not apply, e.g. because no personal data are being processed.

Voluntary self-surveillance and persuasion in the Internet of Things

People use electronic coaches, or e-coaches, to better manage their lives (Kool et al. 2015). These e-coach systems often use softbots which are integrated into smart wearables. For example, the Fitbit is a wrist bracelet which enables self-tracking practices. This device monitors the individual's behaviour, such as their sleep patterns or diet, in order to coach them to improve their lifestyle (such as getting better sleep, exercising more or losing weight). The sum of the data registered by such an *e-coach* constitutes an individual's *data double* and is part of the *datafication* of that individual's daily routine (WRR 2016). This is a form of – voluntary – self-surveillance, which is promoted by the so-called *quantified self*-movement. Quantified selfers aim to steer the quality of their lives for the benefit of their autonomy and self-determination. Indeed, an e-coach can be beneficial to one's autonomy by, for example, encouraging and helping its user to get enough exercise (Kool et al. 2015).

Even though the users of an *e-coach* have the intention of taking control of their lives, they need to consider that there are more parties involved in this technology. The interests of these parties may not be aligned with those of the e-coach user. For instance, employers could try to oblige their employees to wear an e-coach in order to track their activities. By doing so, the employer is able to advise or steer someone into a certain lifestyle. Apart from the evident interference with the individual's private life, the data registered by the e-coach may contain health information that should be treated carefully. This is also an interference with someone's informational privacy, since the individual loses control of his or her personal information.[39] In addition to the employers, the developers of the e-coaches would also have control over the collected data. These data are used to 'tell' users how they should adjust their lives. Here lies the risk of unwanted manipulation in which autonomy turns into heteronomy (Fuchs 2015). Third parties, as well as the developers, are also involved in receiving data and analysing them, for their own commercial purposes, for example. This was reported recently, when the Norwegian Consumer Council lodged a complaint about the fitness app Runkeeper (which has 33 million registered users

[39] The Dutch Data Protection Authority decided negatively about the use of e-coaches by employees which enabled employers to gain insight into, for example, someone's sleeping behaviour (health data). See: Autoriteit Persoonsgegevens, 'Verwerking gezondheidsgegevens wearables door werkgevers mag niet', 8 March 2016, https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-verwerking-gezondheidsgegevens-wearables-door-werkgevers-mag-niet (Dutch).

worldwide) with its national Data Protection Authority.[40] The Consumer Council claimed that the app tracks users and transmits personal data to third parties irrespective of when the app or handset is in use.

The Rathenau Instituut, in order to ensure someone's capability as a proactive manager of his or her life, recommended that technology developers of, for example, e-coaches should be transparent about the persuasive methods they apply (Kool et al. 2015). People should be able to monitor the way in which information reaches them. This also means that transparency about the revenue model should be mandatory. Comparable to care robots (see below), e-coaches can provide care in the form of advice, e.g. lifestyle or psychological advice. In order to address the issues of the quality of e-coaches and the responsibility of their developers, a seal of approval should be developed that informs users about the quality of the e-coaching apps and devices.

Care robots as persuasive technologies

Care robots are designed to provide care to vulnerable groups, such as children, the elderly or disabled people. Robots can be applied both for the benefit and to the detriment of someone's autonomy and self-determination. Think of robots that improve the autonomy of elderly persons by assisting them when they change their clothes or take a bath. The Japanese robot Robear, for example, can lift care recipients from their beds without the help of a human caregiver. Accordingly, these robots could enable elderly persons to play an active part in society and to live independently, as stated in article 23 of the Council of Europe's Revised Social Charter.

In contrast, care robots may also restrain an elderly person when their developers have programmed them to do so. How pushy may a robot become, for example, in reminding someone to take medication? What if someone refuses to take medication? The danger of unwanted paternalism comes into play here. In this case, the robot technology will force users to take a particular course of action on the basis that developers know what is best for these users (Van de Poel & Royakkers 2011). Sharkey and Sharkey (2012) argue that the degree to which a robot intervenes will affect the freedom of the care robots. The risk is that we are on a slippery slope and may create 'authoritarian robots' (Koops 2013).

As stated in chapter 2, physical robots represent embodied AI. This embodiment of the robot offers opportunities to improve the interaction between humans and machines. Machines, like social care robots, capitalise on the ability of people to attribute human form, traits, emotions and intentions to machines. Robotics makes use of this ability to *anthropomorphise* to develop social robots so that they engage with humans on an emotional level (Royakkers & Van Est 2016). Anthropomorphising technology means that people have a strong tendency to attribute human motivation, characteristics or behaviour to animals and inanimate objects (ibid.). Engineers may use this powerful social psychological phenomenon to build persuasive technology. But what are the limits within which this phenomenon may be used? To what level do we want to deploy the emotional bond between people and machines? And how do we ensure that there is no abuse of the trust that is artificially built between humans and machines? Since people can be addicted to their cell phone, or to a virtual reality girlfriend, it is completely conceivable that people can develop strong feelings for socially intelligent artefacts, like social robots. Ylimaula (2010) argues that technologies, or rather the actors behind them, should refrain from taking control over someone's life and should remain 'assistive' with respect to someone's autonomy. In that respect the right to respect for privacy is also about *not being controlled* (Zuiderveen Borgesius 2014, 93).

[40] Forbrukerrådet, 'Runkeeper tracks users when the app is not in use', 13 May 2016, www.forbrukerradet.no/side/runkeeper-tracks-users-when-the-app-is-not-in-use/. See also: Forbrukerrådet, 'Consumer protection in fitness wearables', November 2016, https://www.forbrukerradet.no/siste-nytt/fitness-wristbands-violate-european-law.

Recommendations

In addition to and enabled by mass surveillance and psychological experimentation, persuasion by means of ICTs is taking place on a massive scale. The Council of Europe could form an opinion about the psychological experiments involving humans that are taking place on the Internet and outside the professional domain of, for example, psychologists or anthropologists, since these activities could have a great (negative) impact on a person's autonomy or self-determination. There are ethics codes for doing psychological research. The Council of Europe could clarify whether the firms that are doing the psychological experiments on the Internet should abide by the same codes.

In order to influence people's behaviour, companies and governments make use of powerful social psychological phenomenon, like the fear of missing out and anthropomorphism, which could even lead to addiction and pull people into the 'machine zone', causing them to lose their autonomy. The Council of Europe could form an opinion on whether and how persuasion software can be developed that respects people's agency. This could mean, for example, that persuasion techniques should neither be too addictive nor too authoritarian. In this respect, the Council of Europe could develop fair persuasion principles, such as enabling people to monitor the way in which information reaches them, and demanding that firms must be transparent about the persuasive methods they apply.

3.2.3 Right to respect for family life

Right to respect for family life

The right to respect for private life comprises the right to establish and to develop relationships with other human beings and the outside world, especially in the emotional field, for the development and fulfilment of one's own personality. This is referred to as the right to respect for family life.[41]

Social skilling and deskilling

Over the last few years, the debate has been growing on how new ICTs influence people's emotional and social skills and the quality of human relationships. Clinical psychologist and sociologist Turkle (2011, 2015) presents an influential voice in this debate. She finds that because many young people are absorbed in their devices, they fail to fully develop into independent selves. Researchers at the University of Michigan, for example, found a strong decrease in empathy among American students since the beginning of this century, partly due to the use and content of social media (Konrath et al. 2011). As a result of people's attachment to their devices, Turkle sees a risk of *social deskilling*: the inability to cope with other humans with their problems and shortcomings and the unwillingness to invest in human relationships. If we take this to the extreme, fewer obligatory relationships between humans and technology could result in an avoidance of human intimacy.

As robots are being outfitted with social abilities, how does this challenge the right to respect for family life? Certain types of robots are equipped with AI and are programmed to mimic social abilities in order to, for example, establish a conversation with their user; for instance, a care robot can use affective computing in order to recognise human emotions and subsequently adjust its behaviour (Van Est et al. 2014). Potentially, robots can stimulate human relationships. Think of a care robot, like the Dutch care robot Alice, that asks the recipients of its care whether they have recently contacted their family members, with the aim of (re-)establishing contact and maintaining their relationships. Several studies on the effect of Paro, a soft seal robot, in elderly care in nursing homes seem to suggest that the mood of elderly people improves and that depression levels decrease; their mental condition also improves, advancing communication among those living in the nursing home and strengthening their social bonds (cf. Hansen et al. 2010). However, as technology increasingly nestles between us, the risk exists that robots could interfere with the right to respect for family life as an (un)intentional consequence of how the

[41] Article 8(1) ECHR.

robot affects its users. Because of anthropomorphism, vulnerable people such as the elderly may believe that a social robot is a actual person, for example their grandchild. If the situation is not treated carefully, the care receiver may primarily focus on the care robot instead of, for example, his or her family members or other humans. Designers and developers should be aware of the strength of a human–robot relationship that can be caused by anthropomorphism.

With regard to virtual or augmented reality technologies, similar arguments can be made. These technologies may improve someone's ability to establish and develop relationships with human beings. For instance, such technologies could facilitate communications between family members. Microsoft Research showed this during its 'holoportation' demonstration.[42] On the other hand, it could also decrease someone's ability to establish and develop relationships if, for example, a virtual world is designed in a way which prevents the person from entering into (meaningful) contact with others, and instead is designed to encourage them to interact with virtual entities. The user may become addicted to the virtual world, while simultaneously disregarding his or her human relationships.

Recommendation

ICTs can either improve someone's ability to establish and develop relationships with other human beings or decrease someone's ability to establish and develop meaningful relationships with other human beings. The Council of Europe could form an opinion about how ICTs can be designed in such a way that they comply with the right to respect for family life.

3.3 Human dignity

Human dignity

Human dignity is one of the core principles of fundamental rights. It is the basis of most of the values emphasised in the ECHR.[43] Article 1 of the Universal Declaration of Human Rights – on which the ECHR is based – states: *'*All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.' The Charter of Fundamental Rights of the European Union affirms this notion, stating that human dignity is inviolable and must be respected and protected (article 1). According to the Charter, human dignity includes the right to life (article 2) and the right to the integrity of a person (article 3), among other things.

The ECHR does not explicitly mention 'human dignity'. However, its importance has been highlighted in several legal sources related to the ECHR. For instance, the ECtHR held that 'the very essence of the Convention is respect for human dignity and human freedom'.[44] Furthermore, with regard to the application of biology and medicine, the Oviedo Convention explicitly states that parties to this Convention must protect the dignity and identity of all human beings and guarantee everyone, without discrimination, respect for their integrity and other rights and fundamental freedoms.[45]

Human dignity is not only a fundamental right in itself, but also acts as the basis for freedoms and other rights (EDPS 2015). Therefore, if the use of technologies interferes with human dignity then these technologies are likely to interfere with other rights as well, such as the right to respect for private life. In its report, the JURI Committee explains that communication and interaction with robots have the potential

[42] Engadget,'"Holoportation" demo makes live-video holograms look easy', 26 March 2016, https://www.engadget.com/2016/03/26/holoportation-demo-makes-live-video-holograms-look-easy/. See also: Holoportation – Microsoft Research, https://www.microsoft.com/en-us/research/project/holoportation-3/.

[43] Explanatory Report to the Oviedo Convention, paragraph 9.

[44] ECtHR 29 April 2002, application no. 2346/02 (*Pretty v United Kingdom*), paragraph 65.

[45] Article 1 Oviedo Convention.

to profoundly impact relations, both physical and moral (JURI Committee 2017). This section addresses some of these impacts with respect to care robots.

3.3.1 Robots taking care of us with dignity

Care robots

From a human rights perspective, using technologies to aid the elderly should be done carefully since elderly persons may fall within the group of vulnerable people who are protected by several legal sources. These sources underline the importance of independent living and full participation in society for the elderly. Two such sources are the Council of Europe's Revised Social Charter and the Charter of Fundamental Rights of the European Union.[46] Moreover, Recommendation CM/Rec(2014)2 of the Council of Europe's Committee of Ministers on the promotion of the human rights of older persons underlines that older persons should be able to fully and effectively participate and be included in society and that all older persons should be able to live their lives in dignity and security, free from discrimination, isolation, violence, neglect and abuse, and as autonomously as possible. The Commissioner for Human Rights of the Council of Europe, Thomas Hammarberg, summarised in the conclusion to his report that the human dignity of older persons must always be respected.[47] These considerations should be taken into account when deploying care robots to help the elderly.

Comparable to our observations made in subsection 3.2 regarding the right to respect for private life, the use of care robots – assistive technologies – can have positive consequences for someone's dignity as well as negative ones. For example, a dehumanising version of mechanical feeding would provide elderly people no choice or autonomy with regard to how they would receive their nutrition. In contrast, the users of My Spoon claimed that this feeding robot gave them back their dignity, because it provided them with opportunities to be independent and to preserve their privacy when eating (Leroux & Labruto 2012).

Robot design and culture play important roles. The developers of My Spoon acknowledged that some senior user candidates in South-Korea 'hate having the bowls right in front of their mouth; they prefer to eat the food like ordinary people. Thus, we focus mainly on using a tabletop tray' (Song & Kim 2012, 47). Bespoke solutions are thus necessary in order to maintain dignity, privacy and intimacy without affecting safety (Vermesan & Friess 2015). For instance, within the EU-funded Value-Ageing project it was recommended that the robot must be capable of communicating its intention of doing something to the user, while the user must be able to cancel the intended action or switch off the robot completely (ibid.).

In particular, the development of social robots is a sensitive area. Communication and interaction with robots may potentially impact relations in our society, both physical and moral relations. According to the JURI Committee, this is especially the case for care robots towards which people can develop feelings and attachments (JURI Committee 2017). This causes concerns about human dignity, among other things (ibid.). Indeed, it has been argued that it may become humiliating and may damage self-respect if, for example, an elderly person is somehow forced to consider inanimate objects as the comprehensive universe of his or her own social life (Mordini et al. 2008).

Recommendation

The call for design and development of robotics that preserve human rights has been made recently during the 38th International Conference of Data Protection and Privacy Commissioners, at which the

[46] Article 25 of the Charter of Fundamental Rights of the European Union stipulates as follows: 'The Union recognises and respects the rights of the elderly to lead a life of dignity and independence and to participate in social and cultural life.'

[47] Human rights of older persons: participation, equality and dignity, 5th Warsaw Seminar on Human Rights, Warsaw, 29 September–1 October 2011, Keynote speech by Thomas Hammarberg, Commissioner for Human Rights of the Council of Europe, http://social.un.org/ageing-working-group/documents/egm/reference-documents.pdf.

European Data Protection Supervisor highlighted that engineering techniques and methodologies should be developed that permit AI and robotics to fully respect the dignity and rights of the individual (EDPS 2016). The Council of Europe could follow this call and provide guidelines on how the individual's dignity and rights may be respected, which would allow vulnerable groups such as the elderly to fully and effectively participate in society and live their lives in dignity.

3.4 Ownership

Ownership and the right to enjoy possessions

Ownership is a human rights issue: natural persons (human beings) or legal persons who are entitled to enjoy their possessions should not be deprived of their possessions except in the cases provided in article 1 of the First Protocol to the ECHR. This article directly protects the owner from interference by the state and it obliges states to protect the owner from interferences in his peaceful enjoyment by third parties, such as civilians or companies. The right to property can apply to all sorts of objects, including intangible goods. The case law of the ECtHR shows that the protection offered by article 1 of the First Protocol can therefore be broad, as it includes protection of, among other things, intellectual property rights, business goodwill, welfare benefits, contractual rights over property and virtual assets such as domain names (Sganga 2014). How is the notion of ownership challenged in the current age of technological convergence?

Two main developments can be distinguished in relation to ownership. Firstly, objects that people possess – such as their home or land – may become part of a virtual or augmented reality. This begs the following question: if you own your land, do you also own the virtual space that has been allocated to it by others?

Secondly, ownership questions arise in relation to the *use* of an object, such as a robotised car or a smartphone. The issues here are twofold. For a start, these devices are part of the Internet of (Robotic) Things and are therefore connected to networks. This enables entities other than the user of the device to have control over the device, effectively intervening in someone's use of it. If a device has been bought, is it possible for the buyer to enjoy his or her possession peacefully when, for example, the manufacturer or the previous owner can disable or control that device? In addition, the object as part of the Internet of (Robotic) Things (either bought, rented or otherwise used by someone) registers data for all kinds of purposes. This is especially true with regard to, for example, a robotised car, which needs these data in order to operate safely. Does the user of the device own the data, which can be either *personal data* and activates data protection regulations, or *non-personal* data that may fall within the scope of other legal regimes such as intellectual property laws? These are difficult questions to answer on the basis of current legislation, as a study carried out for the European Commission confirmed that data ownership is not explicitly dealt with by any EU or national legal instruments (DG CONNECT 2016).

Virtual worlds and augmented reality

Firstly, ownership issues arise when artefacts created as part of a virtual or augmented reality are placed 'on top' of possessions in the physical world. For instance, when the developer of the game Pokémon Go put virtual characters – Pokémon – on top of real-world homes and environments for the gamers[48] to find and catch, this led to discussions about trespassing, land rights and the legal boundaries of property.[49] The developer of the Pokémon game did not ask the land owners for permission to put their game

[48] It has been estimated that 45 million people worldwide played the game at its peak in July 2016. See: Bloomberg, 'These charts show that Pokemon Go is already in decline', 22 August 2016, https://www.bloomberg.com/news/articles/2016-08-22/these-charts-show-that-pokemon-go-is-already-in-decline.

[49] Reuters, 'Get off my lawn! Pokemon Go tests global property laws', 22 September 2016, http://www.reuters.com/article/us-landrights-pokemongo-idUSKCN11S1GY.

characters at the same geo-location as their physical homes, gardens or other property. Owners of memorial sites in the United States, Japan and Germany were not amused by this and wanted to stop the gamers from finding virtual Pokémon at their physical premises.[50] In some cases the game developer responded to their complaints and removed the game characters from the corresponding coordinates of their property. The Dutch municipality of The Hague sued the game developer because it claimed that the gamers who were looking for virtual Pokémon demolished protected areas of nature when doing so. The dispute has been settled out of court and it remains unclear whether the Dutch municipality invoked legal arguments relating to property rights as the owner of a so-called Natura 2000 protected area.[51]

Arguments based on property rights are possible. In a case brought by US residents in New Jersey, Florida and Michigan, the plaintiffs are arguing that the virtual Pokémon cause people to physically trespass on their land.[52] They are also claiming that by placing virtual game pieces on or near their private property without their permission, their rights are also violated. According to the game developer, trespass laws only cover physical intrusions and not virtual ones. A federal judge will decide whether this case can continue.

Controlling an object in the age of the Internet of Things

When it comes to physical objects, such as cars, houses and land, we have a rather straightforward idea of what ownership means. Under certain conditions, ownership gives a person the exclusive right to enjoy, occupy, possess, rent, use, give away or even destroy their property. Digital technologies may shift the nature and notion of ownership. For example, in contrast to a physical book, which you own if you buy it, buying an e-book means you merely pay for a licence to read the book. That means the e-book vendor can delete the digital book from your device without warning. In 2009 this actually happened, when Amazon remotely deleted Orwell's *1984* from the Kindles of surprised readers without explanation.[53] Perzanowski and Schultz (2016) hold that consumers should be better informed about the trade-offs of licence agreements – such as privacy, permanence and user constraints – and argue that introducing aspects of private property and ownership into the digital marketplace would affirm our sense of self-direction and autonomy.

Physical objects connected to the Internet of Things, such as robots, cars or even printers, also raise questions about ownership. As these devices and their software become intertwined with and connected to networks, this enables the manufacturer to effectively control, for example, a robot or a device even after it has been bought. This is possible because remote access can be gained via the Internet by the manufacturer or as part of the software's design that is implemented in the device. As a consequence, the individual owning a robot or a device is hindered in his or her peaceful enjoyment of this possession. For instance, a US tractor manufacturer argued – on the basis of its intellectual property rights relating to the tractor's software – that it continued to own the software, even after farmers had purchased the tractor (Coyle 2016). Some tractor owners even buy modified software to circumvent the unauthorised repair locks put in the tractor's software by the manufacturer (Koebler 2017). Another example is a software update issued by Hewlett Packard for its printers. Consequently, the printers were no longer

[50] United States: R. Nakashima & M. Anderson, 'Property owners: Get off my lawn, Pokemon!', *AP*, 14 July 2016, www.bigstory.ap.org/article/907bac533d66441c9cb48b78f0a3b7fb/irked-owners-trying-pry-pokemon-go-clutch-property; Japan: *AP*, 'No more "Pokemon Go" at Hiroshima atomic bomb memorial', 8 August 2016, http://bigstory.ap.org/article/90520fd445d54369b3dc73cc793e52c9/no-more-pokemon-go-hiroshima-atomic-bomb-memorial; Germany: B.Z. Berlin, 'Pokémon-Verbot am Holocaust-Mahnmal', 14 July 2016, www.bz-berlin.de/berlin/mitte/pokemon-verbot-am-holocaust-mahnmal.

[51] Business Insider, 'Dutch freeze court action against Pokemon Go makers', 11 October 2016, http://www.businessinsider.com/afp-dutch-freeze-court-action-against-pokemon-go-makers-2016-10.

[52] The Wall Street Journal, '"Pokémon Go" suit makes case for virtual trespassing', 4 April 2017, https://www.wsj.com/articles/pokemon-go-suit-makes-case-for-virtual-trespassing-1491310800.

[53] The New York Times, 'Amazon erases Orwell books from Kindle', 17 July 2009, www.nytimes.com/2009/07/18/technology/companies/18amazon.html.

able to use third-party ink cartridges.[54] In other cases, manufacturers may disable the owner's access to the device, if this is allowed according to the manufacturers' terms and conditions (Brodkin 2013).

The connected object can in some cases be controlled by its previous owner as well as the manufacturer, as a researcher who worked for IBM discovered. He sold his car but was still able to control it using the car's mobile app.[55]

These examples show that in the current world it is not self-evident that one can exclusively interact with or otherwise use goods such as robots or devices, even if these goods have been purchased. It is possible that some of these issues can be addressed via existing legal instruments that are part of consumer law, competition law or intellectual property law. However, another perspective could be based on the right to property and could argue that once an object has been bought, the manufacturer or other parties may not interfere with this possession unless the owner has provided his or her permission (e.g. for software updates).

Ownership of (personal) data

The 'things' that are part of the Internet of Robotic Things register all kinds of data. For instance, a robotised car collects and analyses the data which are needed to assist the driver or – in the case of self-driving cars – safely drive the car autonomously. The data relate to elements such as the vehicle's performance and its position compared to other objects. Who owns the data that has been 'extracted' from the device or has been otherwise registered as part of a person's use of the device? Before we examine the possible answers to this question, we describe the role of data in the Internet of Robotic Things in more detail.

The collection, analysis and use of data happen in a cyclical manner. This has been called the *digital* or *cybernetic loop*. The collected data – for example information about traffic congestion and how to avoid it – is analysed and subsequently used: the driver receives information in his or her car about how he or she can efficiently continue on the route without getting caught in traffic or, with regard to self-driving cars, how the car can efficiently and automatically divert its route. The steps of data collection, analysis and use have been described as the *(big) data value chain*. In order to refine the data, the steps of the big data value chain are repeated. The information gathered as part of the digital loop may be shared with other cars which are also connected to each other via a network. In this way, a whole fleet may 'learn' about the traffic congestion and how to avoid it (*fleet learning*). The real-time, accurate information also enables other parties involved in the big data value chain, such as road maintenance workers, to quickly and precisely take the appropriate measures in case of, for example, a traffic jam (Moerel & Prins 2016).

The data generated by robotised cars are valuable. The data make it possible to develop self-driving cars and provide an insight into the activities and behaviour of the car's passengers. Because of its value, various parties claim the vehicle's data (fully or partly) as their own. For instance, car manufacturers and advertising companies make 'ownership' claims (Sharman 2015). Yet the concept of data ownership is hard to define and difficult to apply in practice. This is because of complex assignments of different rights in data transactions across different stakeholders (Cattaneo et al. 2016). This is true with regard to both *personal* data and *non-personal* data. Absolute control over *personal* data is difficult to guarantee, given other concerns such as the public interest and the rights and freedoms of others (EDPS 2015). In this respect, the European Data Protection Supervisor notes that under EU law, 'the analogy of ownership cannot be applied as such to personal information, which has an intrinsic link to individual personalities'

[54] BBC, 'HP apologises for ink-blocking update', 29 September 2016, www.bbc.com/news/technology-37503139.

[55] CNN tech, 'Why buying used cars could put your safety at risk', 17 February 2017, http://money.cnn.com/2017/02/17/technology/used-car-hack-safety-location/.

(EDPS 2015). Not everyone agrees with this notion. Data ownership may be a useful concept when considering *personal data* as a rivalrous resource. Here, though, the question is *whose property* personal data should be (Purtova 2013). The purpose of this concept is to strengthen natural persons' position in the digital ecosystem. According to the legal scholar Purtova, property rights have to be assigned in personal data to the data subject, including a default of 'non-disclosure' and 'no use of personal data'. If this is not done, then this would amount to the legitimisation of property rights being 'grabbed' by the information industry. Purtova states that this would render 'the individual defenceless in the face of corporate power eroding his autonomy, privacy and right to information self-determination' (Purtova 2013, 2).

Legal scholars have opted for the idea that propertisation of personal data acknowledges the current commodification of personal data: customers should be fairly compensated for their personal information which is 'traded'. For instance, data can be collected following a person's use of a robotised car, which is then sold by the car manufacturer to, for example, an advertising company. It has been argued that a data ownership model could facilitate this 'trade' by making sure that the person who generates the data due to his driving is compensated (EDPS 2015). The question remains as to whether this concept could be beneficial to someone's fundamental rights, e.g. in terms of human dignity. For example, if a robot or softbot equipped with AI obliges a human to supply 'his or her' data in order to provide a certain service or answers in return, then certain risks arise for the individual. In this respect, Christl and Spiekermann (2016, 150) note that 'data ownership (or legal property rights) embedded in data exchange policies bear the risk of an extensive commodification of the self'. This could potentially lead to a situation in which people with a low or very low income have to provide data in exchange for the service while those who have a higher income pay for the service without having to provide (personal) information. Indeed, the European Data Protection Supervisor warns against the idea that people can pay with their data in the same way that they do with their money. Fundamental rights cannot be reduced to consumer interests, and personal data cannot be considered as a mere commodity, according to the European Data Protection Supervisor (EDPS 2017). These are the potential negative effects of a data ownership concept aimed at providing compensation for the individual.

With regard to *non-personal* data, 'data ownership' deals with various types of legal claims covered by intellectual property rights (e.g. copyright or database protection rights), trade secrets, antitrust regulations, contractual rights, public sector information laws or other regulations. Thus, the question about data ownership is not always the appropriate question if, for example, someone wants to determine his or her rights to access and use the data for specific purposes. When exchanging data, determining the *type of data* produced or collected, etc. is key to determining the appropriate legal data ownership regime (Cattaneo et al. 2016).

Businesses have objected to the need to regulate ownership issues relating to non-personal data, referring to contractual freedom as well as a fear that possible regulation could stifle innovation and impede the development of the market.[56] Without a precedent from the ECtHR on this matter, it is not clear whether data qualify as possessions, although this has not been ruled out by legal scholars (Tjong Tjin Tai 2016). The question remains, however, *who* should be entitled to such ownership, e.g. the consumer, the robot's manufacturer or perhaps someone else. It is clear that questions about allocating data ownership rights to one or the other party may not be *welfare-maximising* and cannot easily be answered (Duch-Brown et al. 2017).

[56] European Commission, Synopsis report on the contributions to the public consultation regulatory environment for data and cloud computing, 24 September 2015–6 January 2016, paragraph 4.2.4, https://ec.europa.eu/digital-single-market/en/news/synopsis-report-contributions-public-consultation-regulatory-environment-data-and-cloud.

Recommendations

This section provided a brief look at how the peaceful enjoyment of possessions is challenged by the use of emerging technologies. Virtual objects may result in interference with the owner's property, bought devices can be disabled without the owner's control and the data value chain leaves us with questions about how 'data ownership' relates to, for example, negotiating access, control and the ability to use and reuse data. This makes 'data ownership' – either as a possession in the sense of article 1 of the First Protocol to the ECHR or as 'propertisation' of (personal) data, for example – a concept worth the Council of Europe considering. The Council of Europe could proactively provide guidance on these matters, setting the boundaries within which someone may enjoy his or her (in)tangible possessions and defining how others have to respect those boundaries.

3.5 Safety, responsibility and liability

Safety, responsibility and liability

Tort rights are human rights (Van Dam 2013). For example, the ECHR obliges the contracting states to provide an effective remedy, often discharged by the national tort law remedies (ibid.). This makes the safety of robots a human rights issue. In this section we elaborate on this matter with a primary focus on car robotisation.

The automotive industry has made cars more and more *intelligent*. This is the long-term trend of *car robotisation* (Royakkers & Van Est 2016). From the 2000s onwards, cars have gradually received automated capabilities, such as cruise control and park assist systems. The European Parliament's Science and Technology Options Assessment holds that safety aspects should be one of our primary concerns, i.e. finding ways for robots and humans to work together without having accidents (STOA 2016). Semi-autonomous vehicles need a human driver with his or her eyes on the road, ready to intervene when the car makes a wrong assessment of the situation. Since current technology still needs human involvement, it has been argued that the term 'auto pilot' that has been used by Tesla is misleading.[57] Many believe that in the future the self-driving car will become an everyday phenomenon, enabling its passengers to ride with their eyes off the road and their hands off the wheel. The path to fully automated autonomous driving involves an ongoing automation and interconnection of vehicles and the traffic's infrastructure (Royakkers & Van Est 2016).

The JURI Committee finds that the civil liability for damage caused by robots is a 'crucial issue which needs to be analysed and addressed in order to ensure the same degree of efficiency, transparency and consistency in the implementation of legal certainty throughout the EU for the benefit of citizens, consumers and businesses alike' (JURI Committee 2017). At this stage, though, it is clear that the following potential actors can be identified who may bear the blame when there is a car crash: the car manufacturer, the software builders who programmed the car's AI, the seller, the buyer and the road authority. Addressing the issue of responsibility and liability will depend on the level of automation of the car. The levels of automation for 'on-road motor vehicles' have been classified by the global association SAE International.[58] The association's classification scheme, which has been used by, for example, the U.S. Department of Transportation as part of its Federal Automated Vehicles Policy,[59] defines six levels of automation. The levels range from no automation (level 0) to full automation (level 5). In between lie vehicles with driver assistance capabilities (level 1), advanced driver assistance/partial automation (level 2), conditional automation (level 3) and highly automated driving (level 4).

[57] Reuters, 'Germany says Tesla should not use "Autopilot" in advertising', 16 October 2016, www.reuters.com/article/us-tesla-germany-idUSKBN12G0KS.

[58] SAE International's new standard J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, http://www.sae.org/misc/pdfs/automated_driving.pdf.

[59] U.S. Department of Transportation, 'Federal Automated Vehicles Policy', https://www.transportation.gov/AV.

Automation levels 0–2: From conventional driving to partial automation

With conventional driving (level 0), a human driver has his or her eyes on the road and both hands on the wheel of the vehicle, although warning or intervention systems as well as automatic transmission may be in place. With regard to level 0 vehicles, the rules regarding how liability should be apportioned have been widely established. In principle, the car's manufacturer is liable when the damage occurred because of a defect in its product, the car. A defect can consist of, for example, brakes physically not working, but also software bugs may lead to failure of the vehicle's functions.[60] What is considered defective depends on what might have been expected of the car given the circumstances. In addition, the road authority may be held liable if the road does not meet the requirements needed for safe travel. The driver may be liable for damage caused by the vehicle, unless he or she can successfully prove *force majeure*. Although legal interpretations may vary on the European continent, *force majeure* cannot usually be invoked by the vehicle's owner if a defect suddenly occurs, even if there was a failure in the driver assistance system, such as cruise control or the park assist systems (levels 2 and 3 respectively) (Royakkers & Van Est 2016).

With regard to conventional driving (level 0), driver assistance (level 1) and certain forms of advanced driver assistance, such as park assist systems (level 2), 'no legislative, regulatory or guidance changes [are] needed for existing technologies', the British government concluded in July 2016 (Department for Transport 2016, 16). In sum, when the driver is at all times in complete control of the vehicle, then – apart from certain exceptions and different national interpretations – how liability should be apportioned is fairly clear.

Automation levels 3–4: From conditional automation to highly automated driving

Automation levels 3 and 4 apply to vehicles in which the driver can (temporarily) take his or her hands off the wheel (level 3) and his or her eyes off the road (level 4). Level 3 is referred to as conditional automation, which is 'the driving mode-specific performance by an automated driving systems of all aspects of the dynamic driving task'.[61] With automation level 3 it is expected that a human driver will respond appropriately to a request to intervene.[62] Examples are remote control parking, motorway assist and mid-range platooning. The last is an example of cooperative driving in which cars or trucks are mutually linked through electronic communication by cooperative systems (Royakkers & Van Est 2016). As a 'platoon' of these cars drives close to each other and exchanges information about, for example, their speed, position and acceleration, the cars become autonomous and the drivers' hands can be taken off the steering wheel. Highly automated, level 4, systems perform all aspects of the dynamic driving tasks, including when a human driver does not respond appropriately to an intervention request.[63] Advanced platooning and a full motorway pilot are examples of this level of automation. These are future technologies (Department for Transport 2016).

Most discussions about the liability issues that arise from the use of autonomous driving are about automation levels 3 and 4, in which the driver can switch the autonomous mode on or off and remains (at least in part) able to operate the vehicle. With regard to liability and the Tesla car with autopilot features, Tesla thinks the main responsibility lies with the driver. Tesla says that the term 'autopilot', just as in aeroplanes, raises the expectation that there will be a human pilot too. In Tesla's view, '[T]he onus is on

[60] See, for instance: CBS News, 'Okla. jury: Toyota liable in sudden acceleration crash', 25 October 2013, www.cbsnews.com/news/okla-jury-toyota-liable-in-sudden-acceleration-crash/; BBC, 'Volvo recalls 59,000 cars over software fault', 20 February 2016, www.bbc.com/news/world-europe-3562275; and Tech Times, 'Nissan recalls Infiniti Q50 sedans over steering glitch, promises software fix', 18 June 2016, www.techtimes.com/articles/165624/20160618/nissan-recalls-infiniti-q50-sedans-over-steering-glitch-promises-software-fix.htm.

[61] SAE International, 'U.S. Department of Transportation's new policy on automated vehicles adopts SAE International's levels of automation for defining driving automation in on-road motor vehicles', 22 September 2016, https://www.sae.org/news/3544/.

[62] Ibid.

[63] Ibid.

the pilot to make sure the autopilot is doing the right thing'.[64] This stance has led to some critical responses, for example: 'If it's controlled by an algorithm, why should you be liable?'[65] Tesla claims that its drivers accept the 'autopilot' conditions when accepting its terms and conditions: the car is merely in a 'beta' phase.[66] However, this notion may leave non-contractual parties in the dark about their position, since terms and conditions would only bind the contractual party, the car's owner, not other people. Should it be accepted that they may be in an AI and car robotics experiment, as unwilling participants? And what about outside sensors that aid the car? Should someone keep track of these sensors that aid connected, cooperative and automated driving systems, comparable to an air traffic controller? If so, what should his or her responsibility be? Is it acceptable to state that a vehicle, driving on the public roads, is in a beta phase? It has been reported that German authorities would not have approved a beta-phase Tesla autopilot.[67] In this respect it is worth nothing that Volvo has stated it will accept full liability whenever one of its cars is in *autonomous mode*, making it one of the first car makers in the world to make such a promise.[68] This statement follows Volvo's survey in which 79% of respondents stated that they would expect the manufacturer to accept liability.[69]

Levels 3 and 4 prove the most difficult when dealing with liability issues. The driver's liability for damage caused to other motorised road users is generally assessed on the basis of tort and is attributable when the damage is the driver's fault (Royakkers & Van Est 2016). Driver assistance systems complicate things if they do not function properly. And the driver alone cannot be blamed when certain hazards are encountered, for instance sudden unforeseeable situations that the driver could not reasonably take into consideration. Also, if driver assistance systems actually allow drivers to better respond to road hazards, this may affect their liability, since a driver cannot claim that he or she was in an unforeseen situation if the system warned him or her about, for example, a slippery surface. It also becomes hard to assess liability questions when a driver has failed to activate a function, for example a collision avoidance system, which could have prevented the damage.

With regard to cooperative systems and autonomous cars, the car's damaging acts can be traced back to external causes. For instance, a cooperative system may have missed a warning for a local hazard because of a defective roadside system (Royakkers & Van Est 2016). As a general rule the injured party should be able to prove this defect, but it is a complex task . With regard to driver assistance systems (levels 2 and 3), liability for the damage can possibly be proved by examining, for example, a defective software system. However, with regard to cooperative systems and autonomous cars, the incorrect functioning of such systems may have several causes, and providing suggestive evidence as part of e.g. legal proceedings may be difficult in practice. Black boxes or eCall systems may address these issues, recording the car's behaviour.[70] The German Federal Cabinet has adopted a draft law that requires manufacturers of semi-autonomous cars to install a black box, which helps to determine responsibility if

[64] Bloomberg TV, 'Elon Musk on Tesla's auto pilot and legal liability', 10 October 2014, https://www.youtube.com/watch?v=60-b09XsyqU.

[65] Rosemary Shahan, president of the Consumers for Auto Reliability and Safety lobbying group in: LA Times, 'Tesla's "autopilot mode" puts it at risk for liability in crashes', 6 July 2016, www.latimes.com/business/technology/la-fi-tn-tesla-liabilty-20160705-snap-story.html.

[66] Tesla, 'A tragic loss', 30 June 2016, https://www.tesla.com/blog/tragic-loss.

[67] Reuters, 'German authority would not have approved beta-phase Tesla autopilot: newspaper', 10 July 2016, www.reuters.com/article/us-germany-tesla-idUSKCN0ZQ0IM.

[68] Volvo Car Group, 'US urged to establish nationwide federal guidelines for autonomous driving', 7 October 2015, https://www.media.volvocars.com/global/en-gb/media/pressreleases/167975/us-urged-to-establish-nationwide-federal-guidelines-for-autonomous-driving.

[69] K. Hall-Geisler, 'Drivers are warming up to autonomous cars. Mostly.', 5 July 2016, *TechCrunch*, https://techcrunch.com/2016/07/05/drivers-are-warming-up-to-autonomous-cars-mostly/.

[70] In practice, car manufacturers are not always willing to provide the car's data logs, as *The Guardian* found out: S. Thielman, 'The customer is always wrong: Tesla lets out self-driving car data – when it suits', *The Guardian*, 3 April 2017, https://www.theguardian.com/technology/2017/apr/03/the-customer-is-always-wrong-tesla-lets-out-self-driving-car-data-when-it-suits.

there is an accident.[71] Evidently, tracking and recording systems such as black boxes challenge privacy and data protection rights.

Automation level 5: Full automation

Even though automation level 5 is currently in an experimental phase, such full automation would have clear implications for liability schemes. With no eyes on the road or hands on the wheel, such autonomous cars shift the responsibility for avoiding accidents to the manufacturer (Royakkers & Van Est 2016). A driverless car is then comparable to a bus, of which the passenger has no control. Common carriers, such as bus companies, must maintain the highest possible standards of care and protect the lives of the passengers. This means that care manufacturers would be liable for even slight negligence, and the lives of the driverless car's passengers are in the hands of the manufacturer (ibid.).

The liability of the road authorities might need clarification, since the self-driving cars will most likely depend (in part) on digital roadside systems. The question is whether these systems are 'road equipment' for which the road authorities are responsible (Royakkers & Van Est 2016). Defining roadside systems and their underlying computer systems as road equipment could prove to be a solution to this question. This definition can be established by following, for example, the 'Declaration of Amsterdam',[72] in which the EU ministers of transport declared that the European Commission will continue to work closely with the industry and EU member states to create the conditions needed for connected vehicles to start using European roads in 2019.[73]

How liability will be apportioned when a robot is involved in causing damage or injuries is a matter of choice – taking all circumstances into account in relation to risk and insurance, etc. As a principal rule, the car's manufacturer should be held responsible. This is the point of view of the German minister of transport.[74] The U.S. Department of Transportation notes that the determination of who or what is the 'driver' of automated vehicles does not necessarily determine liability for crashes involving that vehicle. It notes that states of the US may determine that in some circumstances liability for a crash involving a human driver of an automated vehicle should be assigned to the manufacturer of the vehicle.[75]
The current laws and regulations may not fit properly in relation to robots acting autonomously, especially – as we have seen – with regard to levels 3 and 4 of car automation. As robotised cars become more autonomous and advanced, it can become difficult to apportion responsibility between the car's manufacturers and its users. Therefore clarification on this issue of liability is needed.

Recommendation

Civil liability and insurance are not uncommon areas for the Council of Europe to consider. The Council opened the European Convention on Compulsory Insurance against Civil Liability in respect of Motor Vehicles in 1959 and it entered into force in 1969.[76] The Council of Europe could pave the way for further development in this area, suggesting guidelines on how to apportion liability with regard to robotics.

[71] Bundesrat, 'Entwurf eines ... Gesetzes zur Änderung des Straßenverkehrsgesetzes', adopted on 25 January 2017, https://www.bundesrat.de/SharedDocs/beratungsvorgaenge/2017/0001-0100/0069-17.html (German). See also: Reuters, 'Germany to require "black box" in autonomous cars', 18 July 2016, www.reuters.com/article/us-germany-autos-idUSKCN0ZY1LT.

[72] Declaration of Amsterdam, 14 April 2016, https://english.eu2016.nl/documents/publications/2016/04/14/declaration-of-amsterdam.

[73] V. Bulc, 'Our journey towards the future of smart mobility', 15 April 2016, https://ec.europa.eu/commission/2014-2019/bulc/blog/our-journey-towards-future-smart-mobility_en. In March 2017, 29 European countries signed a letter of intent to intensify cooperation to test connected and automated road transport in cross border test sites: European Commission, 'EU and EEA Member States sign up for cross border experiments on cooperative, connected and automated mobility', 23 March 2017, https://ec.europa.eu/digital-single-market/en/news/eu-and-eea-member-states-sign-cross-border-experiments-cooperative-connected-and-automated.

[74] Wirtschafts Woche, 'Dobrindt gründet Ethikkommission für automatisiertes Fahren', 8 September 2016, www.wiwo.de/politik/europa/selbstfahrende-autos-dobrindt-gruendet-ethikkommission-fuer-automatisiertes-fahren/14513384.html.

[75] U.S. Department of Transportation, 'Federal Automated Vehicles Policy', https://www.transportation.gov/AV.

[76] Also, in 1973 the Council of Europe opened the European Convention on Civil Liability for Damage caused by Motor Vehicles. Unfortunately, this convention was never enforced because the minimum number of required ratifications had not been reached.

Various liability models may be considered, such as ‘shared’ responsibility (between, for example, the robot designer, developer, programmer, manufacturer, seller and user), a model in which robot developers are liable for harm caused by their robots, or a model that is something in between. The JURI Committee suggests, for instance, that liability should be proportionate to the actual level of instructions given to the robot and to its degree of autonomy (JURI Committee 2017).

The guidance offered by the Council of Europe could be the outcome of a balancing act: balancing the freedom of conduct (of Tesla and others) against the protection of (human) rights and interests of others (e.g. car drivers, pedestrians, etc.). When performing this balancing act, the existence of a compensation fund (e.g. liability insurance) is one of the factors that needs to be taken into account. The JURI Committee believes that an insurance system should oblige the autonomous robot’s producer to take out insurance, which should be supplemented by a fund in order to ensure that compensation must be paid if there is no insurance policy that covers the risks (JURI Committee 2017).

3.6 Freedom of expression

Freedom of expression

The first paragraph of article 10 ECHR stipulates that everyone has the freedom of expression.[77] This right includes the freedom to hold opinions and to receive and impart information and ideas without interference by a public authority and regardless of frontiers. The second paragraph of article 10 stipulates the circumstances in which legitimate interference with the exercise of freedom of expression is possible. In certain cases, article 9 ECHR may apply. This article protects the right to freedom of thought, conscience and religion. However, interferences with article 9 will often be treated as giving rise to issues arising within the scope of article 10 (Murdoch 2012). This section focusses on article 10 ECHR.

AI promoting or hindering the right to impart information and ideas without interference

Automated decisions can promote or hinder a free flow of information. If the AI programmer provides the user with tools to gather and disseminate information, then this could favour the right of freedom of expression. For instance, tools that bring together RSS feeds from newspaper sites can be helpful to impart information in an easy manner. However, if AI solely determines what information is to be shown, it challenges the freedom to receive and impart information and ideas without interferences, as protected by article 10 ECHR. For instance, there is a risk that an ‘information cocoon’, ‘echo chamber’ (Sunstein 2001) or ‘filter bubble’ (Pariser 2011) will be created that hinders, among other things, our ability to freely develop our opinions. Limits may even arise when we are (automatically) selecting information out of a seemingly infinite pool. For example, Google’s personalised search results depend, at least in part, on our previous search history.[78] According to the EU–Council of Europe youth partnership report, ‘Both cases of information restriction – individual decisions or automated algorithms – might lead to the loss of relevant “alternative” information that should be included in the decision making process of active participation’ (Zentner 2015, 49).

So, should we worry about filter bubbles? In 2016, researchers concluded that there is no empirical evidence that warrants any strong worries about filter bubbles at the moment (Zuiderveen Borgesius et al. 2016). Nevertheless, the researchers note that a debate about filter bubbles is important, since

[77] See also article 19 of the UN Human Rights Declaration: ‘Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.’ See also article 11 of the Charter of Fundamental Rights of the European Union.

[78] Wired, ‘Exclusive: How Google’s algorithm rules the web’, 2 October 2010, https://www.wired.com/2010/02/ff_google_algorithm/, see also Google, ‘Personalized search for everyone’, December 4, 2009, https://googleblog.blogspot.nl/2009/12/personalized-search-for-everyone.html.

problems for democracy could arise if personalisation technology further improves and personalised news becomes people's main information source. Currently approximately 12% of Internet users worldwide use social media as their main source of news (Newman et al. 2016, 7). Zuiderveen Borgesius et al. (2016) argue that more evidence is needed on the process and effects of personalisation so we can shift the basis of policy discussions from fear to insight.

When AI interferes with the right to freedom of expression

Bozdag (2013) claims that Google and Facebook have become central information gatekeepers of our society. Facebook claims that it is not a traditional media company but acknowledges that it has responsibilities for the way its platform is used.[79] The Reuters Institute for the Study of Journalism (RISJ) finds that for the above-mentioned 12% of users that use social media as their main source of news, 'Facebook is by far the most important network for finding, reading/watching, and sharing news' (Newman et al. 2016, 7).

Online gatekeeping services are a mix of human editors and software code designed by humans. In May 2016, Facebook received allegations that its 'trending topics' section deliberately showed less conservative political views, as opposed to liberal topics. Facebook denied the allegations; their internal investigation 'has revealed no evidence of systematic political bias in the selection or prominence of stories included in the Trending Topics feature' but also indicated it could not fully exclude the possibility of unintentional bias. [80] Accordingly, the company changed the trending topics feature 'to prevent potential misuse and to minimise risks where human judgment is involved'.[81] In September 2016, Facebook removed a post from its site containing the famous photograph of the Vietnamese 'napalm girl' because it was in breach of the website's policy regarding nudity.[82] The photo was later reinstated. It is assumed that the post was tagged for removal by an algorithm and then was followed up by a human editor.[83] This indicates that algorithmic gatekeeping assistance does not remove all human biases. As Bozdag (2013, 224) explains: 'Technical biases such as third party manipulation or popularity will exist due to the computerized form of gatekeeping. Also, individual factors such as personal judgments, organizational factors such as company policies, external factors such as government or advertiser requests will still be present due to the role of humans in providing these services.'

Information gatekeepers can have a financial incentive to refrain from (unwillingly) supporting, for example, hateful or offensive content. For instance, Google's video platform YouTube showed advertisements next to offensive content such as homophobic and anti-Semitic videos. Consequently, certain advertised companies deserted Google for failing to keep its advertisements away from hate-filled videos.[84] Google said in response that it would hire significantly more human staff and would speed up the process of removing advertisements from hateful and offensive content. Recently, Facebook shareholders proposed a report on 'the threat to democracy and free speech from so-called fake news

[79] Reuters, 'Facebook CEO says group will not become a media company', 29 August 2016, www.reuters.com/article/us-facebook-zuckerberg-idUSKCN1141WN. Facebook CEO Zuckerberg recently indicated that the social network is a new platform – not a traditional technology company; not a traditional media company, see: C. Warner, 'Zuckerberg: "Facebook is not a traditional media company"', *Forbes*, 23 December 2016, https://www.forbes.com/sites/charleswarner/2016/12/23/zuckerberg-facebook-is-not-a-traditional-media-company.

[80] Facebook, 'Response to Chairman John Thune's letter on Trending Topic, 23 May, 2016, https://newsroom.fb.com/news/2016/05/response-to-chairman-john-thunes-letter-on-trending-topics/

[81] The Guardian, 'Facebook to change trending topics after investigation into bias claims', 24 May 2016, https://www.theguardian.com/technology/2016/may/24/facebook-changes-trending-topics-anti-conservative-bias. See also footnote 80

[82] The Guardian, 'Facebook backs down from "napalm girl" censorship and reinstates photo', 9 September 2016, https://www.theguardian.com/technology/2016/sep/09/facebook-reinstates-napalm-girl-photo. See also: Reuters, 'Facebook says will learn from mistake over Vietnam photo', 12 September 2016, www.reuters.com/article/us-norway-facebook-idUSKCN11I1VU.

[83] M. Scott & M. Isaac, 'Facebook Restores Iconic Vietnam War Photo It Censored for Nudity', *The New York Times*, 9 September 2016, https://www.nytimes.com/2016/09/10/technology/facebook-vietnam-war-photo-nudity.html.

[84] Reuters, 'Google to revamp policies, hire staff after UK ad scandal,' 21 March 2017, www.reuters.com/article/us-britain-google-idUSKBN16S0TW.

spread on the social media forum, and the dangers it may pose to the company itself'.[85] Shareholders suggested that the company should carry out a broad review of the issue, 'including the extent to which it blocks fake posts, how its strategies impact free speech and how it evaluates claims in posts'.[86]

Incentives in favour of combatting hate speech online can also be found in laws. Germany drafted a law which aims to force social networks like Facebook to quickly remove libellous or threatening online posts.[87] If the social networks do not comply, then they face fines of up to 50 million euros. It remains to be seen whether this is an effective solution to the problem, especially since it is not always clear where someone's protected freedom of expression ends, given the lack of a watertight or authoritative definition of 'hate speech' (McGonagle 2013). The same holds true with regard to defamatory information: it is not always clear to the online intermediary (such as a social network) how to respond appropriately to certain user-generated information it facilitates, as can be observed from the various ECtHR cases concerning defamatory user-generated content.[88] Therefore, the risk exists that parties like Facebook may unjustifiably delete posts or comments – whether or not with the aid of automated tools – in reaction to defamation or hate speech claims which would interfere with someone else's freedom of expression. It therefore comes as no surprise that a consumer group in Germany opposes the draft law, stating that it is the wrong approach and will make social networks into 'content police'.[89]

Recommendations

According to the ECtHR, not only does the media have the task of imparting information and ideas that are in the public interest but the public also has a right to receive them.[90] Facebook might be the world's biggest news outlet, with over 1.86 billion active users worldwide, but it is still unclear whether Facebook should be regarded as a media company and news editor and, if so, should assume its related proper role and responsibility as a 'public watchdog' in our democratic society. The Council of Europe could provide clarification on information gatekeepers, such as Google and Facebook, their role as news editors and their possible duties as public watchdogs. In addition, the Council of Europe could provide a blueprint as to how central information gatekeepers, like Google and Facebook, could use their algorithmic powers for the benefit of human rights, especially in relation to the right to receive and impart information and ideas.[91]

3.7 Prohibition of discrimination

Prohibition of discrimination

Article 14 ECHR states that the enjoyment of the rights and freedoms set out in the ECHR shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other

[85] Reuters, 'Facebook shareholders propose reports on 'fake news', pay equality', 14 April 2017, www.reuters.com/article/us-facebook-fakenews-idUSKBN17H01A.

[86] Ibid.

[87] Reuters, 'Germany plans to fine social media sites over hate speech', 14 March 2017, www.reuters.com/article/us-germany-fakenews-idUSKBN16L14G.

[88] ECtHR (Grand Chamber) 16 June 2015, application no. 64569/09 (*Delfi AS v Estonia)*; ECtHR 2 February 2016, application no. 22947/13 (*MTE & Index.hu ZRT v Hungary*); ECtHR 9 March 2017, application no. 74742/14 (*Pihl v Sweden*).

[89] As stated by Volker Tripp, head of the Digital Society Association consumer group in: Reuters, 'German cabinet agrees to fine social media over hate speech', 5 April 2017, http://uk.reuters.com/article/uk-germany-hatecrime-facebook-idUKKBN1771FK.

[90] ECtHR 26 April 1979, application no. 6538/74 (*The Sunday Times v the United Kingdom* (no. 1)), paragraph 65.

[91] Building upon Recommendation CM/Rec(2012)3 of the Committee of Ministers to member states on the protection of human rights with regard to search engines and Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services.

status.[92] Protocol No. 12 to the ECHR seeks to ensure that nobody shall be discriminated against on any ground by any public authority.

AI combatting or enabling discrimination

The delegation of decision-making to AI may provide an opportunity to combat discrimination. For example, AI tools have been developed with the aim of eliminating bias from the hiring process, such as a tool that automatically alerts the hirer to the use of potentially biased language in job descriptions.[93] Virtual reality technologies have even been deployed to promote diversity in education and to combat discrimination.[94]

As we have seen throughout this report, technologies can also be used to interfere with human rights. This is also true with regard to the prohibition of discrimination. Racist groups may use AI to propagate their message (Council of Europe 2012). Besides such types of intentional use of AI to discriminate against others, *un*intentional algorithmic discrimination, e.g. racism, also exists. For instance, in 2015 Google's Photos app tagged a picture of two black people as 'Gorillas'. This tag was the result of Google's AI, which suggests categories and tags based on machine learning. Google removed the tags and apologised: 'There is still clearly a lot of work to do with automatic image labeling, and we're looking at how we can prevent these types of mistakes from happening in the future.'[95] According to Google, its algorithms will get better at categorising photos if more people correct mistaken tags. The system can thus be 'trained' not to show tag suggestions which almost everyone would consider racist.[96]

Machine learning depends on data that has been collected from society. Goodman and Flaxman (2016) explain that to the extent that society contains inequality, exclusion or other traces of discrimination, so too will the data. Moreover, machine learning will reproduce discriminatory patterns in the 'training' data set. As a consequence, 'unthinking reliance on data mining can deny members of vulnerable groups full participation in society' (Barocas & Selbst 2016, 671). Goodman and Flaxman (2016, 3) warn that 'biased decisions are presented as the outcome of an objective algorithm'.

A specific subset of automated decisions is profiling techniques. These have been used, for instance, to assess how rich a website user is, so prices on the website can automatically be adjusted.[97] Goodman and Flaxman (2016, 3) hold that the use of algorithmic profiling for the allocation of resources is inherently discriminatory, since 'profiling takes place when data subjects are grouped in categories according to various variables, and decisions are made on the basis of subjects falling within so-defined groups'.

Current data protection regulations only partly address the issues

To what extent may a user seek redress if an automated decision interferes with his or her rights? Article 15 of the General Data Protection Directive 95/46/EC, the so-called 'Kafka provision', prohibits certain fully automated decisions with far-reaching effects, which are not only 'legal effects' but also decisions that 'significantly affect a person'. Moreover, in 1992 the European Commission said that 'data processing may provide an aid to decision-making, but it cannot be the end of the matter; human

[92] Article 7 UN Declaration of Human rights: 'All are equal before the law and are entitled without any discrimination to equal protection of the law.' See also article 21 Charter of Fundamental Rights of the European Union.

[93] Fortune, 'SAP Is Building Bias Filters Into Its HR Software', 31 August 2016, fortune.com/2016/08/31/sap-successfactors-bias-filter/.

[94] USA Today, 'Virtual reality tested by NFL as tool to confront racism, sexism', 10 April 2016, www.usatoday.com/story/tech/news/2016/04/08/virtual-reality-tested-tool-confront-racism-sexism/82674406/.

[95] The Wall Street Journal, 'Google mistakenly tags black people as "gorillas," showing limits of algorithms', 1 July 2015, blogs.wsj.com/digits/2015/07/01/google-mistakenly-tags-black-people-as-gorillas-showing-limits-of-algorithms/.

[96] The Wall Street Journal, 'Google mistakenly tags black people as "gorillas," showing limits of algorithms', 1 July 2015, blogs.wsj.com/digits/2015/07/01/google-mistakenly-tags-black-people-as-gorillas-showing-limits-of-algorithms/.

[97] In 2012, it was reported that the website Orbitz showed Apple users a different (more expensive) offer than non-Apple users. See: The Wall Street Journal, 'On Orbitz, Mac Users Steered to Pricier Hotels', 23 August 2012, www.wsj.com/articles/SB10001424052702304458604577488822667325882.

judgment must have its place' (Zuiderveen Borgesius 2014, 373). To safeguard the data subject's rights and freedoms, he or she has a right to obtain *human intervention* on the part of the controller, to express his or her point of view and to contest the decision. However, it is very hard and often even impossible for people to notice that they are excluded from seeing a certain advertisement online or have to pay a higher price because of e.g. a softbot equipped with AI identifying him or her as a 'rich' person. This makes it difficult to challenge the automated decision.

It can also be difficult to determine whether social sorting by automated tools qualifies as unlawful discrimination. An investigation by ProPublica illustrates this. ProPublica concluded that in the US certain insurers were charging premiums that were much higher in areas where most residents have an ethnic minority background than in non-minority neighbourhoods with similar accident costs (Angwin et al. 2017). As the investigators note, efforts to investigate such *redlining* in the car insurance industry were hindered during the past few years by the industry's refusal to make crucial data available. The Insurance Information Institute contested ProPublica's findings, stating that insurance companies do not collect data revealing the racial or ethnic origin of their potential customers and that insurers do not discriminate on the basis of race.[98] As to the question of why some insurers treat minority neighbourhoods differently, the investigators did not rule out that the proprietary algorithms used by insurers may inadvertently favour white neighbourhoods over those in which most residents had an ethnic minority background (Angwin et al. 2017). Given these factors – the lack of crucial data and the lack of transparency about the algorithms' inner workings – it can be hard for an individual to demonstrate unlawful social sorting such as discriminatory practices.

Article 15 of the Directive 95/46/EC does not help to reduce filter bubbles and manipulation risks much either, since these activities might not significantly affect a person in the sense of this article. Based on the EU regulations, the controlling party that processes the data should inform the 'profiled' person of the logic involved in the processing upon request. However, data protection regulations usually do not apply when people are not (in)directly identified. The successor of the Directive 95/46/EC – the GDPR – does not provide a feasible 'right to explanation' either to help individuals to understand easily whether or not algorithms or otherwise automated tools discriminate against them (Wachter et al. 2017).

Because of the above-mentioned shortcomings, various legal scholars want, among other things, to strengthen the position of the person being profiled. Hildebrandt (2012) calls for transparency-enhancing technologies, which would enable meaningful *profiling transparency*.

Recommendation

In order to combat algorithmic discrimination, the notion of *algorithmic accountability* – in addition to the current 'right to explanation' – is worth considering. In practice, this would imply things such as properly dealing with bias in data sets, discrimination-aware data mining, meaningful transparency in relation to algorithms and profiling, restriction of the contexts in which such AI is used and demanding outputs that avoid disparate impacts (cf. Pasquale 2016). It is recommended that the Council of Europe sheds lights on these issues. First of all, how can existing regulations or new ones facilitate algorithmic accountability or fairness? Secondly, how can the developers of algorithms be enabled to devise automated decisions that respect human rights and will not (unintentionally) discriminate against some people?

[98] Angwin et al. 2017. See also: J. Lynch, 'I.I.I.: Why ProPublica Auto Insurance Report Is Inaccurate, Unfair and Irresponsible', *Insurance Journal*, 5 April 2017, www.insurancejournal.com/news/national/2017/04/05/447012.htm. ProPublica's response: Insurance Journal, 'ProPublica, Consumer Reports Hit Back, Cite 'Errors' in Industry Criticism of Their Auto Insurance Report', 7 April 2017, www.insurancejournal.com/news/national/2017/04/07/447294.htm.

3.8 Access to justice and the right to a fair trial

Access to justice and the right to a fair trial

Article 6(2) ECHR plays an important role with regard to predictive AI. This provision mandates that everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.[99] Topics such as predictive policing and other predictive techniques have already been covered by the Council of Europe (cf. Korff and Georges 2015) and fall outside the scope of this report.

Because algorithms may result in biased decisions, this subsection focuses on the *impartiality* condition of article 6(1) ECHR. The first sentence of article 6(1) ECHR stipulates that 'in the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law'.

Artificial Intelligence

Courts are increasingly using tools that automate their decision processes. Softbots promise to make legal decisions faster and more consistently than humans can and drastically reduce the length of court proceedings (Winkels 2011). Another promise is that AI can help litigants to assess their case and estimate their chances of winning or losing. Since people would then have a better understanding of their legal chances, it is expected that people will go to court less (ibid.). The use of automated tools by judges may also help to ensure a fair trial.

Van den Hoogen (2007) argues that using decisions reached by computers should be possible in uncomplicated cases, while respecting article 6 ECHR at the same time (Van den Hoogen 2007). However, several principles should be taken into account when judges use an automated tool to aid the decision-making process. The principles are aimed at maintaining accountability because 'the judge is responsible for the final decision, also if this decision has been reached with or by assistive [computer] systems' (ibid., 12). Other principles are aimed at transparency and recognisability: '[I]f the judge deviates from the advice of the [computer] system, then it has to take note of this' (ibid., 12-13). The assisting systems may indeed operate in favour of the safeguards as provided by article 6(1) ECHR. Especially in uncomplicated cases, these systems can aid a trial, for example by speeding up the proceedings.

On the other hand, the ICT systems could act in breach of the impartiality principle when the AI is biased. In that case, human rights are challenged. The increased use of risk-assessing algorithms in the American justice system raises accountability and transparency issues.[100] It has been reported that software used to set bail, conditions for parole and sentencing decisions is biased against African Americans (Angwin et al. 2016), although the real impact of the software might not be that clear.[101] With regard to AI agents used by police forces that lead to criminal proceedings, Hildebrandt (2016) notes that we have to become resistant to the notion that the outcomes of using an AI tool are necessarily correct, complete or even relevant with regard to potential suspects. According to Hildebrandt, the 'equality of arms' principle of article 6 ECHR should be reinvented the moment that the public prosecutor, the judge or the lawyer are unable to check how the police's AI agent reached its conclusions. Such AI agents should log what they did, for what purpose and how they reached the outcome.

[99] See also article 11 UN Declaration of Human Rights and article 47 Charter of Fundamental Rights of the European Union.

[100] M. Smith, 'In Wisconsin, a backlash against using data to foretell defendants' futures', 22 June 2016, *The New York Times*, www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html.

[101] The Washington Post, 'A computer program used for bail and sentencing decisions was labeled biased against blacks. It's actually not that clear.', 17 October 2016, https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas.

Recommendation

Comparable to the observations made in subsections 3.6 and 3.7 regarding automated decisions, transparency about the AI tools used in relation to court proceedings and the accountability (of the judge) is essential. As part of a fair trial it should be known that e.g. an AI equipped softbot aiding the judge is being used and how this tool affects the decisions reached. The Council of Europe could establish a framework of minimum norms to be taken into account when a court uses AI. This could prevent as far as possible situations in which individual contracting states devise their own frameworks, which risks offering varying degrees of protection in the sense of what is set out in article 6 ECHR.

3.9 Two potential novel human rights

To keep the robot age human-friendly, we propose two potential 'novel' human rights: 1) the right to not be measured, analysed or coached, and 2) the right to meaningful human contact. These two novel rights are indirectly related to, and aim to elaborate on, in the context of the robot age, existing human rights, such as, respectively, the classic privacy right to be let alone and the right to respect for family life, that is, the right to establish and develop relationships with other human beings.

3.9.1 Right to not be measured, analysed or coached

States organise population censuses and install cameras because they rely on information to draft, apply and evaluate their policies. Scott (1999) even observes that states seem to have a natural tendency to make their citizens 'readable' and societies 'searchable' (Scott 1999). Besides governments, companies, such as Google, Apple and Facebook, also gather information about people, although mostly for commercial purposes. Driven by the Internet and the Internet of Things, profiling by companies (Christl & Spiekermann 2016) and state actors (WRR 2016b) has become more and more commonplace. Since many technologies nowadays can operate from a distance, most of us are not even aware of the mass surveillance taking place by state and market actors. This creeping development as a whole, and its impact on human rights and society, has received little attention and there has been scarcely any fundamental political and public debate so far.

As a result, human beings are rather defenceless relative to this mass surveillance culture, since there are few opportunities to escape the surveillance activities if one does not want to be measured, analysed or coached (as part of a persuasive strategy). For instance, researchers from Georgetown University published evidence showing that half of all American adults, including innocent ones, are in a police face-recognition database as part of a 'perpetual line-up' (Garvie et al. 2016). To give another example, in response to worries by consumers about Wi-Fi tracking by shop owners, the former Dutch minister of economic affairs and the state secretary of security and justice stated that people should just turn off their smartphone if they do not want to be tracked.[102] On the basis of this response, it seems that tracking and tracing people is a right which is deemed more important than peoples' (privacy) rights. Until recently, people could turn off their PC if they did not want to be tracked online. In our onlife world this strategy has become outdated. There has been little debate about the accumulative effect of mass surveillance. Instead, triggered by specific applications and incidents, 'mini debates' about a certain topic have been organised, and the outcome of each debate is a balancing act that mostly favours national security or economic interests. The sum of the debates, however, is the gradual but steady dissolving of privacy and anonymity for the individual.

Some authors have stressed certain detrimental effects of ubiquitous monitoring, profiling or scoring (Citron & Pasquale 2014) and persuasion. Strand and Kaiser (2015, 6) note that 'the right to privacy and

[102] Tweakers, 'Kabinet: zet telefoon uit om wifi-tracking tegen te gaan', 12 February 2014, https://tweakers.net/nieuws/94273/kabinet-zet-telefoon-uit-om-wifi-tracking-tegen-te-gaan.html (Dutch).

the possibility to perform everyday undertakings without being seen, monitored or noticed, may be fundamental to the development of a sane personality*'*. Rapporteur for the Council of Europe Douwe Korff stresses that 'profiling poses a fundamental threat to the most basic principles of the Rule of Law and the relationship between the powerful and the people in a democratic society' (Korff 2013, 7; Georges & Korff 2015, 32). The Berlin Telecom Group (2013) considers large-scale monitoring and profiling activities as an unprecedented risk to the privacy of all citizens. As a worst-case scenario, the world could turn into a 'global panopticon' (Berlin Telecom Group 2013). The Group states that governments have largely turned a blind eye to these alarming developments, leaving them to self-regulatory activities. What is at stake here is not only the risk of abuse but the right to remain anonymous and/or the 'right to be let alone' (Warren & Brandeis 1890), which in the robot age could be phrased as the right to not be electronically measured, analysed or coached.

So far, the right to *online anonymity* has received limited recognition under international law (Article 19 2015, 11). With the fast advent of the IoT and the Internet of Robotic Things, we recommend that the Council of Europe recognises the right to *onlife anonymity* as an independent right or as a clarified right linked to existing privacy rights. People should have the right to decide whether or not they want to participate in experiments carried out by other actors (which usually goes hand in hand with surveillance) or other activities that involve registering or otherwise observing people's lives and influencing their behaviour with technological means.

Recommendation

The Council of Europe could clarify to what extent in the context of the robot age the right to respect for privacy implies the right to not be measured, analysed or coached.

3.9.2 Right to meaningful human contact

Sometimes, robots may be able to completely take over a set of human tasks – think of so-called lights-out factories, which are fully automated and require no human presence or decision-making onsite. In these kinds of cases, we accept that people get out of the loop. In many other contexts, however, we would like to keep human beings in and on the loop. As a response to the development of autonomous military drones, hundreds of scientists and experts proposed a ban on offensive autonomous weapons beyond 'meaningful human control'.[103] This concept of meaningful human control is also relevant to other areas in which autonomous or AI systems potentially make critical decisions (AI Now Report 2016). In the case of AI and judges, meaningful human control is also an important theme. In contexts where human contact and interaction plays a central role, such as raising children and caring for elderly people, the 'right to meaningful human contact' could play a role too.

On the personal level, a right to meaningful human contact could safeguard one's well-being and prevent social and emotional deskilling. In the context of human imprisonment, it has been recognised that modern technology should facilitate and not *replace* human contact.[104] In her book on solitary confinement, Shalev (2008) argues that when an individual is removed from the company of other people, then this solitary confinement deprives him or her of most forms of meaningful and sympathetic social interaction, as well as physical contact. Also, with respect to health care for the elderly, it is claimed that the absence of human contact affects the physical and psychological well-being of the elderly. Some researchers believe that contact with care robots cannot compensate for the lack of human contact (cf. Sharkey & Sharkey 2012). Coeckelberg (2010) claims that robots should only be used instrumentally for routine care jobs, and that care-giving tasks that require emotional, intimate and

[103] Future of Life, 'Open Letter on Autonomous Weapons - Future of Life Institute', 28 July 2015, futureoflife.org/open-letter-autonomous-weapons/.
[104] Ambassador Torbjørn Frøysnes, Head of the Council of Europe Office to the EU, opening speech at the 18th Conference of Directors of Prison Administration, 22 November 2013.

personal involvement should be done by people. From a societal point of view, it is argued that caring for other people is a key characteristic and responsibility of human beings and our human culture. As Tufekci puts it: '[W]e cannot outsource our responsibilities to machines.'[105]

The European Parliament's JURI Committee considers that human contact is one of the fundamental aspects of human care and it believes that replacing the human factor with robots could dehumanise caring practices (JURI Committee 2017). We consider that these dehumanising practices may also occur outside the field of human care. Therefore, we recommend that the Council of Europe clarifies in what contexts and to what extent people have the right to meaningful human contact.

Recommendation

The Council of Europe could clarify to what extent in the context of the robot age the right to respect for family life should also include the right to meaningful human contact.

[105] Zeynep Tufekci, 'Machine intelligence makes human morals more important', June 2016, https://www.ted.com/talks/zeynep_tufekci_we_can_t_control_what_our_intelligent_machines_are_learning.

4 Safeguarding human rights in the robot age

Digital technologies affect human rights in numerous ways

This report studied the relationship between the engineering megatrend 'technology is becoming more and more biology' and human rights. The set of digital technologies we have examined ranges from the Internet and big data to AI, robotics and augmented reality, and is often referred to as the Internet of (Robotic) Things. We investigated six specific applications: self-driving cars, care robots, e-coaches, AI that is used for social sorting, judicial applications of AI, and virtual and augmented reality.

We found that these technologies provide new means through which human rights can be exercised as well as violated. Besides affecting the right to respect for private life in numerous ways, digitisation, virtualisation and robotisation influence human dignity, the right to the peaceful enjoyment of possessions, safety and tort rights, the right to freedom of expression, the prohibition of discrimination, access to justice and the right to a fair trial. It is important to note that other human rights issues may well arise due to the use of intelligent artefacts that fall outside the scope of this report.

Lack of attention to the erosion of human rights

Despite this wide-ranging impact of digital technologies on human rights, so far little attention has been paid to this crucial topic and there has been scarcely any fundamental political and public debate on it. As a result, a serious erosion of human rights is taking place. Therefore, the human rights debate, which is seriously lagging behind the fast-growing technological developments, needs to be strengthened rapidly. We agree with the analysis of and share the concern of Donahoe (2016), who states that '[an] understanding of how to protect human rights in the digital context is significantly underdeveloped. As we stumble along and try to adjust to our new digital reality, the relevance and predominance of the international human rights framework could lose salience in the international geo-political arena.'

Time for a wake-up call by PACE

In the context of human rights in the robot age, a wake-up call by the Parliamentary Assembly of the Council of Europe (PACE) would be very welcome. Triggered by many developments in the field of human genetics, PACE called for the preparation of a convention on bioethics in the early 1990s. In 1997 this led to the Oviedo Convention, which created guiding principles – such as the protection of private life, respect for autonomy, the right to information and informed consent – to preserve human dignity in the way humans apply innovations in biomedicine. In article 2, the Oviedo Convention clarifies that the interests of the individual have priority over the sole interests of science or society. Guided by the principle of the primacy of the human being,[106] the general interest only has priority in very precise situations and subject to strict conditions.[107] Also, with respect to, for example, privacy rights, a balance is sought between individual privacy rights on the one hand and the interests of 'national security, public safety or a country's economic wellbeing' on the other hand.[108] However, in the current context, human rights and interests of individuals lose out most of the time, especially with regard to policy making, and

[106] Council of Europe, Explanatory Report to the Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, European Treaty Series – No. 164, paragraphs 21 and 22.
[107] As defined in article 26 of the Oviedo Convention, see: Council of Europe, Explanatory Report to the Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, European Treaty Series – No. 164, paragraph 14.
[108] As mentioned in article 8(2) ECHR.

thus over time become eroded. This does not have to be a *fait accompli*. The Oviedo Convention shows that it is possible that the 'default setting' for striking a balance between individual and general interests can be set in favour of the individual's interests – the sum of which are, in fact, collective interests.

So far, the bulk of the bioethical debate and related human rights treaties have focused on the engineering megatrend 'human biology is becoming technology'. In other words, the focus has been on invasive biomedical technologies that work inside the body, or 'technologies within us'. This report paid special attention to the 'technology is becoming biology' trend and shows that in this robot age humans and digital technologies have become intimately entangled in many different ways. This is a process in which technology is nestling itself within us and between us more and more; it increasingly compiles information about us and is progressively able to act just like us (Van Est 2014). As we have shown, these non-invasive intimate digital technologies can have many bioethical implications and impact human rights in many ways. In an analogy with the activities of the Council of Europe in the 1990s in the field of biomedical technologies and human rights, we have produced the following main recommendation:

Main recommendation: Need for Convention on human rights in the robot age

In order to safeguard human rights in the robot age, we recommend that PACE calls for the preparation of a convention on robot ethics, or, even better, safeguarding human rights in the robot age, which would create common guiding principles to preserve human dignity in the way humans apply innovations in the field of the Internet of Things, including the Internet, robotics, AI, and virtual and augmented reality.

Input for an initial agenda

In chapter 3 we recommended that the Council of Europe forms opinions on various topics. Box 4.1 summarises this list of recommendations. This list may also function as an initial agenda for the preparation of a convention on robot ethics.

Box 4.1 List of recommendations

Right to the protection of personal data (see subsection 3.2.1)
We recommend that the Council of Europe takes a stance with regard to the ubiquitous and massive personal data processing of the modern era, reinforcing the human rights principles as enshrined in the Conventions.

Right to respect for private life (see subsection 3.2.2)
The Council of Europe could form an opinion about the psychological experiments involving humans taking place on the Internet and could clarify whether the firms that are doing these psychological experiments on the Internet should follow the ethics codes that currently apply when doing psychological experiments. The Council of Europe could form an opinion on whether and how persuasion software can be developed that respects people's agency.

Right to respect for family life (see subsection 3.2.3)
The Council of Europe could form an opinion about how ICTs can be designed in such a way that they comply with the right to respect for family life.

Human dignity (see subsection 3.3)
The Council of Europe could provide guidelines on engineering techniques and methods that permit AI and robotics to fully respect the individual's dignity and rights, allowing vulnerable groups such as the elderly to fully and effectively participate in society and live their lives in dignity.

The right to the peaceful enjoyment of possessions (see subsection 3.4)
The Council of Europe could provide guidance on ownership matters in the robot age, setting the boundaries within which someone may enjoy his or her (in)tangible possessions and how others have to respect those boundaries.

Safety, responsibility and liability (see subsection 3.5)
The Council of Europe could offer guidelines on how to apportion liability with regard to robotics.

The right to freedom of expression (see subsection 3.6)
The Council of Europe could provide clarification on the role of information gatekeepers, such as Google and Facebook, as news editors and their possible duties as public watchdogs. In addition, the Council of Europe could provide a blueprint as to how central information gatekeepers, such as Google and Facebook, could use their algorithmic powers for the benefit of human rights, especially in relation to the right to receive and impart information and ideas.

The prohibition of discrimination (see subsection 3.7)
The Council of Europe could shed light on how algorithmic accountability or fairness can be facilitated and how the developers of algorithms can be enabled to devise automated decisions that respect human rights and will not (unintentionally) discriminate against individuals.

Access to justice and the right to a fair trial (see subsection 3.8)
The Council of Europe could establish a framework of minimum norms to be taken into account when a court uses AI. This could prevent as far as possible situations in which individual contracting states devise their own frameworks, which risks offering varying degrees of protection in the sense of what is set out in article 6 ECHR.

The right to not be measured, analysed or coached (see subsection 3.9.1)
The Council of Europe could clarify to what extent in the context of the robot age the right to respect for privacy implies the right to not be measured, analysed or coached.

The right to meaningful human contact (see subsection 3.9.2)
The Council of Europe could clarify to what extent in the context of the robot age the right to respect for family life should also include the right to meaningful human contact.

References

AI Now Report (2016) *The Social and Economic Implications of Artificial Intelligence Technologies in the Near-Term*, A summary of the AI Now public symposium, hosted by the White House and New York University's Information Law Institute, 7 July 2016, version 1.0, 22 September 2016, available at: https://artificialintelligencenow.com.

Angwin, J., Larson, J., Kirchner, L. & Mattu, S. (2017) *Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk*, ProPublica, 5 April 2017, available at: https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk.

Angwin, J., Larson, J., Mattu, S. & Kirchner, L, (2016) *Machine Bias*, ProPublica, 23 May 2016, available at: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Arthur, W.B. (2009) *The nature of technology: What it is and how it evolves*. London: Allen Lane.

Article 19 (2015) *Policy Brief - Right to Online Anonymity*, June 2015, available at: https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf.

Barocas, S. & A,D. Selbst (2016) Big data's disparate impact. *California Law Review* Vol 104: pp. 671-732; doi:10.15779/Z38BG31.

Berloznik, R., R. Casert, R. Deboelpaep, R. van Est, C. Enzing, M. van Lieshout & A. Versleijen (eds.)(2006) *Technology Assessment on converging technologies*. Brussels: European Parliament, STOA.

Biocca, F. (2003) Media and the laws of mind. Preface to: G. Riva, F. Davide & W.A. IJsselsteijn (eds.) *Being there: Concepts, effects and measurements of user presence in synthetic environments.* Amsterdam: IOS Press.

Bosker, B. (2016) The binge breaker: Tristan Harris believes Silicon Valley is addicting us to our phones. He's determined to make it stop. *The Atlantic*, November Issue, available at: https://www.theatlantic.com/magazine/archive/2016/11/the-binge-breaker/501122/.

Bozdag, E. (2013) Bias in algorithmic filtering and personalization. *Ethics and Information Technology* September 2013, Volume 15, Issue 3, pp 209–227; doi:10.1007/s10676-013-9321-6.

Brodkin, J. (2013) 'Google may remotely deactivate Glass if you sell it or lend to a friend', *Ars Technica*, 18 April 2013, https://arstechnica.com/information-technology/2013/04/google-may-remotely-deactivate-glass-if-you-sell-it-or-lend-to-a-friend.

Cattaneo, G., G. Micheletti, A. Woodward & D. Osimo (2016) *European Data Market SMART 2013/0063 D 3.6 and D 3.7 Data Ownership and Access to Data – Key Emerging Issues Final Release*, 29 January 2016.

Christl, W. & Spiekermann, S. (2016) *Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Vienna: Facultas.

Citron, D.K. & F. Pasquale (2014) The Scored Society: Due Process for Automated Predictions *Washington Law Review*, Vol. 89, 2014, p. 1-; U of Maryland Legal Studies Research Paper No. 2014-8, available at: https://ssrn.com/abstract=2376209.

Coeckelbergh, M. (2010). Health care, capabilities, and AI assistive technologies. *Ethical Theory and Moral Practice*, 13(2), 181-190; doi:10.1007/s10677-009-9186-2.

Cohen, J.E. (2016) The Surveillance-Innovation Complex: The Irony of the Participatory Turn. In: Barney, D., Coleman, G., Ross, C., Sterne, J., Tembeck, T. (eds.) *The Participatory Condition in the Digital Age*, University of Minnesota Press, 2016.

Council of Europe (2012) *Young People Combating Hate Speech On-line*, prepared by the British Institute of Human Rights, Strasbourg, DDCP-YD/CHS (2012) 2 Strasbourg, 15 April 2012.

Coyle, D. (2016) How the digital age cuts through notions of material ownership, *Financial Times*, 29 September 2016.

Department for Transport (2016) *Pathway to Driverless Cars: Proposals to support advanced driver assistance systems and automated vehicle technologies*, July 2016, available at: https://www.gov.uk/government/consultations/advanced-driver-assistance-systems-and-automated-vehicle-technologies-supporting-their-use-in-the-uk.

DG CONNECT (2016) *Legal study on Ownership and Access to Data*. A study prepared for the European Commission DG Communications Networks, Content & Technology by: Osborne Clarke LLP; doi:10.2759/299944.

Donahoe, E. (2016) So software has eaten the world: What does it mean for human rights, security & governance? Part 1. *Just Security*, March 22, https://www.hrw.org/news/2016/03/22/so-software-has-eaten-world-what-does-it-mean-human-rights-security-governance.

Duch-Brown, N., B. Martens & F. Mueller-Langer (2017) *The economics of ownership, access and trade in digital data*. Digital Economy Working Paper 2017-01; JRC Technical Reports.

Eskens, S., J. Timmer, L. Kool & Rinie van Est (2016) *Beyond control - Exploratory study on the discourse in Silicon Valley about consumer privacy in the Internet of Things*. The Hague: Rathenau Instituut, available at: https://www.rathenau.nl/en/publication/beyond-control.

European Data Protection Supervisor (EDPS) (2015) *Opinion 4/2015, Towards a new digital ethics - Data, dignity and technology*, 11 September 2015.

European Data Protection Supervisor (EDPS) (2016) *Artificial Intelligence, Robotics, Privacy and Data Protection, Room Document for the 38th International Conference of Data Protection and Privacy Commissioners*, October 2016.

European Data Protection Supervisor (EDPS) (2017) *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 March 2017.

European Parliament, Committee on Legal Affairs (JURI Committee) (2017) *Report with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103(INL)), 27 January 2017.

Eyal, N. with R. Hoover (2014) *Hooked: How to build habit-forming products*. Penguin Random House.

Floridi, L. (ed.) (2015) *The onlife manifesto: Being human in a hyperconnected world*. Springer; doi:10.1007/978-3-319-04093-6.

Fuchs, M. (2015) *Session 2 - Technology, Intervention and Control of Individuals*. In: Whittall, H. (editorial coordinator), L. Palazzani, M. Fuchs & A. GazsóGazo (2015) DH-BIO/INF (2015) 15, *Emerging technologies and human rights*, international symposium 4 – 5 may 2015.

Garvie, C., A. M. Bedoya & J. Frankle (2016) The Perpetual Line-up: Unregulated Police Face Recognition in America - Unregulated Police Face Recognition in America, Center on Privacy & Technology at Georgetown Law, 18 October 2016, available at: www.perpetuallineup.org.

Goodman, B. & S. Flaxman (2016) European Union regulations on algorithmic decision-making and a "right to explanation", arXiv:1606.08813v3 [stat.ML], 31 August 2016.

Grimmelmann, J. (2015) The Law and Ethics of Experiments on Social Media Users. 13 *Colo. Tech.* L.J. 219, 2015, U of Maryland Legal Studies Research Paper No. 2015-15, available at: https://ssrn.com/abstract=2604168.

Hansen, S.T., H.J. Anderseon & T. Bak (2010) Practical evaluation of robots for elderly in Denmark: An overview. *Proceedings of the fifth ACM/IEEE international conference on human-robot interaction* (pp. 149-150), Osaka, Japan, March 2-5. Piscataway, NJ. US: IEEE Press; doi:10.1109/HRI.2010.5453220.

Harris, J. (2012) Modern medicine. *The Farmer & Farmer Review: Essays about Humans & Technology*, May 7, available at: http://farmerandfarmer.org/medicine/.

Hern, A. (2016) 'Partnership on AI' formed by Google, Facebook, Amazon, IBM and Microsoft. *The Guardian*. 28 September 2016. https://www.theguardian.com/technology/2016/sep/28/google-facebook-amazon-ibm-microsoft-partnership-on-ai-tech-firms. Accessed 20 April 2017.

Hildebrandt (2012) The Dawn of a Critical Transparency Right for the Profiling Era. In: Bus, J. (ed.), *Digital Enlightenment Yearbook 2012*, pp. 41-56, Amsterdam IOS Press 2012; doi:10.3233/978-1-61499-057-4-41.

Hildebrandt, M. (2016) Data-gestuurde intelligentie in het strafrecht. In: Moerel, E.M.L. & J.E.J. Prins, M. Hildebrandt, T.F.E Tjong Tjin Tai, G-J. Zwenne & A.H.J. Schmidt (2016) *Homo Digitalis*. Handelingen Nederlandse Juristen-Vereniging 146e jaargang/2016-I. Wolters Kluwer.

International Working Group on Data Protection in Telecommunications (Berlin Telecom Group) (2013) *Working Paper on Web Tracking and Privacy – Respect for context, transparency and control remains essential* 53rd meeting, 15-16 April 2013, Prague.

International Working Group on Data Protection in Telecommunications (Berlin Telecom Group) (2014) *Working Paper on Big Data and Privacy – Privacy principles under pressure in the age of Big Data analytics* 55th Meeting, 5 – 6 May 2014, Skopje.

Kaminski, M. E. & Witnov, S. (2015) The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech. *University of Richmond Law Review*, Vol. 49, 2015; Ohio State Public Law Working Paper No. 288, available at: https://ssrn.com/abstract=2550385.

KNAW (Royal Netherlands Academy of Science) (2016) *Ethical and legal aspects of informatics research*, Amsterdam, KNAW. https://www.knaw.nl/nl/actueel/publicaties/ethical-and-legal-aspects-of-informatics-research.

Koebler, J. (2017) 'Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware,' *Motherboard*, 21 March 2017, https://motherboard.vice.com/en_us/article/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware.

Konrath, S.H., E.H. O'Brien & C. Hsing (2011) Changes in dispositional empathy in American college students over time: A meta-analysis. *Personality and Social Psychology Review* 15 (2): 180-198; doi: 10.1177/1088868310377395.

Kool, L., J. Timmer & R. van Est (eds.)(2015) *Sincere support: The rise of the e-coach*. The Hague: Rathenau Instituut, available at: https://www.rathenau.nl/nl/publicatie/sincere-support-rise-e-coach.

Koops, E. J., Di Carlo, A., Nocco, L., Cassamassima, V., & Stradella, E. (2013) Robotic technologies and fundamental rights: Robotics challenging the European constitutional framework. *International Journal of Technoethics*, 4(2), 15-35; doi:10.4018/jte.2013070102.

Korff, D. & M. Georges (2015) *Passenger Name Records, data mining & data protection: the need for strong safeguards*. T-PD(2015)11, Strasbourg,15 June 2015.

Korff, D. (2013) *The use of the Internet & related services, private life & data protection: Trends & technologies, threats & implications*. T-PD(2013)07Rev, 31 March 2013.

Kosinski, M., Stillwell, D. and Graepel, T. (2013) Private traits and attributes are predictable from digital records of human behavior, *Proceedings of the National Academy of Sciences of the United States of America (PNAS)*, vol. 110 no. 15, 5802–5805; doi:10.1073/pnas.1218772110.

Kramer, A.D.I, J.E. Guillory & J.T. Hancock (2014) Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences* 111 (24): 8788-8790; doi:10.1073/pnas.1320040111.

Kranzberg, M. (1986) Technology and History: 'Kranzberg's Laws", *Technology and Culture* 27, 3: 544-560.

Leroux, C. & R. Labruto (2012) *D3.2.1 Ethical Legal and Societal Issues in Robotics*, The European Robotics Coordination Action, 31 December 2012.

McGonagle, T. (2013) *The Council of Europe against online hate speech: Conundrums and challenges*. Expert paper, doc.no. MCM 2013(005), the Council of Europe Conference of Ministers responsible for Media and Information Society, 'Freedom of Expression and Democracy in the Digital Age: Opportunities, Rights, Responsibilities', Belgrade, 7-8 November 2013, available at: http://www.ivir.nl/publicaties/download/Expert_paper_hate_speech.pdf.

Moerel & J.E.J. Prins (2016) Privacy voor de homo digitalis. In: Moerel, E.M.L. & J.E.J. Prins, M. Hildebrandt, T.F.E Tjong Tjin Tai, G-J. Zwenne & A.H.J. Schmidt (2016) *Homo Digitalis*. Handelingen Nederlandse Juristen-Vereniging 146e jaargang/2016-I. Wolters Kluwer.

Mordini, E., I. Vater, K. Wadhwa, A. D'Amico, J. Thestrup, G. Van Steendam, D. Wright & P. De Hert (2008) *SENIOR Discussion Paper 'Ethics of e-inclusion of older people'*, 12 May 2008, available at: http://www.cssc.eu/public/Ethics%20of%20e-Inclusion%20of%20older%20people%20-%20Bled%20%20Paper.pdf.

Murdoch, J. (2012) *Protecting the right to freedom of thought, conscience and religion under the European Convention on Human Rights*. Strasbourg: Council of Europe human rights handbooks.

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

Pasquale, F. (2016) Bittersweet Mysteries of Machine Learning (A Provocation). LSE Media Policy Project, The London School of Economics and Political Science, Media Policy Project Blog, available at: https://blogs.lse.ac.uk/mediapolicyproject/2016/02/05/bittersweet-mysteries-of-machine-learning-a-provocation.

Pentland, A. (2014) *Social physics: How networks can make us smarter*. Penguin Books.

Perzanowski, A. & W. Schultz (2016) *The end of ownership: Personal property in the digital economy*. Cambridge: The MIT Press.

Purtova, N. (2013) Illusion of Personal Data as No One's Property, *Law, Innovation, and Technology*, Volume 7, Issue 1, 2015, available at: https://ssrn.com/abstract=2346693.

Roosendaal, A.P.C. (2012) "We Are All Connected to Facebook…by Facebook!". In: S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?,* Heidelberg: Springer, pp. 3-19.

Roosendaal, A.P.C., T. Van den Broek, A.F.E. Van Veenstra (2014) Vertrouwen in big data-toepassingen: accountability en eigenaarschap als waarborgen voor privacy. *Privacy en informatie,* 2014 (3). ISSN 1388-0241.

Rouvroy, A. (2016) *"Of Data and Men" - Fundamental rights and freedoms in a world of big data*, T-PD-BUR(2015)09REV, 11 January 2016, available at: http://works.bepress.com/antoinette_rouvroy/64/.

Royakkers, L. & R. van Est (2016) *Just Ordinary Robots: Automation from Love to War*. Boca Raton, FL: CRC Press.

Schneier, B. (2013) The Public-Private Surveillance Partnership, *Bloomberg View* 31 July 2013, available at: https://www.bloomberg.com/view/articles/2013-07-31/the-public-private-surveillance-partnership.

Schüll, N.D. (2013) *Addiction by Design: Machine Gambling in Las Vegas*. Princeton: Princeton University Press.

Schüll, N.D. (2016) Interviewed in Tegenlicht-documentary 'What makes you click?', September 25, Hilversum: VPRO, available at: https://www.vpro.nl/programmas/tegenlicht/kijk/afleveringen/2016-2017/what-makes-you-click.html.

Schutz, B. (2016) Interviewed in Tegenlicht-documentary 'What makes you click?', September 25, Hilversum: VPRO, available at: https://www.vpro.nl/programmas/tegenlicht/kijk/afleveringen/2016-2017/what-makes-you-click.html.

Science and Technology Options Assessment (STOA) (2016) *Ethical Aspects of Cyber-Physical Systems Scientific Foresight study*, June 2016.

Scott, J.C. (1999) *Seeing Like a State*, Yale University Press 1999.

Sganga, C. (2014) Cracking the citadel walls: a functional approach to cosmopolitan property models within and beyond national property regimes, *Cambridge Journal of International and Comparative Law* (3)1: 770–794; doi:10.7574/cjicl.03.03.230.

Shalev, S. (2008) *A Sourcebook on Solitary Confinement*. London: Mannheim Centre for Criminology,

London School of Economics, available online at: http://www.solitaryconfinement.org/sourcebook.

Sharkey, A. & N. Sharkey (2012) Granny and the robots: Ethical issues in robot care for elderly. *Ethics and Information Technology* 14 (1) 27-40.

Sharman, A. (2015) 'BMW sounds alarm over tech companies seeking connected car data', *Financial Times*, 14 January 2015.

Song, W.-K. & J. Kim (2012) Novel assistive robot for self-feeding. In: Dutta, A. (eds.) *Robotic Systems - Applications, Control and Programming*, inTech; doi:10.5772/1398.

Stahl, B.C., J. Timmermans & C. Flick (2016) Ethics of emerging information and communication technologies: On the implementation of responsible research and innovation. *Science and Public Policy*, pp. 1-13; doi:10.1093/scipol/scw069.

Strand, R. & M. Kaiser (2015) *Report on Ethical Issues Raised by Emerging Sciences and Technologies*, Centre for the Study of the Sciences and the Humanities, University of Bergen, Norway, 23 January 2015.

Sunstein, C. (2001) *Echo chambers: Bush v. Gore, impeachment, and beyond.* Princeton & Oxford: Princeton University Press.

Tjong Tjin Tai, T.F.E. (2016) Privaatrecht voor de homo digitalis: eigendom, gebruik en handhaving. In: Moerel, E.M.L. & J.E.J. Prins, M. Hildebrandt, T.F.E Tjong Tjin Tai, G-J. Zwenne & A.H.J. Schmidt (2016) *Homo Digitalis*. Handelingen Nederlandse Juristen-Vereniging 146e jaargang/2016-I. Wolters Kluwer.

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

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

Van Alsenoy, B., V. Verdoodt, R. Heyman, E. Wauters, J. Ausloos & G. Acar (2015) *From social media service to advertising network A critical analysis of Facebook's Revised Policies and Terms*, KU Leuven Center for IT & IP Law - iMinds, Working Paper, version: 1.3, available at: https://www.law.kuleuven.be/citip/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation.

Van Dam, C. (2013) *European Tort Law*, Oxford: Oxford University Press.

Van de Poel, I.R. & L.M.M. Royakkers (2011) *Ethics, technology, and engineering: An introduction*. Oxford, UK: Wiley-Blackwell.

Van den Hoogen, R.H. (2007) *E-Justice, beginselen van behoorlijke elektronische rechtspraak,* The Hague: SDu Uitgevers.

Van der Sloot, B. (2014) Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data? *JIPITEC* 230, 5 (2014), available at: https://www.jipitec.eu/issues/jipitec-5-3-2014/4097.

Van Est, R. & D. Stemerding (eds.)(2012) *European governance challenges in bio-engineering – Making perfect life: Bio-engineering (in) the 21st century. Final report*. Brussels: European Parliament, STOA, available at: https://www.rathenau.nl/nl/publicatie/making-perfect-life-final-report.

Van Est, R., D. Stemerdink, V. Rerimassie, M. Schuijff, J. Timmer & F. Brom (2014) *From bio to NBIC – From medical practice to daily life. Report written for Council of Europe, Committee on Bioethics*. The Hague: Rathenau Instituut, available at: https://www.rathenau.nl/nl/publicatie/bio-nbic-convergence-medical-practice-daily-life.

Van Est, R., J. Timmer, L. Kool, N. Nijsingh, V. Rerimassie & D. Stemerding (2016) *Rules for the digital human park: Two paradigmatic cases of breeding and taming human beings: Human germline editing and persuasive technology*. Peer reviewed background paper for the 11th Global Summit of National Ethics / Bioethics Commissions, Berlin, March 16-18, organized by Deutscher Ethikrat, World Health Organization and United Nations Educational, Scientific and Cultural Organization (UNESCO), available at: https://www.rathenau.nl/nl/publicatie/regels-voor-het-digitale-mensenpark.

Van Est, R., with the assistance of V. Rerimassie, I. van Keulen & G. Dorren (translation K. Kaldenbach) (2014) *Intimate technology: The battle for our body and behaviour*. Den Haag: Rathenau Instituut, available at: https://www.rathenau.nl/en/publication/intimate-technology-battly-our-body-and-behaviour.

Vermesan, O. & P. Friess (coordinators)(2015) *Internet of Things – IoT Governance, Privacy and Security Issues.* European Research Cluster on the Internet of Things (IERC).

Wachter, S., B. Mittelstadt & L. Floridi (2016) *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation* (December 28, 2016), available at: https://ssrn.com/abstract=2903469.

Warren, S. D. & L.D. Brandeis (1890) The right to privacy. *Harvard Law Review*, Vol. 4(5): 193-220.

Weisberg, J. (2016) We are hopelessly hooked. *The New York Review of Books*, February 2016, pp. 6-9, available at: http://www.nybooks.com/articles/2016/02/25/we-are-hopelessly-hooked/.

Winkels, R. (2011) Lex ex Machina: Kunnen robots rechtspreken? In: F. Brom et al. (red.) *Kenniskamer Intelligente Robots – Feiten, fabels, fictie.* The Hague: Ministerie van Veiligheid & Justitie, Rathenau Instituut, available at: https://www.rathenau.nl/nl/publicatie/kenniskamer-intelligente-robots-feiten-fabels-en-ficties.

WRR, Wetenschappelijke Raad voor het Regeringsbeleid (2016) *Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press, available at: https://www.wrr.nl/publicaties/verkenningen/2016/04/28/exploring-the-boundaries-of-big-data-32.

WRR, Wetenschappelijke Raad voor het Regeringsbeleid (2016b) *Big Data in een vrije en veilige samenleving*, Amsterdam: Amsterdam University Press, available at: https://www.wrr.nl/publicaties/rapporten/2016/04/28/big-data-in-een-vrije-en-veilige-samenleving.

Ylimaula, A., Roelofsma, P.H.M.P., Versteeg, L. (2010) *Ambient Assisted Living - Deliverable 3.2 Ethical and legal requirements*.

Zentner, M. (2015) Education for participation in a digitalised world. In: Youth Partnership – Partnership between the European Commission and the Council of Europe in the field of youth. *Report - Symposium on youth participation in a digitalised world*, Budapest, 14 - 16 September 2015, available via: https://pjp-eu.coe.int/web/youth-partnership/digitalised-world.

Zuboff, S. (2015) Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 3 (1), pp. 75-89; doi:10.1057/jit.2015.5.

Zuiderveen Borgesius, F. & D. Trilling, J. Möller, B. Bodó, C. de Vreese & N. Helberger (2016). Should

we worry about filter bubbles?. *Internet Policy Review*, 5(1); doi:10.14763/2016.1.401.

Zuiderveen Borgesius, F. (2014) *Improving privacy protection in the area of behavioural targeting*, Alphen aan den Rijn: Kluwer Law International.

About the authors

Rinie van Est is research coordinator with the Rathenau Instituut. He has a background in applied physics and political science. At the Rathenau Instituut he is primarily concerned with emerging technologies such as nanotechnology, cognitive sciences, persuasive technology, robotics and synthetic biology. He has many years of hands-on experience with designing and applying methods to involve experts, stakeholders and citizens in debates on science and technology in society. He also lectures at the School of Innovation Sciences of the Eindhoven University of Technology. Some relevant publications are *Just ordinary robots: Automation from love to war* (2016), *Working on the robot society* (2015), *Intimate technology: The battle for our body and behaviour* (2014), *From bio to NBIC: From medical practice to daily life* (2014), *Check in / check out: The public space as an Internet of Things* (2011).

Joost Gerritsen is a privacy and data lawyer at Legal Beetle, The Netherlands. His legal expertise is primarily focused on the legal aspects of (emerging) technologies, such as robotics, big data and AI.

Linda Kool is a senior researcher at the Rathenau Instituut. She conducts research on various social issues in the field of Information and Communication Technology (ICT), such as Big Data, robotics, persuasive technology, and Artificial Intelligence. She studied Social Science Informatics at the University of Amsterdam and has a Master's in European Studies of Society, Science and Technology (ESST) from Maastricht University and the University of Oslo. Some relevant publications are *Beyond Control* (2016) about privacy and the Internet-of-Things, *Sincere Support* (2015) about e-coaches and *Working on the robot society* (2015).

Who was Rathenau?

The Rathenau Instituut is named after Professor G.W. Rathenau (1911-1989), who was successively professor of experimental physics at the University of Amsterdam, director of the Philips Physics Laboratory in Eindhoven, and a member of the Scientific Advisory Council on Government Policy. He achieved national fame as chairman of the commission formed in 1978 to investigate the societal implications of micro-electronics. One of the commission's recommendations was that there should be ongoing and systematic monitoring of the societal significance of all technological advances. Rathenau's activities led to the foundation of the Netherlands Organization for Technology Assessment (NOTA) in 1986. In 1994 this organization was renamed 'the Rathenau Instituut'.