The Digital Self

Digital Transformation in Learning for Active Citizenship

By Nils-Eyk Zimmermann

dare
Democracy and
Human Rights Education
in Europe

BLUE LINES

Digital Self
Part of the reader
“Smart City, Smart Teaching: Understanding Digital Transformation in Teaching and Learning.”

Author: Nils-Eyk Zimmermann
Co-edited by: Ramón Martínez and Elisa Rapetti
Copy-editing: Katja Greeson
Design: Katharina Scholkmann (layout), Felix Kumpfe, Atelier Hurra (illustration)
Publisher: DARE – Democracy and Human Rights Education in Europe vzw., Brussels 2020
Editors of the series: Sulev Valdmaa, Nils-Eyk Zimmermann

The project DIGIT-AL – Digital Transformation in Adult Learning for Active Citizenship – is a European cooperation,
coordinated by Association of German Educational Organizations (AdB)
with
DARE – Democracy and Human Rights Education in Europe vzw. (BE)
Centre for International Cooperation CCI (IT)
Education Development Center (LV)
Jaan Tõnisson Institute (EE)
Partners Bulgaria Foundation (BG)
Rede Inducar (PT)

Supported by:

Federal Ministry for
Family Affairs, Senior Citizens,
Women and Youth

Co-funded by the
Erasmus + Programme
of the European Union

The project is supported in the framework of the Erasmus+ program of the European Commission (Strategic Partnership in the field of Adult Education). Project Number: 2019-1-DE02-KA204-006421

The European Commission‘s support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Preface:

Into Digital Transformation

The social, economic, cultural and political impact of digital change in education and learning

Digitalisation is an essential part of our lives across all dimensions. Many people think that it is a technological process, i.e. it is mainly about computer servers, algorithms, Internet and the like. But that is only half of the truth. For example, it is difficult to separate digitalisation from almost all activities in our lives. When we shop online – are we online or are we shopping? When we play computer games – are we playing or are we at the computer? And when we are active in social media, we are both social and active in an electronic medium. Moreover, our health system is already digitised, the pollution of the planet is, to a growing extent, caused by digital technology, and activities such as navigating a car or collaboration in civil society are increasingly facilitated by digital technology.

This example seeks to point out that what we ultimately understand by ”digitalisation” depends very much on how we look at the topic. It is after all possible to engage in all the aforementioned activities without information and communication technology (ICT). In this sense, we prefer the term *digital transformation*, because it explains a social, cultural or economic process in which things are done seemingly differently – made possible by information and communication technology. In this sense, education for digital transformation is learning about social, economic and cultural processes and about understanding the differences caused by technology. As such, in further exploring the topic, it is important to:

1. Look at both the technology and the nature of economic, social and cultural activities, for example, what we do in different social roles as digital customers, digital activists, digital workers and digital citizens.

2. Take an interest in the difference that digitalisation brings to such activities. What is changing thanks to new technology? What impact does it have on society?

There is No Overly Complex Issue for Education

A lot of curiosity and increasing concerns regarding digitalisation today have to do with its ‘engine room’ - the fascinating global infrastructure of the Internet, its enormous costs and hunger for energy, Big Data, AI, and the increasing economic value of digital platforms.

In particular, the growth of new kinds of platforms, fuelled by digital business models successfully capitalizing on users, is a widely visible phenomenon of this new technological and economic configuration. Consequently, their users are at the same time subjects and objects of digital change. They experience the opportunities made available through new, platform-mediated forms of interaction, but also feel uncomfortable since they are also symmetrically affected in their role as autonomous subjects. The right to independent information, privacy and security are, from this perspective, not yet sufficiently respected in the digital sphere.

The migration of substantial parts of working and communication processes to the digital sphere during the last decades is also simultaneously a benefit and a challenge. One aspect is technical mastery – access to current technology and the ability to use it in a competent way. A more fundamental aspect is that the “digital self” is completing people’s analogue identity. Their digital traces are accompanying people’s lives with related consequences for their various social roles as private subjects, employees and citizens.

Feeling overtaxed by all the associated challenges and concerns is a bad prerequisite for learning and a bad basis for considering future personal and social decisions. It is high time for adult education and youth work to do something about this double-edged sword.

In particular, adult citizenship education has a lot of experience teaching complex social issues and could transfer its methodology and approach to the topic of digital transformation. We know, for example, that nobody needs to be an economist to be able to co-decide on political decisions affecting the economy. We also are capable of understanding the social impact of cars, despite very limited knowledge of automotive engineering. Considering that it is possible to acquire knowledge about digital transformation, could we not even enjoy learning about Big Data, robotics, algorithms or the Internet of tomorrow similar to the way we passionately discuss political issues such as transport, ecology, or democracy? We should not, however, be blinded by the technical complexity of the digital transformation. It is important that we pay more attention to the social dimension, the intentions behind a technology, exploring its effects and regulations.

Although not familiar with all technical or legal details, most people intuit that it is ill-advised to give out personal information without consent. We suppose what the right to privacy should entail and what distinguishes conscious decisions from uninformed ones, and in our analogue world, we discourage the ”used car salesmen” of our society from taking unsuspecting customers for a ride. After all, most of us have experienced the discomfort of having been deceived as a result of not understanding the fine print.

If we transfer this insight to a pedagogy of digital transformation, we must admit that we should also be willing to explore new aspects of the technical dimension such as data processing or the nudging mechanisms in online platforms. But that is not the only priority! The most important thing is that we know what our *rights* and *ethical foundations* are and how they relate to the new digital contexts and are able to act accordingly. These questions are not solely related to privacy and safety, as seemingly no aspect of social life is unaffected by digital transformation.

Using this foundation, we might further explore the potentials and risks of digitalisation in context, assessing its impact. Personal rights, for instance, entail privacy issues, but digital transformation has also led to new opportunities for co-creating, better information, or involvement of citizens in decision-making processes. On this basis, we are then able to define the conditions and rules under which certain digital practices should be rolled-out or restricted.

E*lectronic* communication has changed the character of *human communication* as a whole. There are fewer impermanent ideas or assertions that go undocumented, to later be searched and rehashed. This change is both positive and negative, for example from the perspective of an employee who may be judged based on past decisions which live forever online. Pedagogy might help people to better understand the risks and benefits associated with electronic communication.

In addition, it will be a creative challenge to imagine the technology we want to develop as a society and what will help us to initiate social, economic and cultural changes in the future. In this regard, it is also important to develop a view towards the so-called ‘skill gaps’ and ‘digital gaps’ people may face when mastering digitalisation. What is the purpose of defining a gap; for whom is the gap relevant; in whose interest is it to argue the risk of gaps as opposed to their benefits?

Why Democracy and Rights-based Learning Makes the Difference

The essence of a definition of democracy and rights-based education can be found in the Council of Europe's Declaration regarding Education for Democratic Citizenship (EDC), which is "education, training, awareness-raising, information, practices, and activities which aim, by equipping learners with knowledge, skills and understanding and developing their attitudes and behaviour, to empower them to exercise and defend their democratic rights and responsibilities in society, to value diversity and to play an active part in democratic life, with a view to the promotion and protection of democracy and the rule of law" (CoE CM/Rec(2010)7).

Transferred to the context of learning about digital transformation, we extract three core questions from this:

1. *What digital transformation competence* – knowledge, skills, values and attitudes – do citizens need to understand the digital transformation in their society and how it affects them in their different social roles?

2. How are *fundamental rights and ethical foundations* related to the transformation? Where do they shift their nature, what weakens them and what kind of development strengthens their enforcement?

3. What *active civic competences* do citizens need to contribute to the transformation, including participation in relevant public discourses and decisions, self-organisation and social engagement, and the development of social innovations?

Stakeholders from many different sectors have high expectations in education. In particular, they demand from earning for active citizenship a better preparation of Europeans for big societal changes. Only if we implement ideals of democracy "by design" into digital progress will we create a *democratic* digital society.

Enjoy and Explore

This reader series aims to introduce selected key aspects of digital transformation to educators and teachers in formal, non-formal or informal education. Our perspective is *Education for Democratic Citizenship* and our main goal is to motivate you as educators in adult education and in youthwork or other education fields to dive into the topics connected to digital transformation with curiosity and critical thinking as well as ideas for educational action. In other words: Nobody has to adore technology, but it is definitely worthwhile to become more comfortable with it. Digital transformation is a reality and as such, in principle, relevant for any specific field of education, any subject, or pedagogy.

Together we might work on a broader understanding of what digital literacy is and explore as educators and learners in lifelong learning processes how it affects our lives. With a strong aspect of democracy and human rights in lifelong learning, we should lay the foundations for a democratic digital transformation and empower learners to find a constructive and active position in this transformation.

We aim to provide basic insights into some of the various aspects of digital transformation as a basis for further exploration. They tackle the digital-self, participation, the e-state, digital culture, media and journalism and the future of work and education. In each of the publications we also present our ideas as to how education might take up this specific topic.

You may access, read, copy, reassemble and distribute our information free of charge. Also, thanks to digital transformation (and the Erasmus+ program of the European Commission) we are able to publish it as an "Open Educational Resource" (OER) under a "Creative Commons License" (CC-BY-SA 4.0 International).

About the Digital Self

For generations, people have done many things in order to extend their abilities or consciousness. Even before the invention of the term "wearable", we have used tools like glasses, watches, walking sticks, steel helmets, hearing devices and wheelchairs or used mind-altering consumables. Extending our bodies and connecting ourselves with others through such tools has influenced the imagination of the self and of the human body's abilities. The question of how digitalisation instigates changes to our body, our social identity and our self-image is becoming apparent for adult and lifelong learning.

This chapter describes the conditions and aspects constituting a digital identity. One important aspect is the machine-human relationship and its underlying constructive conditions. Another is the identificatory aspect of digital technology – the tension between privacy and identifiability (and for whom), and also we need to explore mechanisms of exclusion and inclusion. Therefore, digital transformation has an impact on the ideas of privacy and autonomy and how they might be achieved in the digital social reality, especially under the conditions that big data create.

The second part tackles the question of how the exposure to and embeddedness in digital interaction affects the abilities and attitudes of us as individuals. On a personal level, these are health or performance issues, but on a social level, the question is raised of whether quantification and datafication influence key assumptions in regard to democracy like pluralism, individualism, inclusion, or the ability to innovate.

1. Into the Internet of Everything

As we become more accustomed to devices and digital services, digitalisation is changing our imagination of the body and is influencing our perception of autonomy. In particular, our imagination of humanity is enshrined in the human body and our biggest concerns are about safeguarding its physical inviolability, dignity, and opportunities to move and to participate.

The Internet of Things (IoT) is no longer limited to surrounding devices like intelligent plug sockets, fridges, automotive board computers and factory robots. Wearables and also implants have now "become social actors in a networked environment" (Spiekermann, 2010, p. 2).

The coexistence of more and more apps and of more and more devices around us makes the vision of ubiquitous computing more realistic. *Ubiquitous Computing* describes the 21st century technology as embedded technology. In an Internet of Everything, the machine is spatially no longer separated, for instance in big metal boxes in specific rooms. In the words of digitalisation pioneer Mark Weiser in 1991, a lot of our devices today are more or less "invisible in fact as well as in metaphor". They are small, and we don't recognize them as computers although they technically are. Their value lies in their intuitiveness and connection: "The real power of the concept comes not from any one of these devices; it emerges from the interaction of all of them" (Weiser, 1991, p. 98).

Digital assistants like Amazon's Alexa, Google Assistant and Samsung's Bixby are good examples that have brought ubiquitous home computing to a new scale: They are always on and monitoring their environment including the beings around them, communicating independently with the services behind them.

We no longer experience "stupid" machines that sense environmental data and send it to other machines. More and more, they actively accompany us. When objects become subjects through their interaction with humans, they acquire an identity much different from the serial number engraved on the back. Because they relate to us and have influence on our (self) perception, one key question in this chapter asks how the human-machine interaction contributes to a shifted perception of our self and enriches our analogue identity – what we call the *digital self*.

Beyond interaction, construction is another aspect helpful for understanding the

Digital Identity

Objects and machines become subjects, interacting with people.

Identity is a construction, co-created by the creators and owners of (digitalised) artefacts and digital infrastructure. The identity construction is pre-structured through the principles and rules of computer mediation, which are influencing how individuals are appearing in the digital sphere.

The interaction between things and individuals (among each other and with each other) is creating a new social space, affecting and challenging personal identity and its mastery or management.

Identification of individuals along many diverse and unique (identifiable) features, allows transformation of personal data into meaningful information, a key condition for big data and algorithmic processing.

Digital self: the contribution of human-machine interaction to individual self-description and self-perception.

Inspired by: Chaudron & Eichinger: Eagle-eye on – Identities in the digital world (2018)

issues of digital identity. In an environment that is to a large extent computer-mediated, this term can be literally understood as relying on the construction and infrastructure of providers and creators. The ubiquitous computing was a vision, but today it is a system of devices and a ready-to-use infrastructure. In 1975 Kraftwerk saw this in a visionary way: “This is the voice of energy speaking/I am a huge electronic generator/I am delivering to you light and power/And enable you to send and receive/Language, music and image through the ether, I am servant and master at once…”.

When technology is servant and master at once, users also have a certain influence on how the technical environment around them is formed, similar to how they decide what kind of space they reside in physically. Users plug computers in and attribute them with meaning for their life. But the extent of pre-construction is constantly increasing. While the birth myth of the internet was the promise of horizontal communication, today there is a growing asymmetry to the individual user’s disadvantage. In contrast to the earlier days of the World Wide Web, a network of servers, services and digital norms are co-structuring our social behaviour via platforms, apps, proprietary devices. The underlying

Five biggest concerns against digital assistants

1. Data abuse through the company	33%
2. Interception	33%
3. It’s uncomfortable to talk to computers	29%
4. Wrong interpretation of language	28%
5. Data abuse by third parties	24%
“I have no concerns”	21%

question in regard to our digital identities is how individuals might meet providers and creators at eye-level.

Especially when the Internet of Things and big data come into play, the condition for our interaction is the active involvement of computing power somewhere outside our private sphere. Coming back to the personal digital assistants, we can also phrase it as such: the price for intuitive and individualized computing is reliance on external infrastructure – and also interception.

Technically these devices need to always be in stand-by mode which allows them to cable to their, mostly external, home. A key word activates the process, which privacy activists like the founder of the German association Digitalcourage, Padeluun, criticize. In his criticism of Alexa during the Big Brother Award ceremony in 2018 he described that “the device eavesdrops 24 hours a day in my apartment, always lurking for me saying ‘Alexa’. As soon as it ‘hears’ this, it is going to record the following sentences and send these to the Amazon cloud servers in order to analyse them. My text is going to be translated here, analysed, and actions are then triggered remotely” (Digitalcourage, 2018).

Although most owners of such a device trust in the discretion of the services behind the devices, they raise new challenges. The collected information is going to be saved for longer (if not permanently) not on our individual property but on servers of the service providers which allow them to analyse the collected data afterwards and use it also for other offerings. Second, it is not only algorithms that interpret the information collected through digital services and assistants. The public was informed in 2019 about Amazon letting employees transcribe some Alexa sound snippets. In some cases, conversations were recorded even if the trigger word indicating the activation was not said (Day et al., 2019). In reaction to the Amazon scandal, Microsoft had to admit too that they had intercepted some Skype calls, in particular those where the “intelligent” Skype translator was offering automatic translation.

These human interventions and interceptions are, from a technical point of view, necessary due to lacking intelligence of technology. Humans need to correct and to step into the automatized processes “manually”. Even David Limp, a leading manager at Amazon agrees with this conclusion and is demanding to disenthrall the myths behind Artificial Intelligence (unfortunately only after the scandal). “As a sector, we perceived

Five biggest advantages

1. Quick access to information and search, in example Wikipedia	39%
2. Searching	38%
3. Navigation	28%
4. Using multimedia like music and video	28%
5. Dictates	25%

Source: BVDW, 2017

it as normal that all customers know how artificial intelligence functions. Every such application includes manual checking: For instance, navigation apps are as precise as they are today, because people look and check the routes driven by the users for accuracy. The sector should have communicated this more clearly" (Kapalschinski & Rexer, 2019). This is particularly relevant as people have privacy and integrity concerns as a study from the German lobby organization for digital economy demonstrates (BVDW, 2017).

Gain of Intuition, Loss of Overview

When we recognize the digital sphere as an *environment*, which according to Merriam Webster is "the circumstances, objects, or conditions by which one is surrounded", then a key aspect of digital identity is that persons, services and devices create together a technical-social environment, consisting of devices and infrastructure, apps and data traces. Everybody could be perceived also as the creator of a unique (which also means increasingly unique to identify) app and data ecosystem, that must be managed and mastered.

As previously mentioned, the smartphone is the most distributed digital wearable. It has merged different functions that formerly would have been assigned to different devices like navigators, mp3 players, laptops and watches. New devices like smart watches and fitness trackers have also emerged in recent years. The apps relevant for the body focus in particular on workout/shaping, weight, pregnancy/menstruation, fitness-tracking, movement/maps, and food/cooking. In connection to an always-on tracking device like a smart watch, it is possible to track the body in a simple way. Furthermore, fitness apps are nudging and motivating people to follow health-related goals. Most apps, however, are very generous with data. 16 of 19 fitness apps are, according to a test of German consumer protectionists, "already sending data to third parties (analysis/PR) before consumers have accepted the terms of service and have been informed about the processing of their data" (Moll et al., 2017, p. 21). The integrity of our digital identity relies on how carefully and confidentially others treat it.

Terms and Conditions

21%	always check terms and conditions when using online services
44%	sometimes
34 %	not
48%	finding it easy to consent to personal data usage through online services
50%	no

Source: EU-FRA 2020-2

People typically install numerous apps, using on average ten daily and more than thirty in a month (AppAnnie, 2017). Only in the health sector, the most data-sensitive in regard to the body and physical self, does one find a very differentiated app ecosystem with manifold models of data usage and exploitation (Bertelsmann Stiftung, 2016):

Strengthening health competence: health portals comparing services and providers

Supporting self-efficacy, adherent behaviour and security: digital diaries for chronically ill people, pill reminders, patient communities

Analysis and insight: symptom checkers, hearing tests

Change of abilities, behaviour, and conditions: online courses, tutorials, smartphones as hearing aids

Documentation: electronic patient files

Shopping and supply: online pharmacies

Process management in the health sector: online health insurance apps, appointment apps

What counts for smartphone apps is also valid for different IoT devices. According to CISCO, the number of devices per capita will grow to 9.4 in Western Europe and 4 in Eastern Europe before 2023 (CISCO 2020).

It is easy to go into a forest but challenging to find the way out. The app and data ecosystem is similar. Many efforts intend to make things user-friendly from the very beginning. However, with every new app, update, new device, feature, app authorization, or new way of processing, people lack overview over their connected IT or their manifold installations during its use. Control may become more challenging and confusing. While this could be seen as a question of regular checking and cleaning, another issue is that updates initiated by the services might change fundamental conditions or functions. In particular, the terms of service, ownership and privacy-related adjustments might change unidirectionally through new roll outs. Moreover, the explanations in the terms of service are not helpful for gaining increased clarity. Unlike in the pharmacy, you will most often not find an informative product insert enclosed in digital devices and services.

Beyond the smart mobile devices, the *smart home* should also be mentioned as a part of the environment of this Internet of Everything. It includes not only digital assistants, but the whole collection of digitalised technology in between our four walls. Currently in many countries, water, heating and electricity consumption is measured by smart meters. Manual documentation is not required anymore as the data is transmitted automatically to the supplier. As an added value, digitalisation allows better tracking and analysis. For instance, one can assess the consumption in much more detail than only once or twice a year in aggregated form. In 2019, Google, Amazon, and Apple joined forces to establish a new standard for the Internet of Things: "Connected Home over IP". In 2020, apps and devices for the monitoring and steering of light, heating and plug sockets appeared on the consumer market, as well as connected kitchen machines and fridges. Vacuum cleaners are drawing detailed ichnographies and storing them in a cloud.

On average, each household has ten connected devices, but the tendency to adopt these tools is rising because of the availability of more available and affordable smart home technology (Bitdefender, 2016). More and more tablets, smartphones, TVs, consoles and eBook readers with smart features are complementing or replacing the desktop computer. Connected entertainment and data storage solutions are appearing in our households. Media servers (hard disks with internet access) are replacing spacious CD and DVD collections. Storage disks and network printers are, thanks to their connectivity,

Ubiquitous Computing: A technological vision of many, often small, and very differently connected computing devices, deeply embedded in our daily routines, interacting intuitively with us and with each other.

Internet of Everything: Computed devices for different purposes, of different sizes and with different abilities interact with other devices (Internet of Things), and with the surrounding space through our facility-installed technology (Smart Home), and the social environment.

Tracking: Recording personal data constantly over a certain time period and drawing information out of it.

accessible for different users in our home network or even from outside our home, through the internet. Cameras are becoming connected to smartphones, PCs, or printers, over Wi-Fi or via memory cards with Wi-Fi modules.

Finally, the picture would not be complete if we did not mention the ”datafied” infrastructures outside our four walls. Sensors embedded in our public life measure pollution, noise, traffic and lead to improved management and maintenance of these infrastructures. But also personal information is collected and analysed, for instance by license plate or facial recognition. The combination of such infrastructural information with personal data is making new forms of ubiquitous computing imaginable. This is the narrative of the smart city. The discussion about smart infrastructure is oscillating between visions of horizontal and open data on the one side, and a commodification of public infrastructures through IT, often in private ownership on the other side.

Your Self in Your Digital Home

The more common they are, the more invisible and intuitive technology and processes become, with an ambivalent effect on people’s knowledge and awareness of them. Stocktaking can be a starting point for their control. On average, ten connected devices are part of each household.

- ➡ **How many devices do you connect via your router or mobile?**
- ➡ **How many meters are digitized in your household?**

Between 30% and 40% of users never updated firmware or initiated security updates.

- ➡ **And you?**
- ➡ **Many people don’t know, how that would work. Do you?**

You might control your router through a website (the user interface). For example, you might see how many devices are online and how much data volume you used and when. Here you might as well initiate updates and change passwords or set new accounts.

- ➡ **Have you ever had a look into this backend?**
- ➡ **When did you update your router last?**

Conclusions for Education

Ubiquitous computing is intuitive and becoming a matter of course. However, this comes with two challenges – information and overview. The more we take things for granted, the more we forget them or ignore the conditions necessary for their existence. Only when they don't work, do we realize how dependent we are on them.

Adult learning opportunities might contribute to **information** about the functioning and abilities of the ubiquitous technology close to our body in our everyday space, at work, and also in the public space. It might raise awareness of learners about the concrete activities of the technology under the surface of the visible interaction.

Overview is a condition for control and mastery. Education might facilitate the visualisation of the **extent of personal computerization** and help to see it in relation to others. Learners might be enabled to compare and assess tools and services and also their risks.

This includes knowledge about the **tools and also about the infrastructure** and processing of the data "backstage".

Body-Machine-Interaction

Some devices form very strong and sometimes even permanent bonds with our physical body, most obviously in medical therapy. Some are invasive, e.g. implanting a sensor in the body. Probably most familiar are cardiac pacemakers. According to the European Society for Cardiology, an average of 59 people per one million Central Europeans and 295 out of one million West-Europeans had such a device implanted in 2013 (EUROPACE, 2015).

Others are used in non-invasive therapy, e.g. measuring brain activity through Electroencephalography (EEG), small machines that send electronic stimuli into specific brain regions. Electric implants are common in therapy, such as cardiac pacemakers, cochlear implants (for improving hearing), as well as deep brain stimulation, applied in Parkinson therapy. Artificial lenses increase people's ability to see and might in the future become equipped with sensors – although smart contact lenses seem to be the more feasible technology as they are non-invasive. Exoskeletons, a mixture of a robotic device and a wearable, have started being used in therapy and are expected to help people carry heavy weights in the future. One international research team working in this domain is forecasting that "brain-controlled prosthetic robots that restore independent activities of daily living to paralysed people are about to enter everyday life environments" (Clausen et al., 2017, p. 1338).

It is clear that such devices will have connectivity features implemented in the future. The aforementioned cardiac pacemakers and brain pacemakers are already measuring the body's activities and sharing this data. And other brain-machine interfaces (BMI) are usually not embedded in intensive secondary datafication processes, this might change with their dissemination.

In line with a trend toward automatization, industrial robots are also developing new features toward better interaction. The technological trend hints in the direction of more ubiquitous robotics. The International Federation of Robotics assumes that sensors and smarter control will make robots more cautious or collaborative, no longer fenced in cages for safety reasons (IFR, 2020). Although such collaborative robotics are still only a small part of the worldwide installations, there is a huge potential for broader dissemination of this technology:

"Rather than a large-scale full-automation, the ease of being able to easily incorporate robots into people's work environments as they are is no longer just a large benefit to large companies: It also opens up the possibility of using robots in small to medium-sized enterprises (SME) – often in the form of semi-automation" (IFR, 2019). A feasible future scenario is that robots in industry and in services will accompany human activity to a greater extent, learning from interactions with individuals – requiring an archival of personal data of co-workers and sharing of said data with algorithmic systems.

Clausen et al. help us think about responsibility as human-machine-interaction becomes more ubiquitous "A semi-autonomous robot directly linked to and interacting with a brain makes the source of an act difficult to identify" (2017, p. 1338). A necessity for reliability of such technology is the human ability to control the action of the device or the action triggered by the device. Therefore, the authors advocate that "any semi-autonomous system should include a form of veto control" (Clausen et al., 2017).

In particular, the risk of manipulation of body-machine interaction must also be taken into account. Basically, robots might make unexpected moves from the perspective of their coworkers or their security mechanisms might be turned off. In particular, the risk

Brain-machine Interfaces (BMI):
Electronic connection between brain and computer.

Invasive:
Implanted in the body through a medical surgery.

Non-invasive:
No break in the skin and (temporary) damage to the body.

Brain-hacking:
Manipulating the mental processing, thinking or perception through BMIs or through blocking or manipulating the functions of BMIs

Right to the Integrity of the Person:
"Everyone has the right to respect for his or her physical and mental integrity." Article 3 of the Charter of Fundamental Rights of the European Union (CFR)

of manipulation is high in regard to BMI: “However, development of advanced sensors, allowing brain activity to be recorded at higher spatial resolution, coupled with advances in machine learning and artificial intelligence, could substantially enhance BMI capabilities in the near future and overcome the input-output constraint. This could enable more in-depth ‘mind-reading,’ i. e., classification of brain states related to perceptions, thoughts, emotions, or intentions” (Clausen et al., 2017, p. 1338).

Especially the indirect manipulation through influencing the connection between human and device becomes a feasible technical scenario. Why learn to manipulate an implanted chip if you could just turn it off? “For example, neurally-controlled robotic limbs used to compensate for the motor deficits of amputated patients are potentially vulnerable to mechanical destruction by malicious actors, which would deprive the users of their required motor abilities” (Ienca & Haselager, 2016, p. 3).

Luckily, brain-hacking by input manipulation (false input values), measurement manipulation (inexact measurement results), decoding and classifying manipulation (mistakes in interpretation) or feedback manipulation (when manipulated feedback signals trigger wrong actions) is more difficult. However, such machine manipulation would open new opportunities for enabling people to use their brains and regain autonomy and also for direct manipulation, limiting their autonomy: “The same neural device (e.g. the same BCI) has the potential to be used for good (e.g. assisting cognitive function in neurological patients) as well as bad purposes (e.g. identity theft, password cracking and other forms of brain-hacking)” (Ienca & Haselager, 2016).

The society needs to hedge the manipulation opportunities drastically as they have a bigger damage potential than other forms of influence, since autonomy and freedom of action and perception are at stake. In particular this risk is disparately higher for vulnerable groups, for instance in hospitals, militaries or prisons. The exponential risk would need to be limited by stronger specifications for privacy, control and integrity by design. “If the Charter of the Fundamental Rights of the European Union is claiming in Article 3 a right to integrity (’Every person has the right to physical and mental integrity‘), then the conclusion is [...] that there cannot be an unauthorized access to the brain” (Meckel, 2018, p. 232).

Users need also to rely on the integrity of other connected and surrounding devices and on the integrity of the services acting in their intention. These services should not be allowed to spy or change functionality “behind users’ backs”, whether by stopping support of a heartbeat in the case of a pacemaker nor by sharing data with others. Integrity must also consider actions related to user intention and interest, particularly important in legal cases, when the question arises of whether personal data could be used against an individual (Lobe, 2019, p. 85). To whom are the producers of devices loyal if my right is vis-a-vis others? Legal privileges are foreseen for trusted persons in the analogue world. Lawyers, priests, and doctors are bound to confidentiality and discretion. What kind of loyalties do we need to legally bind other actors in the digital world?

> **Right to the Integrity of the Person**
> **1.** Everyone has the right to respect for his or her physical and mental integrity.
> **2**. In the fields of medicine and biology, the following must be respected in particular:
>
> **(a)** the free and informed consent of the person concerned, according to the procedures laid down by law;
> **(b)** the prohibition of eugenic practices, in particular those aiming at the selection of persons;
> **(c)** the prohibition on making the human body and its parts as such a source of financial gain;
> **(d)** the prohibition of the reproductive cloning of human beings.
>
> Article 3 of the Charter of Fundamental Rights of the European Union (CFR)

Beyond therapeutic implants, there are other more banal purposes for mainstreaming implanted devices, for instance for access or identification. In the future, people might become most familiar with microchipping, which is basically the injection of an Near-Field Communication (NFC) chip as small as a grain of rice into the hand. In Sweden, this seems to be an increasingly accepted technology, triggered by the company Biohax. Around 500 employees of the Swedish branch of TUI allowed their corporation to conduct such implantation in order to simplify access to their offices (Frankfurter Allgemeine Zeitung, 2019). At least 2,000 Swedes wore such implants for access or payment in 2017 (Graveling et al., 2018). Like RFID labels or chips on bank cards (so-called EVM chips) or health insurance cards, NFC chips do not require direct connection to electricity. Instead, they are provided the needed electricity for transmitting their data by the reading device (by induction). Every new smartphone has a built in NFC unit as well.

The example is perhaps the first sign of a larger trend. Prosthetics and implants could increasingly not only help overcome physical limitations but figure as an instrument for over-average performance that could become interesting for larger audiences. “I am the fastest without legs” said the runner Oskar Pistorius. While the first person with disabilities became competitive in a professional athletics arena, immediately the discussion over fairness began. It is possible that the image of ‘able-bodied people’ will shift in the future thanks to such examples (Meyer & Asbrock, 2018).

Disabled or Cyborg?
A Social and Technological Challenge

Interview with Bertolt Meyer, Technical University Chemnitz (Germany)
professor for organizational and economic psychology.

16% of the world population have a disability. In regard to digital transformation, can they expect a golden age?

I would say yes and no. The issues for people having disabilities are manifold. On the one hand, there are dysfunctional limitations that come with a disability. In regard to this aspect, new technology offers to offset these functional limitations to a greater extent than before. In that regard, new technologies promise new inclusion especially for people with certain physical disabilities.

On the other hand, the issues for people with disabilities are not only functional ones. One of the biggest problems that they have beside functional limitations is the stigma and stereotypes leading to structural and psychological disadvantages that they face. Stereotypes and stigma are at least equal problems for inclusion, if not even more compared to the functional limitations.

That being said new technology is a promise to offset functional limitation. Several prosthesis', wheelchairs that can climb stairs, artificial eyes for blind people or cochlear implants for people that lost hearing are examples.

When it comes to stigmas, the idea that the majority of society needs not to change to make society more inclusive, the idea is oppositional, that we have the technology that we might strap on to the disabled persons' body and technology and make the disability disappear. In that sense, the disability would become a burden and responsibility of the disabled person – and not of the majority society. Thereby, stigmas that exclude do not change.

You mentioned in your study a shift in the perception of disabled persons, also in pop culture. Looking at Jaws in James Bond, modernity was no longer reproducing the stereotype of the old veterans with the simple wooden prosthesis.
How does this shift impact the majority's perception of disabled people?

The most common stereotype that people with disability face is the so-called paternalistic stereotype. They are seen by others as what we call 'warm but incompetent'. The two core dimensions of stereotyping are first, how warmly people perceive others from certain groups, and the second is competence or how well people put their intentions into action. Old people and people with disabilities are seen as warm but incompetent. That is why we offer them help, which in so doing we signal to the person that we perceive them as less competent.

What technology can do is to offset this stigma. Modern system devices stand for technological advancement. There is also a weird pop culture discourse happening between the Transhumanist movement that portrays technology as a tool to overcome the limitation of the human body, and prosthetic devices. And suddenly we have a new generation of prosthetics and assisting devices that signal anything but incompetence. We find in our study that such people are almost perceived as able-bodied. Bionic prosthesis not only have a functional benefit to their wearers but also a psychological one.

But again this reduces the stigma to a functional problem. The stigma does not need to change, and that is far away from my idea of an inclusive society.

Activists for inclusion, like Raul Krauthausen, shift the focus from the discourse about the disabled person to the social discourse on disability. They hold the majority responsible for lowering barriers. Could technology lower social barriers?

It seems we are experiencing the effect of technology lowering barriers in early stages. Subtitles in TV shows and on Netflix were initially used as an aid for people with hearing issues, But now others also appreciate subtitles as as they make life easier, for instance enjoying content when you have no headphones with you on your mobile device while on in public transportation. Or we can think about accessibility technology in buildings, originally envisioned for people in wheelchairs but also benefitting the elderly. It's clear that technology makes things barrier-free, making things easier for everyone. The trend in this direction comes with more technology on the way. Making things accessible makes life nicer for everyone.

As this does not lead to singling out people and to othering, I fundamentally agree with the development. I agree with Raul because he says he is fed up with the request to change people's mind before more inclusion could happen. What he says is, the other way around works: Making inclusion happen forces changes on the majority of society.

When looking at the possibilities of technology, to which aspects should we raise more attention?

The discourse reduces disability to certain limitation of the body. Coming back to a quotation of Hugh Herr, the MIT professor amputated below the knees with bionic legs he developed himself: 'I don't see disability, I just see bad technology'. But the central barrier to inclusion is not the inability of the disabled body, it's how the disabled bodies are treated by the mainstream of society on the basis of unconscious biases and systematic discrimination.

What should education address or do better?

First of all, we need to create environments where people are forced to meet and collaborate with people different to themselves. People need experiences with difference. Where better to create such experience than in educational settings? Learners need to appreciate things as normal that are rare or uncommon. We assume that things that are frequent would be normal and good. But we need to appreciate that bodies and minds of people with disabilities are not unnatural or problematic, just less common.

We can create this experience in a lecture hall or a classroom but, of course, we need institutional support and require the necessary resources. And we need teachers and educators with the specific skills to cater to such an inclusive classroom, such as assisting teachers. This is also a structural question.

And in regard to technical literacy and security literacy?

We require in general more technical literacy, for instance in regards to social media. The security aspect you mentioned is also important. New assistive technologies are part of the wider narrative of the merging of network technology and of the human body.

Take my hand prosthesis as an example. It has a Bluetooth interface connected to my mobile phone and my mobile phone again is connected to the internet. Basically, my left hand is something connected to the internet which occludes fundamental issues about privacy and security. Maybe it would become possible to hack someone in the most literal sense of the word. That requires designing privacy-conscious devices and not just strapping it on the top after the design is done. These things are relevant for educating future generations for a more inclusive society.

Conclusions for Education

Prosthetics and BMI are shifting the image of the body. Prosthetics might transform disabilities in extraordinary ways and so shift the discourse on disability. In particular, Education for Democratic Citizenship needs to address the challenges related to **democratic attitudes and rights**. Especially the issue of full participation in society is connected with the idea of **inclusion,** lowering barriers to active participation for all and appreciating social and bodily diversity as a key.

Stigmatization therefore needs to be addressed and reflected upon, and the question of how we as a society can assure people with a specific need fair access to high-tech health technology must be raised

Technology directly linked to our body like implants or other Body Machine Interfaces amplify **security and manipulation risks**. Its development and governance would need broader public attention, but in particular the information and attention of those citizens concerned and affected by them. Here, education has an important role to play, also in the fields of engineering.

Integrity becomes an issue for education. Traditionally this is understood as the physical integrity of the body and under the condition of digital transformation it reaches out to questions tackling the reliability and loyalty of devices and services (technical integrity).

Biometry and Identification

Another meaning of ‘identity’ refers to *identification*. In the digital sphere, this can be a unique set of data, a digital identifier or the sum of diverse traces and pieces referring to us, and unique body characteristics. *Biometry* is technology aiming to identify a person through their personal characteristics or body features.

Taking the example of access technology, one difference of biometry to other systems is the need for storing sensitive body data. The aforementioned injected RFID rice grain or an access chip-card like the ones we use as door keys, for feeding the attendance clock, or as tracking labels in shirts, might send signals every time somebody passes a reading unit (a gate or a box). However, in contrast to biometry, chip-cards can be removed, or it’s possible to shield them (e.g. with aluminium foil).

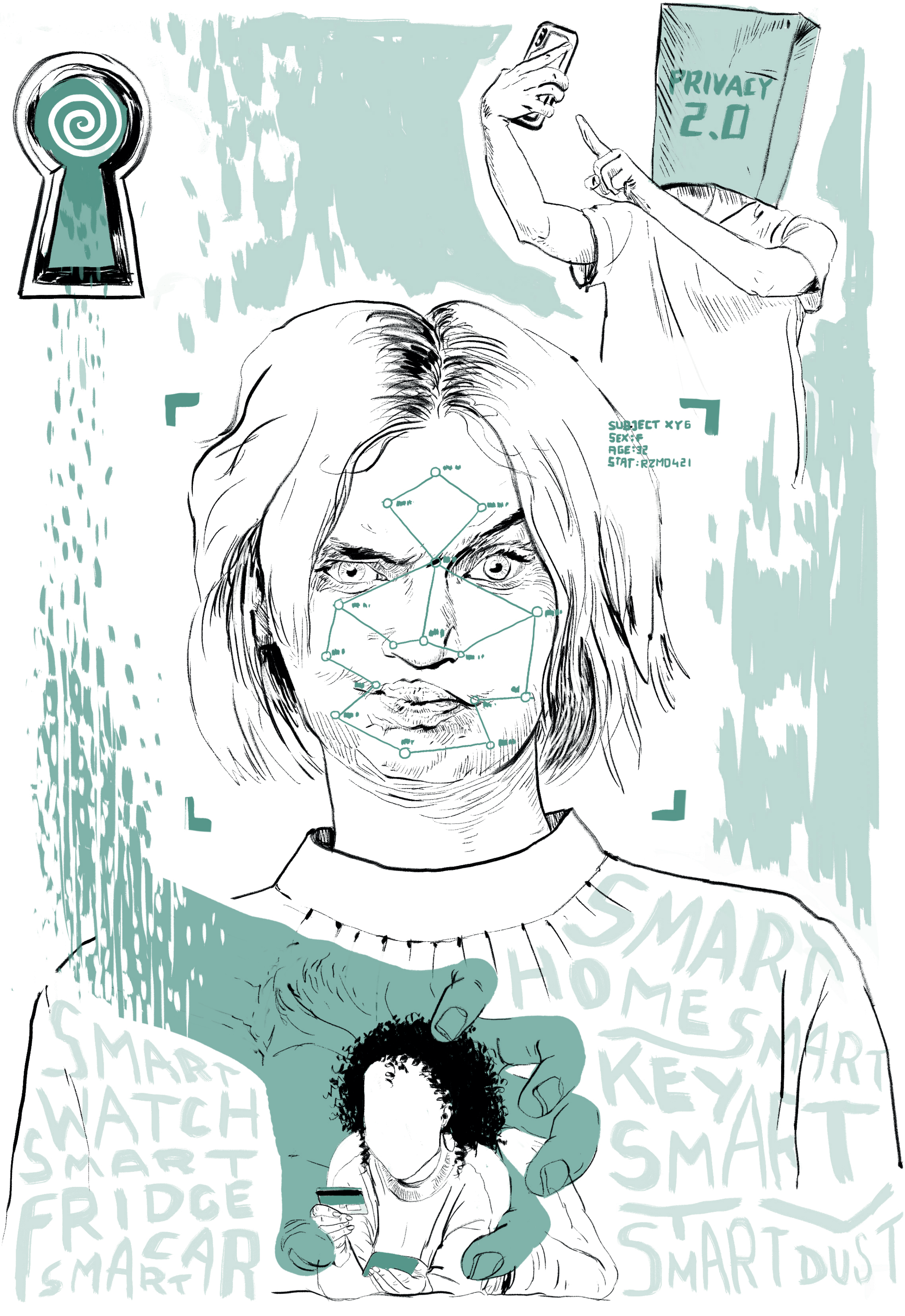
If they are not identified, they will not send signals. Even the injected RFID sensor is more a discrete tattoo – it stays but may be hidden under a shirt.

With biometry this is not so easy. It identifies people through their unique body features directly and not via the detour of identifiers only referring to a person, which can be a unique electronic ID, a password or an access card. In this regard, biometric information must be stored somewhere and compared with the person, facilitated through a biometric system. The European Social and Economic Committee warns in regard to the dangers connected with massively available biometric technology: “Facial recognition, however, will become cheaper and easily accessible to all, for any shop, business or even private individual to use. There are attempts to use these techniques even for emotional recognition. The fear is that facial recognition technology could ultimately lead to a situation where it is no longer possible to walk down the street or go shopping anonymously” (EESC, 2019).

This technology is already widespread. On each European identity card, mandatory fingerprints and facial images are stored. Since biometry was a domain of state data processing for a long time, the technology has become a standard feature for identification in smartphones and computers. Services and employers

Biometry: comparing real body features with stored profiles, e.g. of irises.

Biometric Data: Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
Article 4 (14) EU GDPR


PRIVACY
2.0
SUBJECT XY6
SEX:F
AGE:32
STAT:RZM0421
SMART
HOME
SMART
KEY
SMART
SMART DUST
SMART
WATCH
SMART
FRIDGE
SMART
CAR

collect DNA profiles and scan vein patterns, irises and voice profiles as well. Technology is progressing. At the moment, 3D face scan (Apple) is in focus. Here, the face is reconstructed by a three-dimensional point cloud with the help of a combination of infrared camera, an infrared illuminator and a point projector. In 2020, the start-up, Clearview AI, gained negative publicity because they collected a biometric database of facial pictures and offered their services to around 600 public authorities (Hill, 2020; Holland, 2020). To a large extent, their three billion pictures were collected from publicly accessible accounts such as Twitter and Facebook. Beyond police investigation, the Clearview AI tools might as well be used for questionable purposes such as stalking or identifying political opposition. The company seemed to cross a taboo line and illustrates the damaging potential of biometric products for democracy.

On the other hand, biometric identification techniques regularly confront barriers. One of the major risks of biotechnology is its openness to failure. Iris scans and fingerprint access can be manipulated. A poster from a voting campaign could include enough information for cheating simple iris scanners. The German Chaos Computer Club demonstrated how a fingerprint on a glass held by Germany's Minister of the Interior was replicated with simple materials in silicon, which could have been used to cheat fingerprint sensors (Chaos Computer Club 2014/12/27; Chaos Computer Club 2013/09/21; Kleinz, 2008). The Fundamental Rights Agency of the European Union concludes for facial recognition: "Accuracy has strongly increased, but the technology still always comes with a certain rate of error, which can negatively impact fundamental rights" (EU-FRA, 2020-1).

The European Commission also mentions biometry explicitly as a risky technology. It discusses its governance under strict regulatory limitations and in line with ethical standards, for instance in the 2020 white paper on artificial intelligence (EU COM, 2020/65 final, p. 18).

One challenge is the large-scale usage of biometric technology in *public and semi-public spaces*. Usually, these controls only pay attention to aberrations from normal behaviour, which result in more detailed control measures – for instance through the security service in a shopping centre. Unfortunately, with more technical opportunities, the approach might shift – searching for specific biometric profiles – by profiling individual voices or moving styles. The danger of widespread life biometric technology is that the 'dive into the anonymity' of a city, or discrete meeting in the public is not possible anymore, or at least connected with a lot of obstacles: "There is also a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life (EU-FRA, 2020-1, p. 23).

In witnessing the use of biometry during the beginning of the COVID-19 pandemic, we saw that the body temperature might be measured for monitoring purposes. Increased temperature might be an indicator for a possible infection with a virus, and could entail deeper control at an airport as a result.

Also the COVID-19 apps developed aim to track movements and contacts. They use Bluetooth signals sent out by smartphones, which are more detailed than WiFi or mobile

Measurement and Analysis of Biometric Data:

Built in Sensors in Smartwatches or Fitness Trackers:
Air pressure (height), acceleration, position, geographical position, pulse, surrounding light, heart frequency, sound/voice, blood pressure, body temperature

Other Collections of Biometric Data:
Iris/retina, fingerprint, DNA, ear, signature, style of moving, voice, blood pressure, veins, heart frequency, face

Tracking of States and Activities:
Sleep, activity, steps, emotion/mood, work, keyboard activity, movement, eye movement, interaction with other people, non-activity, consumption, etc.

network login data (particularly inside buildings). Depending on the implementation of such technology, it is possible to track citizens real life networks and their movements by comparing the tracking data of different people. In an authoritarian implementation of such an apps, all would be readable and accessible for the state. The more democratic alternative is to anonymise the tracking profiles before uploading them and then only inform the people that they had contact to an infected person at a certain date and a certain place (without knowing nor sharing the real life *ID* of the person).

The danger of abuse of biometric data is greater for minorities, since norms for surveillance are mostly set by the majority population. What they perceive as ”normal” becomes an unquestionable or more universal norm. Therefore, abusive application of biometric technology and biometric data might enforce conformism, discrimination, or exclusion of specific groups from (public) spaces. How sophisticated would be the racist theories of the late 19th century, if researchers and eugenicists from that time had access to algorithms and big data?

Another concern is that more biometric data is stored in commercial and state databases without the possibility to access and control it by the affected persons. DNA analysis grew as a popular service provided by enterprises like Ancestry.com, 23 & Me, or deCODEme. They offer consumers cheap information about one’s biological linkage and family heritage, when in fact the services collect a social DNA map and try to commodify this very precious (because of its uniqueness) information.

Privacy

The growing ubiquitous computing is challenging our private sphere. Technically the intimate space cannot anymore be separated from its environment, our most discreet emails are not laying in a drawer under the towels but very often on servers out of “our four walls” somewhere. Our discrete things, a pregnancy app or a fitness tracker, are tracking sensitive body data and saving them maybe as long as a drawer would keep them. In contrast to the analogue world, creating a private intimate environment relies heavily on the cooperation and sense of responsibility of others. Even if we treat our apps and services as friends, it is not necessarily true that we want them always to be very close to us. Privacy includes also the right to remoteness, invisibility or disconnection.

In the Internet of Everything, the opportunities for use and abuse increase as data processing and collaboration between devices behind their owners’ backs intensify. When the private sphere is the space closed to the public and the space for intimacy, smart devices and smart homes can also be seen as an invasive technology potentially enabling IT companies and states to execute control in our private spheres. Sometimes

Conclusions for Education

Biometric Technology is increasingly distributed to private customers, companies and the state. It allows easier identification, access regulation but also monitoring and control of individuals. However, it is applied in an unregulated way in public and private spaces. Again, **overview and information** are key for understanding. Education might explain, to what extent and how access and identification technology are used factually and how this affects learners already today.

The use of biometry for monitoring spaces and access to spaces raises concerns for privacy like no other digital technology. A discrete use of public and semi-public spaces would become more difficult, if not impossible, if spatial surveillance were to use biometric technology. Furthermore, modern systems have the opportunity to not only identify the exceptions among a crowd of people, but all persons. Unauthorized access to biometric data allows (automatic) identification of individuals. Education with a strong **fundamental rights focus** might discuss how ubiquitous public and private surveillance relates to the right to private anonymity and also how it affects public engagement and the right to access public space unconditionally.

Biometric technology is becoming a marketable good and as such, it is among the most sensitive types of personal data. The stored information is directly linked to a person and might easily be used for exerting control over individuals or whole groups of the citizenry. **Data economic literacy** would be required in order to enable learners to make informed decisions over whether they would like to share biometric data and information and about their **privacy and property rights**.

an overall social goal such as navigating a pandemic outbreak by collecting and analysing personal data might be accepted, but often not.

Without powerful regulation and ethical limitations, we are not only at risk of losing privacy but also of becoming enmeshed in the Internet of Things, dependent on the digital market and its invisible services, sensors, and algorithms.

Privacy as a right is the legal response to the danger of potential interception. E-Privacy is the response of Human Rights to the challenges of digital transformation in regard to our privacy. New security and surveillance gaps arise in the Internet of Things, if we talk about a smartwatch, a lightning bulb or a printer. With the EU's "ePrivacy Regulation" (Art. 24) which is currently under revision (EP, EC 2002/58/EC) and with the cookie case of the European Court (1. 10. 2019) (European Court of Justice C-673-17), the understanding that devices and personal data are part of the private sphere was confirmed: "Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere". Setting cookies without explicit consent of the owner of a device is already an intrusion into this sphere. Owners and users need to be sure that not only services and infrastructure, but also their technology is not harming them.

Privacy: Respect for private life

"Everyone has the right to respect for his or her private and family life, home and communications."

Article 7 of the Charter of Fundamental Rights of the European Union (CFR)

"Everyone has the right to respect for his private and family life, his home and his correspondence."

Article 8 of the European Convention on Human Rights (Council of Europe)

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Article 12 of the Universal Declaration of Human Rights (United Nations)

E-Privacy:

"Fundamental rights and freedoms [...] in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data"

(Draft of the new EU ePrivacy regulation, EC-COM/2017/010)

Edward Snowden on Privacy:

“What really matters is to be conscious of the principles of compromise. How can the adversary, in general, gain access to information that is sensitive to you? What kinds of things do you need to protect? Because of course you don’t need to hide everything from the adversary. You don’t need to live a paranoid life, off the grid, in hiding, in the woods in Montana.

What we do need to protect are the facts of our activities, our beliefs, and our lives that could be used against us in manners that are contrary to our interests. So when we think about this for whistleblowers, for example, if you witnessed some kind of wrongdoing and you need to reveal this information, and you believe there are people that want to interfere with that, you need to think about how to compartmentalize that” (The Intercept, 2015).

Approaches to privacy protection are in line with Snowden’s recommendation. For instance, the use of integer apps for messaging or browsing. Password messengers protect against phishing. Websites can be accessed through anonymising browsers (like TOR) inhibiting effectively data extraction or the share of system information (location, browser, operating system).

In consequence, devices that we have not paid much attention to for a long time are gaining in importance. The domestic router is the increasingly security-sensitive device and regular software updates are becoming more and more important. Another problem is the lack of security and encryption built in to concrete devices. For instance, WiFi passwords are, in some smart devices, stored in clear text allowing others to extract them and later to access a home network with this information. Other devices have standard passwords (like bulbs, locks, or thermostats). In this regard, a budget bulb could allow the intrusion of a home network (Krempl, 2018).

Privacy Risks

Information collection: Surveillance, interrogation
Information processing: Aggregation, identification, insecurity, secondary and third use, exclusion
Information dissemination: breach of confidentiality, disclosure, exposure, blackmail, appropriation, distortion, increased accessibility
Invasion: intrusion, decisional interference

Source: Solove 2006

Processing and Refinement of Personal Data

The services offered by all kind of platforms are raising questions of privacy in the digital age. Online shops, social media, co-working platforms and other services aimed at connecting people with people or businesses through a technical infrastructure track users and often store and interpret a lot of personal data. The quantity of such collected and stored data is enormous. The author Katharina Nocun requested her data from the online platform Amazon. This enabled her to recall in 15,365 lines and 50 columns her former searches, purchases, dreams, locations from where she accessed the website of Amazon and more (Nocun, 2018, p. 51 ff.).

And the picture would not be complete without mentioning state authorities as interceptors in the interest of public safety or national security. In particular after 9/11/2001, in probably all countries, the investment in surveillance technology, the collaboration between state and private entrepreneurships and the development of state capacity in this field increased. Intelligence Agencies are intercepting internet data, telephone connections, email traffic and also exchanging their information with each other. 29 petabytes of data is monitored by day only by the most prominent world signal intelligence (sigint) agency, the NSA. In particular the monitoring of mobile telecommunication, in some EU countries like France or Poland even without the approval of a judge or the monitoring of internet traffic and storage of meta-data, often under weak legal or political control, are subjects of concern for privacy activists and citizens.

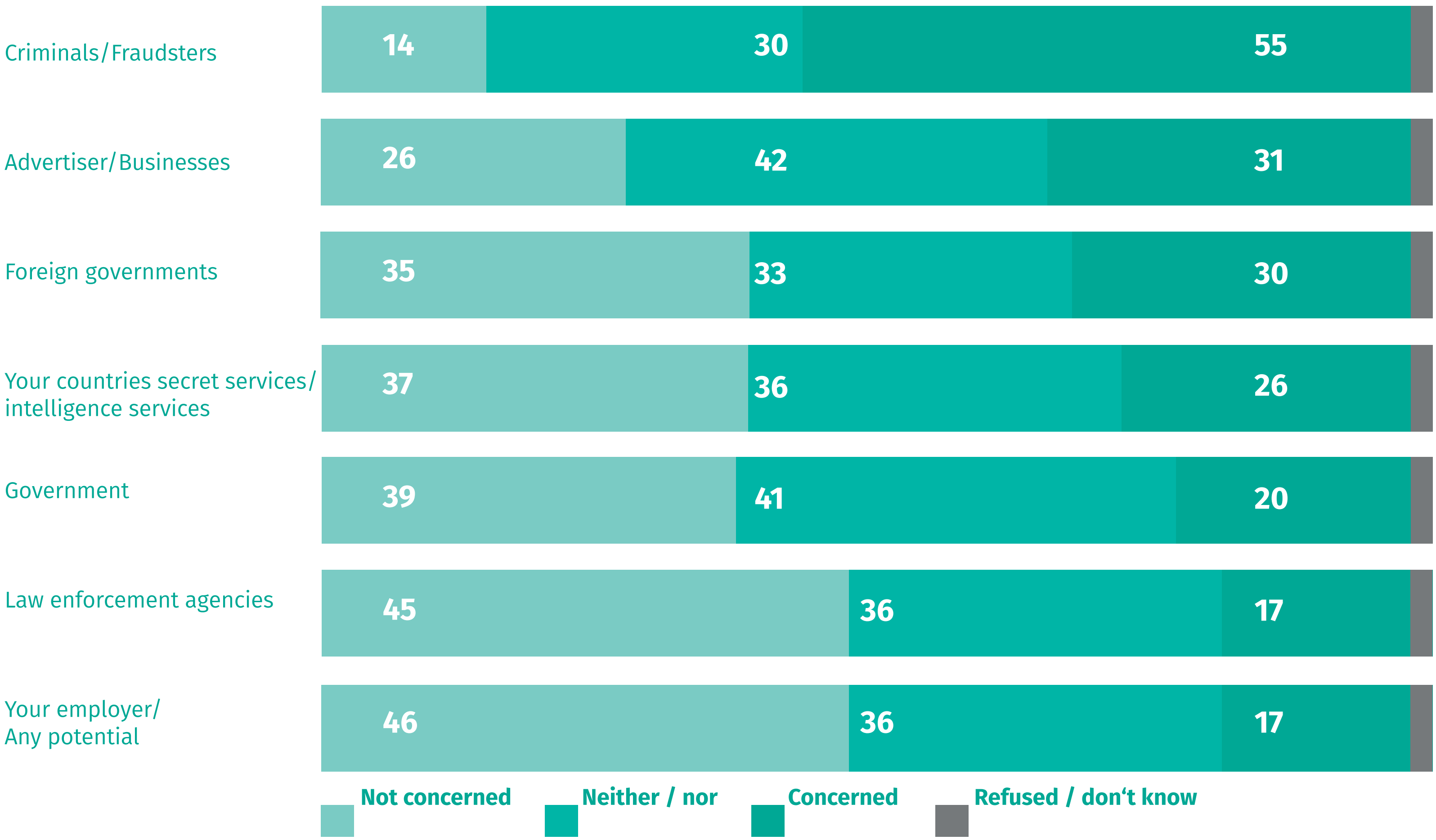
In regard to the newest findings of the EU Fundamental Rights Agency, EU citizens are concerned most with data collection of advertisers/businesses, governments and also employers and law enforcement agencies (EU-FRA 2020-2; p. 5.).

In order to transmute personal data into meaningful information, personal data is becoming also a ware and a mobile good roaming through different servers and used for different purposes. As it is perceived as a raw material for information, this data becomes also a valuable good that is regularly sold and shared.

The shift towards big data can be illustrated with the example of music platforms. During the decade of MP3 players, the legal and illegal music platforms focused on downloads. Today streaming and subscription models have replaced them. Whereas with streaming, a client of Spotify accesses the right of data usage, when downloading, they instead own the files. The ownership shifted from the users to the platforms, which transition away from their role as mediators. Furthermore with streaming, any new access of a music file initiates a new transfer of personal data. Thanks to these mechanisms, the streaming services might monitor and analyse their users' behaviours more in depth than the old platforms. They have access to a full personal consumption profile, including length of usage, kind of music played, skipped parts, how this information relates to that of other users or how a profile fits into the big picture of music consumption in a territory or country.

The machines are drawing constantly more and better information about us and it

Degree of Concern about Third Parties Accessing Personal Information Shared Online, EU-27



Source: EU-FRA 2020-2

is possible to gain more information than traditional statistics, which would categorize people in broad but still anonymous categories (or to stay with the example of mp3 download – the main relevant information was the download statistics).

The main impact of big data in regard to sensitive personal data is the growing availability and marketability of quite detailed personal profiles, describing or even predicting an individual behaviour. Drawing the information out of a huge diversity of different data and through algorithmic and increasingly intelligent processing, insurance companies, online trader or public authorities could, as an example, use this data to better assess risks, tailor contracts, or identify risk groups among their clients or 'data subjects'.

Consumer protection organizations highlight the dilemma caused by the increasing practice of storing and scoring for individuals. In particular health and body data might be useful for one's own purpose but these data are not under personal control: "While using wearables and fitness apps might lead to more autonomy over the personal health, the price is a loss of control over the personally sensitive data" (Moll et al., 2017, p. 42). The DNA service Ancestry.com is exemplary and was for this purpose, like Alexa, prized with the negative Big Brother Award. The statement of the jury: "Who once gives their consent to the 'Ancestry Human Diversity Project' loses control over their genetic data and further, has no influence on who, what and where research with it will be undertaken" (Digitalcourage, 2019).

Since data flow is a common practice, it might happen that data collected in the frame of non-profit activities is landing finally in the database of a commercial enterprise (e.g. from bankruptcy assets). Here, it might be merged with other data under a totally different purpose. Or, perhaps, data is going to be processed under the roof of the state in the public interest. Personal health data could be anonymised and aggregated with health data of other people in order to give insight into potentials for therapies, risks or in better resource management tactics for the health system.

The more normalised tracking through apps and devices becomes, the less transparent one's *data body* is for individuals. That we are more prone to expounding the problems of big data correlates with the emergence of a powerful data economic income model, prominently enforced by the big platforms. In particular, Google and Facebook are avant-garde in this domain. Shoshana Zuboff diagnoses that the valiant purchase and sale of personal data is not the exception one should hedge. Rather, such processing-intensive services and platforms are becoming more and more synonymous with people's associations with the term ”digitalisation”. Zuboff calls this prominent and dominant model a surveillance capitalism.

“Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data” (Zuboff, 2018, p. 8). The transformation of a quantity of seemingly not meaningful data into models for behavioural forecasting is its data-economic surplus.

How does a service provider gain from big data? The data acquired out of an app or website – and in consequence from users – serves only partially the superficial aim of the service, which often is itself offered without charge. The bigger outcome might be the “by-catch” of data collection, or in other words, the by-catch becomes the aim.

In this context, the word *extraction* describes a processing of data in an asymmetric relation with the aim of extracting unilaterally value out of it – or us – which means in “absence of structural reciprocities between the firm and its populations” (Zuboff, 2015, p. 80).

Data Protection:

The right and rules connected to protection of personal data from unauthorized access or use. In particular, personal data must be “processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.”

Article 8 of the Charter of Fundamental Rights of the European Union (CFR)

Personal Data:

“Any information relating to an identified or identifiable natural person (‘data subject’); [...], in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

Article 4 (1) of the EU General Data Protection Regulation (GDPR)

Data Body:

The digital traces of a person complementary to the physical body, in particular the behavioural information or sensitive data that can be drawn out of personal data by others, often not accessible to oneself (data shadow).

Sensitive Data:

"Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

Article 9 (1) of the EU General Data Protection Regulation (GDPR)

Data Processing:

"Any operation or set of operations which is performed on personal data or on sets of personal data, [...] such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

Article 4 (2) of the EU General Data Protection Regulation (GDPR)

Data Extraction:

Gaining information about individual behaviour through data collection and processing for other purposes than those, to which users were aiming to give their consent. In particular, more information about users is collected and processed than necessary for their satisfaction (proprietary behavioural surplus) (Zuboff, 2015)

Visualization of Online Tracking:

Browser plugins like Greenbeam (for Firefox browser) or Ghostery are visualizing the third parties involved in your online media consumption.

While the author was visiting the website Der Spiegel (DE), 35 trackers alone were "advertisement", 5 belonged to the category "website analytics". Also apps on mobile phones relate to third parties.

This (bigger) part of the collected data would serve as a "proprietary behavioural surplus" (owned by the service provider, therefore proprietary), and as raw material to predict behaviour and control citizens, users, customers, and employees. Therefore, other services (legally: third parties), might demand the different raw materials or semi-raw information, for instance in order to place more efficient advertisements or to improve their rating algorithms or their content.

The anti-virus software provider, Avast, is a pretty brazen illustration of such practice. While offering their popular software for free, the connected company, Jumpshot, sold the personal browser data of their circa 435 million clients to third parties since 2013. In other words: The software spied on and recorded their users. Although anonymised by an ID, it is quite easy to attach the data again to concrete users (Eikenberg, 2020). Customers were, among others, Microsoft, Google, Yelp and TripAdvisor. In light of such facts, we might ask – what was the income model behind Avast software? The anti-virus software package or user tracking?

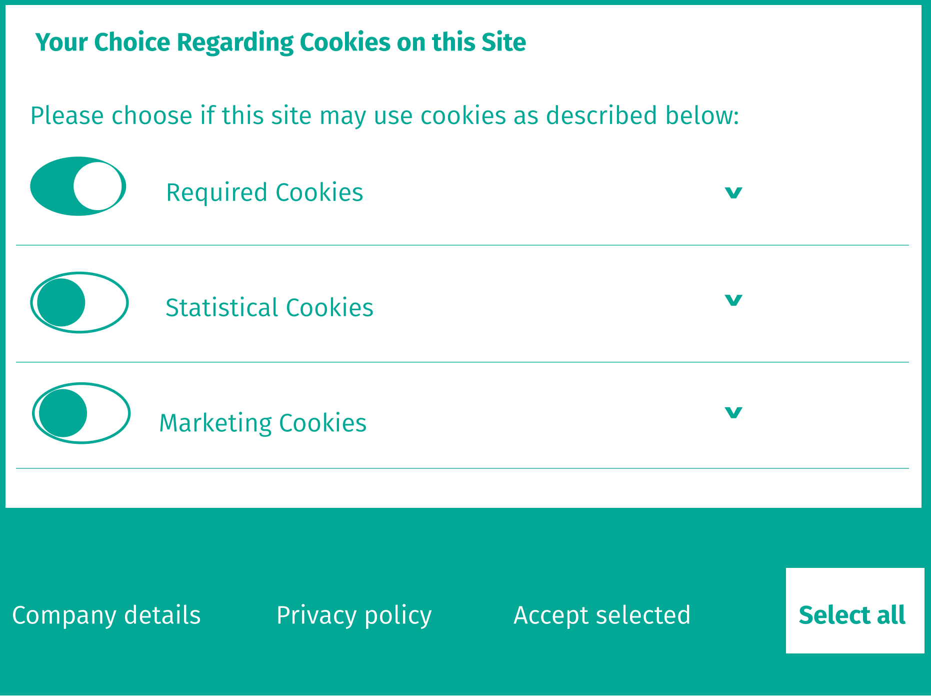
By merging different data via such a (for the users) invisible market, they are producing massively new data and designing overly complex analysis and prediction models. Aiming to always collect fresh data, in consequence, data capitalism would generate and use instrumental power and disseminate its logic into society.

Supported by techniques from the methodology of behavioural psychology (like implementing gamification elements or undertaking social experiments with their users, nudging, or reframing), the behaviour of people would be directly influenced. In effect, the surveillance capitalism is giving birth to a new total power, the "instrumentarianism" (Zuboff, 2018, p. 376), merging (psychological) behaviouralism, (economic) capitalism, and (technical) ubiquitous machines.

Very visible are manipulative user interface designs to make people consent to their sharing of data or buying things, so called *dark patterns* (https://darkpatterns.org). A common example is that the button for giving consent to third-party cookies is more colourful than the button for the minimal settings. Other examples are trying to make people click on supplements or installing unnecessary software. Also known are warnings with messages like 'only a few offerings for that price left'.

Legal Dark Pattern:

Although Privacy by design is default (conform with the GDPR), users are triggered to “Select all” thus also activating marketing and statistical cookies.



Your Choice Regarding Cookies on this Site

Please choose if this site may use cookies as described below:

- Required Cookies
- Statistical Cookies
- Marketing Cookies

While Zuboff emphasizes the new configuration, Nick Couldry and Ulises A. Mejias (2019, p. 4) use the term data colonialism to point out historical analogies. In doing so, they draw a connection to the global dimension and asymmetries in the age of big data, for example when enterprises or countries force people to contribute to their databases (for instance under the roof of development aid or Public Private Partnerships): “While the modes, intensities, scales and contexts of dispossession have changed, the underlying drive of today’s data processes remains the same: to acquire ‘territory’ and resources from which economic value can be extracted” (Couldry &Mejias, 2019, p. 3).

The text above describes how a growing number of businesses aspire to commodify and resell personal data in order to develop products and tools for behavioural prediction and control. The experience of datafication shapes perspectives, how people look at privacy or autonomy. Some groups are, in consequence, discussing under the headline, Post Privacy, if privacy in the digital age is generally possible or if it should be treated further as relevant.

However, the majority of experts and activists come to a different conclusion. A representative for digital activism across Europe, Jan Penfrat, from the network European Digital Rights (EDRi) says:

> **“Digital rights are digital Human Rights, they are whether another category of rights, nor something relevant only for the industry.“**
>
> European Digital Rights EDRi

If privacy and integrity of the body are fundamental rights, it is not simply possible to suspend these in a kind of capitulation toward reality. Rather it would mean undertaking considerable efforts of the legal and ethical regimes to put rights back on the map.

Challenges for Effective Regulation of Privacy

- The massive extent of state interception became visible with Edward Snowden’s whistleblowing in regard to the NSA and its allies. [Guardian, 2013].
- Data extraction through apps and services “for free” is usual practice and seems to replace payment models.
- Privacy protection is not understood as a concept and concrete right.
- The acceptance for quantification is increasing and people are welcoming their (partial and limited) involvement in big data processes.

Market Regulation

Connected with the collection of personal data and body data, one guiding question is tackling the topic of ownership and property: Despite belonging to myself, am I the owner of the data? Is personal data a marketable good? And if personal data is marketable — who would have the power to decide on its stipulation and might delete, share, change, or select the license conditions? The author and lawyer, Juli Zeh, (who used her book, The Method, to draw a concisely elaborated picture of a data-driven and just social order) also emphasizes the importance of equal treatment of the data body and its consequent integration into the idea of autonomy: "In the core, the digital identity would need a comparable protection level like physical integrity or the inviolability of private property" (Zeh, 2014)

Theoretically, "markets for personal data would need to rely on legal frameworks that establish alienability, rivalry, and excludability for personal data, and assign initial ownership to an entity such as the data subject" (Spiekermann-Hoff et al., 2015). However, the extractive platform businesses prefer not to negotiate with their users on an eye-level, nor are they seeking alternative income models in their future. Their strategies seem rather to connect the public interest with their profit interest and to generate public-private, win-win partnerships, based on data-intensive computing.

In the interest of the public far beyond the already well known security interest and in order to make access to analytical data easier, lobby groups, governments and think tanks (like the German Council for Ethics) are exploring possibilities for how the legal privacy level might be lowered. In partial compensation they see the need to increase the transparency level for shared data and their authorized commodification. In Germany this was discussed under the tag personal data sovereignty (Datensouveränität; which is not "data sovereignty" as the latter describes that data falls under the law of the territory where it is stored). In this way an opportunity would open "on the basis of personal preferences to intervene in the stream of personally relevant data"(Deutscher Ethikrat, 2018, p. 31ff). It is a crucial question: what kind of limitations for data extraction might efficiently be set, if such new opportunities are paid by lowering the legally granted personal privacy level? Strong voices in governments, science and business are unified in support of this initiative as they all would gain by such softening of privacy.

But would the citizens? The General Data Protection Regulation offers a comprehensive set of rights to citizens (EP, EC Regulation 2016/679). The future will show if this is a basis for effective regulation of (transnational) data capitalism. Also, in regard to state surveillance, there is reason for optimism. While in the 80s in the Soviet Union people went around the omnipresent surveillance state by meeting in their legendary private kitchens, today more surveillance leads to digital kitchens, private islands in the internet. Privacy-friendly, decentralized technology for connecting and communicating is becoming more attractive and in fact, we are observing also a race-to-the-top in regard to privacy standards. For instance, the WhatsApp messenger uses the security technology originally developed for Signal. The consumer-driven demand for open source and alternative operating systems is also increasing. Since citizens express their demands by using discrete tools, this will probably stimulate their development.

Does the existence of a market for personal data, or like Zuboff puts it, a market for behavioural futures contracts follow Human Rights principles and is it in the interest of democracy? Is our interest as society in this market higher than the interest in privacy? To what extent are we as a society tolerant of the market's effect on our privacy? On the basis of these answers, effective regulation needs to be enacted and enforced.

General Data Protection Regulation (GDPR)

The regulation is the central element of the EU data protection law. As a directive it is superordinate to the national legislation. More here: https://data.europa.eu/eli/reg/2016/679/oj In regard to the processing and storage of personal data, it enforces the following principles:

Lawfulness, fairness and transparency:

Processing needs consent or a ground provided in the GDPR. Furthermore, data subjects need to understand what is happening with their personal data and be informed about how and for what purpose it is stored and processed.

Purpose limitation:

If the purpose of processing is specific and clear, individuals know what to expect. The processing of personal data for undefined and/or unlimited purposes is thus unlawful.

Data minimization:

Allowed is the processing of what is necessary to fulfil a legitimate purpose, not more.

Accuracy:

data must be kept up to date and accurate

Storage limitation:

Personal data must be deleted or anonymised as soon as they are no longer needed for the purpose of collection.

Integrity and confidentiality:

High quality security measures have to be made by the data collector and processor. This includes servers and technical infrastructure and also methods like pseudonymization.

Handbook on European data protection law

Published by FRA – European Union Agency for Fundamental Rights. Detailed explanation to the legal basis of data protection, with explanation of cases and context of the GDPR. https://doi.org/10.2811/58814.
Free download or order of a hardcopy at the Publications Office of the EU.

Conclusions for Education

The function of the private space in a democracy: Digital human rights often circulate around privacy and data protection, since the private sphere is recognized as the citizens' safe space. Its existence is a fundamental condition for free expression and self-organization. Therefore, democratic pluralist public spaces rely on the existence of privacy, or as the former German president Theodor Heuss put it: "The outer freedom of the many is dependent on the inner freedom of the individual." Education needs to emphasize the relatedness of a democratic, pluralist public and the private freedom of the citizens.

Integrity/safety: Human Rights Education and Education for Active Citizenship need to facilitate knowledge about the technological threats to privacy and also about the related rights of European citizens. This involves privacy in the narrow sense and also the complementary rights, like access to the digital sphere, ownership of data, or free choice. In particular, we might ask, how processing in the frame of big data can get along with fundamental rights? A deeper exploration of the GDPR seems to be a good starting point for adult education.

Informed consent: A central issue that needs more awareness is the concept of informed decision-making. Although, if citizens are often voluntarily not claiming their rights, there needs to always be an opportunity to revisit such decisions. In a lot of cases, informed consent is not possible or fails. Very often, consent is superficial, rather a formal consent expressed by a fast click on cryptic terms of service or privacy agreements. Education might bring light to this cryptic process.

Informed choice: Beyond consent, this is a question of good choice. People need to assess the pros and cons of a certain service or device in regard to private data. Alternative options must be known and must be available for use. Also, educational institutions can be a role model with their informed decisions regarding digital infrastructures and platforms.

Regaining control: Once data is stored, analysed and shared, how can users then learn about their data traces? Where and how are they stored and for what purposes? What would make people factually exert control over their personal information is also related? In particular, how might they control the shadow texts and data traces? Education on privacy intersects with big-data-literacy.

Interplay of protection, regulation and governance: Last but not least, we need to instigate debate on data and privacy protection, algorithmic regulation, data process governance in particular in the context of a market as an explicit political learning.

2. Mentally Controlled by Data?

Although people compare and measure each other and themselves, for instance to extend their abilities or to grow, it seems that the space where they practice this measuring and competition was, in the past, a space, where the majority of people were just temporary guests. After doing a physical workout people sat together, drinking and smoking and therefore giving evidence that anarchy and sociability are of equal importance for the human balance as order and competition. Critics argue, the ongoing presence of optimization and rating, the permanent availability of performance data and the present (mainstream) images of bodies on the internet might lead to a silent "dashboardification" and subordination under dominant beauty and body ideals. Critics argue that the society as a whole might now internalize these norms too much.

The Quantified Self

Quantified self describes the acceptance of quantification tools by individuals. The term describes according to Meidert & Scheermesser "a person actively measuring oneself with apps and devices in order to generate knowledge through the analysis contributing to optimizing lifestyle and behaviour in the fields fitness, wellness, or health" (Meidert et al., 2018, p. 44). To what extent do people accept this?

Quantified Self:
A person, actively measuring and tracking oneself in order to generate knowledge through the analysis of personal data, often performance data.
Self-tracking: Individual usage of tracking tools and analysis of their data output.

Otherization:
Perceiving a human identity only through its measurable data.

Othering:
Excluding individuals from a group or the society as fully equal.

According to a study based on empirical research from Switzerland, healthy people are particularly driven by curiosity.

Example Switzerland: Quantified Self

Quantified self support people in their body perception (42%) and help to observe it (27%). Therefore, it would open an opportunity to a better life (30%).

On the other hand, many have privacy concerns (31%), assess quantified self-practice as negative resulting in undermining the natural competence for self-observation (21%) and/or criticize the non-exact measurement and consider it a gimmick (24%).

Less healthy people, however, are more reserved. They use measuring generally when they have to, whether for prevention, for preparing a consultation or because they are sick. In particular amid unhealthy people, there are growing concerns. From their interviews, researchers conclude, "there is a general fear to be in the future discriminated or disadvantaged for lifestyle choices" (ibid., p. 84).

In general people are measuring: steps (63%), weight (26%), pulse (26%), calories (26%), menstruation (23%), sleep (21%), stairs (15%), other parameters (15%), and blood pressure (9%) (p. 81). Mainly, they use their smartphones with an app (62%), conventional devices (26%), activity trackers (25%), and smart watches (17%) (ibid., p. 84).

It seems to be empirically proven that there would be an upward-oriented and a performance-oriented milieu of "many trackers" for whom the body as a symbolic capital plays an important role. Therefore, quantification is a practice enabling them to achieve this.

However, most people seem to have a mixed attitude toward the new digital tools mixed with pragmatism, criticism, fear of addiction, or compulsion for autonomy. The vast majority seem to be aware of the risk of losing social and cultural variety in light of excessive quantified self-practice. We might assume a general scoring scepticism as soon as they feel constrained by behavioural expectations in a system of social scoring or "bossed around" by some external pressure.

It is also a fact that thanks to digitalisation and the authority of algorithms, norms are easier to roll out for markets or state or influential social groups. Although the idea of norming and sorting people is not a new one, their increasing presence makes them more "normal". The personality models underlying a lot of the algorithms (like the Big Five personality inventory) have been used for decades to quantify and assess employees, not for the purpose of shaping the working environment according to their needs but for forecasting their performance and learning about their usefulness. Very quickly therapeutic insights like this and other research from behavioural psychology were exploited and, in that way, commodified. The tests and control routines were perfected. Under this perspective, digitalisation is not contributing to new perspectives but lowering the costs and enabling more actors to use these approaches on a larger and broader scale for self-tracking or lifelogging (Selke). Cambridge Analytica used the Big-Five test for the purpose of consumer manipulation, not constructing a new inventory.

Skeptics say, habituation, obedience under the utilitarian dogma of modern capitalist organization and the norming power of technology inspired by psychological insights could lead to a *digital alienation*, in a too-rational view of oneself and fellow citizens. The sociologist, Stefan Selke, calls this "the shift of the idea of man toward a human defective or susceptible to faults" (Selke, 2016, p. 11).

Zuboff sees here an implicit need for big data, promoting tools and instruments for quantification, because its income models would rely on the harvesting of behavioural surplus for behavioural prediction. She uses the word "big other" in order to describe a threat of de-individualization or otherisation. Believing in behaviourism, that human behaviour might and should become predictable or objectified, data analytics would randomize individuals and reduce them to "organisms that behave" (Zuboff, 2018, p. 377). In consequence, such *"instrumentarianism"* would decompose people's individuality and natural groups and "otherise" them in an invisible way, "shaped in secret, camouflaged by technology and technical complexity, and obfuscated by endearing rhetoric" (Zuboff, 2018, p. 360).

On the other hand, tracking and analysis can also be seen as a helpful tool in a complex, liquid modernity. They are a promise of regaining individual control and *instigating self-efficacy*. In particular when it is undertaken on one's own initiative and embedded in a self-reflective way, this might lead to satisfaction and autonomy (Selke, 2016, p. 316ff.). Despite all criticism, the reasons that people are using such tools is understandable – a little bit more control here is perhaps compensating a laissez-faire approach somewhere else. However, Selke describes the challenges connected to self-induced quantification.

First, people need analytical competence. They follow quite often the illusion that qualitative experience might be transferred simply to quantified data. Although one will receive data at the end, the results and conclusions might be wrong as the data is not fitting to the individual question. Much better ways of interpretation of one's own behaviour would be pushed aside because no quantitative dataset is available for measuring them.

Second, the human ambition to "transform the body to a lifestyle product and a temple" is, under the new conditions of digital capitalism, capitalizing the body in order to gain social distinction (Selke, 2016). Fourcade and Healy expect people to "accrue 'übercapital', a form of capital arising from one's position and trajectory according to various scoring, grading and ranking methods" (Fourcade & Healy, 2017, p.).

Impact on Health

The existing control optimization and evaluation mechanisms around us are impacting our self-perception. The Internet, and in particular social networks, are trying to exceed behavioural control, for instance by amplifying existing norms and enabling extremes to become more visible, very often extreme ideals of the body and of beauty. The discussions about overly skinny models and about photoshopping were already starting before Instagram. Today, it's not only a small group of privileged gatekeepers discussing and imposing their body image on us but millions of multipliers co-creating the imagination of beauty, amplified by algorithms triggering emotions.

A study about the body weight of Italian women points out that "normality" as a statistical spectre is not similar to an ethical "norm". Their interviews show "that girls and young women wish to be thinner, which leads them to neglect healthy behaviours. They prioritize social acceptance rather than their own wellness and lifestyle quality" (Di Giacomo et al., 2018). Social media amplifies such outcomes, although one needs to concede that it has also supported the emergence of counter trends such as #BodyPositivity (a hashtag used by people not wanting to subordinate to the dominant beauty trend). Each social media platform seems to have a different impact. For example, the Royal Society for Public Health established that YouTube appears to be less normative in their promotion of body images than Instagram (Royal Society for Public Health, 2017).

Obviously, these tendencies also have a socio-political impact. In particular, age groups in the population in which people wish to fit into certain beauty and body norms are affected more than those who have a less careful eye on their body and body image. A body compliant with norms serves the inclusion in a group. Distinction and segregation often take place through the body, it is not only a social practice on the basis of intellectual abilities. If extreme perceptions of thinness and physical fitness are becoming the norm, this would influence our inclusion and exclusion mechanisms – who is "in" and in particular who is "out". Therefore, the

Cyber-bullying:
Bullying on social media, messaging platforms, gaming platforms and mobile phones, aimed at scaring, angering or shaming those who are targeted.
(UNESCO #ENDviolence campaign)

Internet Addiction:
Compulsory use of internet in a way that interferes with normal living, and causes impairment, distress, and stress on close people.
(Brey, Gauttier, Milam, 2019, p. 19)

society relies on the existence of a realistic picture of the body, not only due to reasons related to health policy. At the core this is about information freedom and everyday ideas of pluralism and diversity.

In particular, micro-targeting causes a loss of knowledge about diverse body images. This term describes the presentation of content in social media in a non-linear way, targeted for specific user groups and arranged by algorithms. What you see in your timeline is not what others will get. Although this practice is publicly more discussed under the aspect of political disinformation, it has a huge impact on the perception of beauty and bodies. While micro-targeting enables users to act more intuitively, limiting efforts to select relevant content and contacts and to receive information addressed more specifically to them, it is questionable, because usually they will neither influence nor control these algorithms. If not obviously relevant knowledge and experience is more and more efficiently excluded, this will affect the ability or competence of the citizens to understand society, the difference between a tailored and presented narrative and the plurality of all existing narratives.

In regard to the body, this would impact the ability to perceive the broad diversity of body images and the variety of existing groups. Pluralism relies on diversity of other people with different backgrounds and appearances, but the construction of social networks is making this challenge harder, because they were not developed in order to inform people in a comprehensive way but to build communities. "The rational discourse is not the purpose of social media", but of emotionally driven mobilization (Suarez, 2017, p. 158).

Discrimination mainly happens on the basis of physical attributions such as skin colour, sex/gender, physical (dis)ability, age, sexual orientation or other characteristics. If somebody would like to discriminate and exclude people from the public, they would make use of this technology and exclude "abnormal" bodies from our perception or emotionalize the "wrongness" of their appearance, so that we do not face overweight, people with different skin colours. Also, offensive actions toward vulnerable groups or individuals like cyber-bullying might be amplified by mechanisms of social media.

Certainly addiction also needs to be mentioned as another health-related aspect. General internet use, gambling addiction and (online) gaming can cause addiction (Lopez-Fernandez & Kuss, 2019). The focus of awareness here is mostly on youth and adolescents (p. 41).

Addiction often results from a combination of different factors, like online gaming addiction illustrates. In particular, factors such as the specific game type (especially role-playing games), social aspects (relations) age and gender (young male) and co-morbidities or psychological dispositions (for instance weak control) correlate with addictive behaviours (p. 47). Gambling disorder shares some features with gaming addiction, but "higher harm avoidance and reward dependent traits than normative groups" would come into play (p. 49).

The authors describe specific amplifiers in the internet. Users "experience multiple layers of compounding reward and reinforcement loops", the engagement in online applications would create "habitual behaviour patterns" and the reward experienced "is intensified when combined with stimulating content" (p. 12).

When addictive, technology lets us search for rewards, transforming our habit and exposing us to harder emotional and affecting content, we might draw conclusions for the design of apps and platforms which would lower the risk of addiction.

Especially amplifying algorithms (preferring emotional instead informational content), gamification (including stimulation and reward systems from gaming), dark patterns (manipulating our inbuilt control mechanisms) and the instrumental aim behind the platforms and apps (binding users deeply and over time instead of empowering them to a reflective usage) can be identified as problematic key factors. Mozilla Foundation's "Internet Health Report" concludes: "Smartphone apps and social media are often also explicitly designed to optimize engagement, like comments and shares, and to increase the amount of time we spend, watching, reading, scrolling or playing" (Mozilla Foundation, 2019, p. 94).

Promoting Conformism?

Bertolt Meyer outlined before that devices and tools lower barriers and increase opportunities for participation. But there is also a potential threat. What if prosthesis in the case of people with disabilities but also wearables for working activities would become an implicit obligation? In the working space, we already experience the use of norming technology. Then one might question to what extent nonconformist behaviour is actually possible. The extreme is a scenario illustrated by the Chinese social scoring system, where the definition of what should be normal is less and less dependent on the citizens: "Mathematization of the social norming practices are becoming easier (because measurable) and less contestable. For instance, in China's social credit system a score between 550 to 600 is perceived as 'normal'" (Lobe, 2019, p. 180). Although China's approach is an extreme example, the logic of social scoring could lead to a system of seemingly rational perfection and (non-transparent) moral control elsewhere too. The aggregated data is extracted from behaviour, and behaviour is assumed to arise from a moral intention or decision. "With access to our most intimate and unconscious behaviour, new digital tools make a new economy of moral judgement possible" (Fourcade & Healy, 2017, p. 24).

In 2019, it became evident that the Chinese government was treating the smartphones of members of the Uighur minority like electronic tags. Even their non-usage might spawn consequences. So the possibility of becoming deported to one of the reeducation prisons would increase if the frequency of turning off the phone seemed to be extraordinarily high. Another extreme case is the new model of insurance contracts, which are experimenting by nudging people to track themselves by offering lower fees. Data helps insurance companies to analyse risks faster, for instance if social habits change (e.g. when people shift at different places in a country from individual car ownership toward shared mobility), "so the customer is always under control" (Garriga, 2019).

As for now, the moral fundament of our social contract is shaped openly, allowing for exceptions and discrepancies. There still seems to be broad consensus that life quality is to develop our talent for rational thinking where we would include quantification, and simultaneously, to feel free from the obligation to always use a rational approach. In this sense, people acknowledge "that zones of non-transparency are important for the personality and that life is not mainly about being perfect" (Selke, 2016, p. 335). Second, life is a non-linear process of growth, learning and socializing and our world is too complex for its quantification. The third, is the most fundamentally related to social life. In line with Arendt's findings in the The Human Condition, one neither sees the deeper destination of humanity in the utilitarian "labour" nor in the result-oriented "work", but in "action" or "engagement", which is understood as a more pro-social, non-utilitarian, open-ended, cooperative activity free from monetisation (Arendt, 1958).

Impact on Abilities and Competences

With the broad availability of television in the 70s and home computers during the 80s, the new popularity of consoles and online games during the last twenty years, several questions became relevant: Does the computer affect our mental abilities in a negative way? Is it a cause of addiction and does it harm people's sociability?

According to gaming, scientific judgments are sometimes contradictory or present themselves in a contradictory way. On the one hand the continued play of World of Warcraft seems to harm the development of the dorsolateral prefrontal cortex and of the left orbitofrontal cortex. The results are reduced conscientiousness and emotional blunting (Zhou et al., 2019). Others have examined the changes induced by playing Super Mario. They conclude more positively: The right hippocampus, the right dorsolateral prefrontal cortex (DLPFC) and the bilateral cerebellum grew. Connected to this growth, also the ability to think spatially, joy of playing and allocentric navigation grew (Kühn et al., 2014). Is it too banal to ask if back and brain have something in common? Manifold activities strengthen the back muscles, but monotonous stone crushing might damage it.

It is no question that new media and technology have an impact on the brain and also on the physical abilities of our children. "But that applies to books and any other form of learning and experiencing too" (Reinberger, 2017, p. 3). There is evidence that internet usage has an impact on the ability to think analytically and leads one to focus on where to find content rather than on acquiring the content's meaning (Brey et al., 2019, p. 23). On the other hand, the opportunity to access a variety of content can lead to improved information-related skills and enable cognitive learning (p. 24). This seems to be the case for the elderly in particular.

Also information management as a competence is becoming more necessary for broader groups of the population. Today it has become integrated in a lot of concepts for digital media competence. In particular, it aims to tackle information overload – having too much information which prevents a person from making decisions and feeling overwhelmed. Strategies to cope with overload are information withdrawal (minimizing sources), avoidance of information or satisficing (deciding when one has enough information) (Brey et al., 2019, p. 28).

The ability to deal with the different "presences", the social roles one fills, is becoming crucial in the information society. Their continuous online presence leaves people limited space to separate these sometimes even contradictory appearances (for example separating private from professional habits) (p. 33).

Furthermore, a word should be raised in regard to the dichotomy of digital and social relations. "In the end, it appears that there is some evidence for the replacement of offline by online social relationships, although the jury is still out on how worrisome this is for the quality of social relationships" (p. 36).

When comparing online relations with traditionally built relations in the community the question is raised over what form the specific social media facilitated relations take. Therefore, we would need to compare deeper online relations with deeper offline relations to reflect on to what extent the ability of individuals to build relationships and maintain them is increasing or decreasing. For instance, families seem to adopt social networks and messengers broadly and therefore strengthen their ties online and offline. The existing social web seems to stimulate the involved persons also to acquire the necessary digital competence for using these tools, which is from a pedagogical point of view remarkable, since the elderly are too often perceived as technically incompetent. However, the internet seems to also degrade relationships, leading to loneliness compensated by online facilitated social relation of ambiguous quality (p. 38).

It seems to be crucial to look at abilities not from the technology but also from their purpose and from the concrete activity. “Dumb” tasks like redrawing lines on printed templates are in digital and in analogue education less challenging than drawing free lines (Reinberger, 2017, p. 5). If this appears to be true, how many dendrites were killed by Solitaire but also by monotonous app-swiping which are not really seen as threats?

In this sense, apps and tools need to be designed in a way that makes neuronal development, relationship building, critical thinking and learning more feasible or they need to be embedded in rich learning processes. By discussing digital tools from this perspective, it could help us to reflect on analogue experiences in learning and education. In particular in adult education and intermediary work, too often formal settings like lecture, panel discussions and conferences seem more aimed at serving the status quo than stimulating creativity, whether provided in Zoom or in the traditional style of a conference centre.

Conclusions for Education

Self-optimization: People are seeking the balance between self-optimization and critical reflection of the implicit norms of the quantified self. Education might encourage them to find their balance. Furthermore, critical citizens are those critically assessing the normative systems behind these practices and deciding to what extent they want to follow them. Education might also help to make alternatives visible.

Body uniqueness and diversity: Pluralism is also the diversity of appearances, bodies and beauty ideals. Educators need to address these, similar to how they would address opinion pluralism. Furthermore, education can also encourage people to showcase their own uniqueness:
#BodyDiversity.

Addiction: Addiction to general internet use, gaming and gambling online are often seen as a specific youth problem, but need to be tackled also in adult education. Gamification, dark patterns or amplification of emotions through platform mechanisms pander to addictive behaviour of those people with addictive predispositions or vulnerable groups (in particular young people). Education might help learners to reflect on these mechanisms and strengthen their ability to cope with their digital omnipresence.

Normal is not uniform: Educational settings in adult education are an important opportunity where people beyond their jobs and private lives might meet with people from other communities and backgrounds, where they might get in touch with social diversity at eye-level. An important requirement for resilient democratic spaces of the future is a critical mass of adult citizens appreciating diversity and eager to learn how to deal with more individuality and a broader spectrum of normality.

Control of identity and information: Dealing with different presences, like playing and showing private roles or professional appearances also toward different audiences becomes a challenge, since the spheres become ubiquitously interlinked. The need for supporting learners in building information management competence is growing, which is not a new field for adult educators but becoming more relevant for an increasing number of people in a variety of contexts.

Social relation competence: A remarkable part of today’s internet is built around social relations, and also analogue and digitally facilitated relation-building are intersecting more and more. Thus, relationship competencies gain in importance, understood as a reflective assessment of ones position in the network of social relations and also the individual ability to create and maintain relations in the online and analogue world. As a result, this becomes an explicit topic for adult education whereas it was formerly sought more implicitly.

Digital tools in pedagogical settings: The useful and problematic aspects of digital tools are evident in the context of learning. From this perspective, any tool would potentially make sense, even location tracking, smart watches or other tools which we discussed critically before, could have a pedagogical potential. For example, geocaching (as provided by the portals belonging to the non-commercial Opencaching Network like https:// www.opencaching.us) would be an interesting pedagogical use case although geocaching apps do track location data of learners.

In general, the potential of digital tools is unleashed when they are embedded in rich holistic learning processes, where competencies of the learners are mobilized. This can be a digital or analogue learning environment. In particular, blended learning designs make use of the potentials of both domains, the advantages of the analogue and the digital.

Ethical and legal aspects: The Human Rights perspective must take the ethical and legal aspects, such as privacy and sharing data with third parties, into consideration. Since there are always alternatives to tools that must be assessed as critical, often the question is not what kind of tool would make sense to use, but rather what specific tool will be selected by the educators.

3. Our Creepy Lines

In general, technology and their producers are perceived widely as competent authorities. Even if serious breaches of the law and security problems appear, this does not necessarily lead to a questioning of their authority. Around 350,000 clients of one big producer of cardiac pacemakers needed to get an update in 2017 (US-FDA, 2017/08/29) and yet no one remembers this in 2020, even those with a cardiac pacemaker, and thus directly impacted. I highlight this example because it illustrates that our concerns are not always related to the risks. The reason is trust. Instead of broad panic, the public seems to trust the producers of special devices and health institutions implanting and monitoring them. Why are they more trustworthy than others? One partial answer is that humans do not act rationally in the definition of a rationalist idea of man. One characteristic of trust is confidence and belief in the good intentions of the people and institutions we trust. This allows us to reduce complexity and not to run away scared when potential risks emerge.

An experiment of the Georgia Institute for Technology highlights this. They developed an Emergency Evacuation Robot aimed to guide students out of their dorms in case of emergencies. Sometimes it led them on the correct path and sometimes on a strange route out of the building. The latter case – for instance, if the robot was driving past the emergency exit – did not generally lead to distrust or disobedience of the students: "Eighty-one percent of participants indicated that their decision to follow the robot meant they trusted the robot" (Robinette et al., 2016, p. 4). They followed the machine because it had a good purpose inscribed: "many participants wrote that they followed the robot specifically because it stated it was an emergency guide robot on its sign" (Robinette et al., 2016). One might add, certainly it is not only about the purpose but also about the institutions pretending to follow the purpose and hereby warranting the robot's trustworthiness. A study of the EU's Fundamental Rights Agency has shown that a majority of people feel comfortable or very comfortable with biometric surveillance technology in public spaces for the purpose of security. The motivations behind that trust were that "they use the technology ethically" and that the result was increased security (EU-FRA, 2019). Police forces are still trusted institutions in Europe. However, children seem to trust adults more than the internet (Basu, 2019; Lovato et al., 2019; Wang et al., 2019).

In times where people don't know if they should marvel at digitalisation or be scared of it, this must be perceived also as a relevant product design decision. Eric Schmidt (Google) used the term creepy line to explain how big data platforms and IT companies respond to the danger that people could consider them as going too far.: "Google policy about a lot of these things is to get right up to the creepy line but not cross it. Implanting things in your brain is beyond the creepy line. At least for the moment until the technology gets better" (Schmidt, 2010).

Eric Schmidt represents here a management perspective on aspects related to the digital self. He understands the concept of a creepy line not as an ethical problem, rather as one of habituation. This perspective is obviously fundamentally different to the majority of people which are on one hand fascinated from the opportunities technology opens up, but on the other hand constantly concerned about its impact on their digital self.

Beyond *curiosity*, people also inherit a *critical attitude* that might shift to *anthropomorphism phobia*, a fear of technology becoming too human-like or of the human becoming too technology-like. Humans would humanize machines as long as it is clear that they are only machines (van Mensvoort, 2017, p. 175ff.). But what is perceived as 'too human-like' is subject to habituation. The author, Koert van Mensvoort, purported that our fears might be used constructively if we registered them more consciously. On the one hand, we should try to prevent anthropomorphism phobia by eliminating its rationale. On the other hand, it might be a guideline or indicator for how much technology people find acceptable or comfortable in a given context.

What are our Creepy Lines?

Our fears in regard to new developments – are a natural reminder not to go too far not to cross our *creepy line*. In this sense, they are helpful signals inducing us to reflect our needs and goals.

On the other hand, critical thinking involves a reflection of these concerns and fears and their intellectual foundation.

What is acceptable? What is beyond the creepy line?

- Monitoring of the private space
- Processing of private data and sharing it with third state or other third parties
- Data analysis on the basis of individual profiles
- Non-invasive human-machine interaction
- Implants, prothesis
- Performance tracking through others (employer, partner, doctor, ...)

A Gender Perspective on IT

Why do Google, Apple and Microsoft choose female names and voices?
Female voices are often considered as peaceful instead of threatening and assisting instead of directing. For this reason, personal digital assistants and other services that work with generic voices have female attributes.

What do the concrete devices say about women?

How does their appearance and behaviour replicate gender stereotypes?

What would change if we were to talk to Sirius, Alex or D. Vice?

In particular, when we consider technology at the interface of thinking, concerns about technology's ability to think is the creepy line for many people. The brain seems to hold a specific meaning for the individuality of people. *Cogito, ergo sum*. Brain pacemakers are so far tolerated as they serve therapeutic purposes and enable people to participate. They would be less accepted if they served other purposes like learning or the "programming" of people's brains. We must remember the ethically questionable and dangerous experiments from the 1950s where electricity and lobotomies were used in order to delete criminal dispositions or to "reprogram" homosexual people. Similar skepticism is growing in regard to the tracking and analysis of feelings and emotions, because we are convinced that the key features which distinguish humans from machines are the ability and right to think independently, and they might feel free if they are allowed to feel freely.

An interesting aspect of digitalisation according to Schmidt's dogma is that exactly the most common "intelligent" or "smart" devices in our surroundings are trying not to evoke associations with humanoids or robots. Amazon's assistant Alexa and Apple's Siri were consciously named inline with this idea. Loidean and Adams pointed out the problematic choices of the digital assistants' designers in regard to the representation of female – serving and helpful with mystical names – in consequence perpetuating discriminating gender images: "These communications are delivered by witty and flirtatious characters revealed through programmed responses to even the most perverse questions" (Loidean & Adams, 2019, p. 2).

Seeking the Balance

Although in the past humans were also very ambitious to find ways to measure, compete with each other, and confine themselves to social groups with similar attributes, they were simultaneously sensible enough not to overestimate their meaning. What we describe as scepticism might as well be seen as a search for balance – in the sense of an individual risk assessment in regard to digitalisation.

One way to achieve this balance is promoted by the supporters of the concept *digital detox*. They try to de-digitize their course of life. In contrast to the idea of quantified self, its proponents see purpose in the redundant and qualitative “analogue” experience. Similar to how an analogue vinyl record includes a whole spectrum of useful and non-useful (because not perceivable) sound information, they hope that analogue life would bring a richer experiential spectrum back. Translating the vinyl experience into the social sphere, the added quality to life is more sociability by more personal encounter – more surprise, emotion and sensitivity.

Most people would rather try finding a *mixed* approach. At the end, an important skill in the frame of technological competence is neither to immediately fall into panic, nor to use quantification tools uncritically. Many of the tools and instruments presented at https://quantifiedself.com/ might also be interesting for occasional self-reflection for those that don’t share the whole ideology of the quantified self movement.

TWO CONTRARY POSITIONS

Quantified Self	**Small Data**
“The Quantified Self is an international community of users and makers of self-tracking tools who share an interest in “self-knowledge through numbers”. If you are tracking for any reason — to answer a health question, achieve a goal, explore an idea, or simply because you are curious — you can find help and support”.	“The limitations of the digital are qualitative. Digital is not able to deliver things like physical places, haptics and the things emerging in and by analogue like effects of surprise, aha-moments or thought-flashes. Dazzling new insights evolve seldom from linear planning. It requires space for disorder and the imperfect”.
“Quantified Self supports every person‘s right and ability to learn from their own data”. Offering Tools and Advice on how to track, analyse and gather data. https://quantifiedself.com/change passwords or set new accounts. .	“Like eco has been a response to industrial food mass production […] analogue might be one answer on industrial data mass production and processing and as well affect their development. In short, analogue is non-connected and the opposite of connecting big amounts of data, of big data. One could say it’s small data”. Andre Wilkens (Wilkens, 2015)

In fact, we are part of a fluid process of negotiation of norms and values in regard to information technology. By applying new technology, our priorities shift. Although we might not be in favour of tracking and measuring, it might still be interesting for many to explore such tools. Even critical citizens who feel that our way of reading and communicating is shifting and that don't like some of the aspects of digital communication (like the 'always available' expectation, cut-off sense of short messages, or being pushed to immediate reaction) are making peace with smartphones. And beyond the individual perspective we should also consider that digital transformation is driven by markets and powers. They challenge our assumptions of what is right, normal and healthy and are influencing our public discourse on such issues.

More common to Europeans than being pushed by authorities is voluntary appropriation and subordination. This might be illustrated by the ever present rating systems of platforms. It would be too naive to simply ban rating systems as long as they seem to fill a transparency gap for many of their users which older feedback or information systems left out. But we also know that a more conscious reflection of this new practice might be appropriate.

At Airbnb, not only the providers of places to stay, but also their clients, are rated. Whether intended or not, the rating becomes normatively relevant as a conflict between the parties is no longer an issue in their two-party relationship, but also one that would affect either of their future social possibilities. Is a 4 out of 5-star evaluation OK or a problem? Usually one does not know the outcome but will assume that it could become an issue. In response, people are identifying different ways to deal with this challenge. Most probably many of them seek to avoid provoking serious consequences for them or the other involved party and find a silent agreement – a kind rating. Others, however, might try to reject the mechanism and not rate at all. A third category of people might try to seek advantage and put pressure on the partner. For all involved, there is also the fact that ongoing rating practice will accustom us to quantified evaluation of other people and also to the norms set by the platforms, if the latter face no impactful legal or moral limitations.

The democratic discourse's and policy's role hereby is to ensure that the implicit update of the social contract regarding what people perceive as "normal", non-discriminatory, ”appropriate” or ”healthy” does not soften an individual's rights and democratic values.

Norming and developing are brothers in a conflict-prone relationship. They are results of evolutionary aspects, both opposite and complementary of each other – Campbell's "blind variation and selective retention". What might be seen as normal might change. Taking an illustration from the ”old” world: How legitimate would it be today to boycott corrective eye glasses in the work place because one is treating his reduced eyesight as natural? 100 years ago, the question would probably have been answered differently. How will the perspective on implants, tracking or wearables change, and for what reason? The answer to these questions we do not yet know, but it seems to be clear: They will be different from our answers today.

Human Rights Education is helping people to find their answers to how *new* developments might be brought together with *older* rights and values. It facilitates the exploration where new rights and morals need to be developed when necessary. Last but not least, Human Rights Education is supporting autonomous, free and equal ”real” individuals to find a balance with what we call the digital self and, if necessary, effective ways to master it.

Literature

Arendt, H.: The Human Condition (1958). Chicago, University of Chicago Press.

AppAnnie (2017). Spotlight–App-Nutzung durch Verbraucher.
http://files.appannie.com.s3.amazonaws.com/reports/1705_Report_Consumer_App_Usage_DE.pdf

Jakob Augstein, J (Ed. 2018). Reclaim Autonomy – Selbstermächtigung in der digitalen Weltordnung. Berlin 2017.

Bertelsmann Stiftung (2016). Health Apps, Spotlight Healthcare. Gütersloh.
https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/SpotGes_Health_apps_en_final.pdf

Basu, T. (2019, December 13). Warum Kinder Alexa nicht vertrauen. Heise Online. Retrieved September 10, 2020, from https://www.heise.de/tr/artikel/Warum-Kinder-Alexa-nicht-vertrauen-4613817.html

Bitdefender (2016). Security Awareness in the Age of Internet of Things. A 2016 Bitdefender Study.
http://download.bitdefender.com/resources/files/News/CaseStudies/study/136/Bitdefender-Whitepaper-IoTSecurity-A4-en-EN-web.pdf

BITKOM (2011).nDatenschutz im Internet. Eine repräsentative Untersuchung zum Thema Daten im Internet aus Nutzersicht. Bundesverband Informationswirtschaft,Telekommunikation und neue Medien e. V. Berlin. https://www.bitkom.org/sites/default/files/file/import/BITKOM-Publikation-Datenschutz-im-Internet.pdf

Brey, P.; Gauttier, S.; Milam, P. (2019). Harmful internet use Part II: Impact on culture and society. Scientific Foresight Unit (STOA), Directorate for Impact Assessment and European Added Value, European Parliament, Brussels. https://doi.org/10.2861/391152

Bundesverband Digitale Wirtschaft e.V (BVDW, 2017). Digital Trends Umfrage zu digitalen Sprachassistenten. November 2017.
https://www.bvdw.org/fileadmin/user_upload/BVDW_Digital_Trends_Sprachassistenten.pdf

Chaos Computer Club (2013/09/21). Chaos Computer Club breaks Apple TouchID.
https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

Chaos Computer Club (2014/12/27). Starbug: Ich sehe, also bin ich ...Du. Gefahren von Kameras für (biometrische) Authentifizierungsverfahren. https://media.ccc.de/v/31c3_-_6450_-_de_-_saal_1_-_201412272030_-_ich_sehe_also_bin_ich_du_-_starbug

Chaudron, S.; Eichinger, H. (2018). Eagle_eye on – Identities in the digital world, Evolution and challenges. Joint Research Council (JRC), Publications Office of the European Union, Luxembourg. https://doi.org/10.2760/48837

CISCO (2020). Cisco Annual Internet Report (2018–2023), White paper.
https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf

Clausen, J.; Fetz, E., Donoghue, J.; John Donoghue, Ushiba, J; Chandler, J.; Spörhase, U.; Birbaumer, N.; Soekadar, S. (2017). Help, hope, and hype: Ethical dimensions of neuroprosthetics. Science 2017/06/30, p.1338 f. https://doi.org/10.1126/science.aam7731

Couldry, N.; Mejias U. A. (2019). Making data colonialism liveable: how might data's social order be regulated? Internet Policy Review,[online] 8(2). https://policyreview.info/articles/analysis/making-data-colonialism-liveable-how-might-datas-social-order-be-regulated, accessed: 2019/12/09

Couldry, N. (2018). Colonised by data – the hollowing out of digital society. Lecture held at the Alexander von Humboldt Institute for the Digital Society, held at 20 Nov 2018.
https://www.hiig.de/en/events/nick-couldry-colonised-by-data-the-hollowing-out-of-digital-society

Council of Europe (CoE CM/Rec(2010)7). Recommendation CM/Rec(2010)7
of the Committee of Ministers to member states on the Council of Europe Charter on Education for Democratic Citizenship and Human Rights Education (Adopted by the Committee of Ministers on 11 May 2010 at the 120th Session).
https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cf01f

Day, M.; Turner, G.; Drozdiak, N. (2019). Amazon Workers Are Listening to What You Tell Alexa. Bloomberg 2019/04/11.
https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio

Eikenberg, E. (2020). Wie Avast die Daten seiner Kunden verkaufte. In c‘t – magazin für computer und technik, 05/2020.

Dark Patterns. https://darkpatterns.org

Deutscher Ethikrat (2018). Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung – Stellungnahme – Kurzfassung. Berlin.
https://www.ethikrat.org/themen/forschung-und-technik/big-data

Di Giacomo, D.; De Liso, G.; Ranieri, J. (2018). Self body-management and thinness in youth: survey study on Italian girls in: Health and Quality of Life Outcomes.
https://doi.org/10.1186/s12955-018-0937-4

Digitalcourage (2018). Big Brother Award 2018: Laudatio of padeluun for Alexa.
https://bigbrotherawards.de/2018/verbraucherschutz-amazon-alexa

Digitalcourage (2019). Big Brother Award 2019: Laudatio of Thilo Weichert for Ancestry.com.
https://bigbrotherawards.de/2019/bio technik-ancestry_com

EDRi (2018/03/21). Control of sorts over personal data for UK healthcare patients (21 Mar 2018)
https://edri.org/control-sorts-personal-data-uk-healthcare-patients/

European Court of Justice C-673-17. Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband e.V. vs. Planet49 GmbH.

European Commission (EU FORESIGHT). Topic: Changing Nauture of Work.
https://ec.europa.eu/knowledge4policy/foresight/topic/changing-nature-work_en

European Parliament, European Commission (EP, EC 2002/58/EC). 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). https://eur-lex.europa.eu/eli/dir/2002/58/oj

European Parliament, European Commission (EP, EC Regulation 2016/679). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation. https://data.europa.eu/eli/reg/2016/679/oj

European Commission (EC COM 2017/010). Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD).

European Commission (EU COM 2020/65 final). Directorate-General for Communications Networks, Content and Technology: White Paper - Artificial Intelligence -A European approach to excellence and trust. https://op.europa.eu/s/oaNu

European Economic and Social Committee (EESC 2019/02/20). The digital revolution in view of citizens' needs and rights OPINION TEN/679, Rapporteur: Ulrich Samm

European Union Agency for Fundamental Rights (EU-FRA 2018). Handbook on European data protection law; Luxembourg: Publications Office of the European Union. https://doi.org/10.2811/58814
Gittleman, M.; Monaco, K (2019). Truck-Driving Jobs: Are They Headed for Rapid Elimination? ILR Review. 001979391985807. https://doi.org/10.1177/0019793919858079

European Union Agency for Fundamental Rights (EU-FRA 2019). Facial recognition technology: fundamental rights considerations in the context of law enforcement; Luxembourg: Publications Office of the European Union. https://doi.org/10.2811/52597

European Union Agency for Fundamental Rights (EU-FRA 2020-1). Facial recognition technology: fundamental rights considerations in the context of law enforcement, Publications Office of the European Union, Luxemburg. https://doi.org/10.2811/231789

European Union Agency for Fundamental Rights (EU-FRA 2020-2). Your Rights Matter: Data Protection and Privacy; , Publications Office of the European Union, Luxemburg. https://doi.org/10.2811/292617

Fourcade, M.; Healy, K. (2017). Seeing like a market. In Socio-Economic Review, 2017, Vol. 15, No. 1, 9–29. https://doi.org/10.1093/ser/mww033

Frankfurter Allgemeine Zeitung (2019). Warum Tui-Mitarbeiter einen Chip unter der Haut tragen. https://www.faz.net/-ikh-9sut7

Garriga, G. (2019). AI Reinventing Insurance: Speech held at 5th Digital Future Science Match, Berlin, May 14, 2019, hosted by Der Tagesspiegel.

Graveling. R.; Winski, T.; Dixon, K. (2017). The Use of Chip Implants for Workers, Study requested by the European Parliament's Committee on Employment and Social Affairs (EMPL). https://doi.org/10.2861/34896

The Guardian (2013). NSA files: decoded. Retrieved from: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

Hill, K. (2020, January 18). The Secret Company That Might End Privacy as We Know It. The New York Times. Retrieved September 10, 2020, from https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Holland, V. (2020, January 23). Geschichtsdaten: Twitter fordert Clearview zur Löschung auf. Heise Online. Retrieved September 10, 2020, from https://www.heise.de/newsticker/meldung/Immense-Gesichtsdatenbank-von-Clearview-Twitter-verlangt-Bilderloeschung-4644811.html

Ienca, M; Haselager, P. (2016). Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity. In Ethics Inf Technol (2016) 18: 117. https://doi.org/10.1007/s10676-016-9398-9

IFR International Federation of Robotics (2019). Executive Summary World Robotics 2019 Industrial Robots - Editorial https://ifr.org/downloads/press2018/Editorial_WR_2019_Industrial_Robots.pdf

IFR International Federation of Robotics (2020). Top Trends Robotics 2020. https://ifr.org/ifr-press-releases/news/top-trends-robotics-2020

Kapalschinski, C.; Rexer, A. (2019). Amazons Alexa-Chef: “Wir haben Fehler gemacht”. Retrieved from https://www.handelsblatt.com/technik/it-internet/david-limp-im-interview-amazons-alexa-chef-wir-haben-fehler-gemacht/25091330.html

Krempl, S. (2018, December 29). 35C3: Über die “smarte” Glühbirne das Heimnetzwerk hacken. Heise Online. Retrieved September 10, 2020, from https://www.heise.de/newsticker/meldung/35C3-Ueber-die-smarte-Gluehbirne-das-Heimnetzwerk-hacken-4259891.html

Kleinz, T. (2008, March 29). CCC publiziert die Fingerabdrücke von Wolfgang Schäble. Heise Online. Retrieved September 10, 2020, from https://www.heise.de/security/meldung/CCC-publiziert-die-Fingerabdruecke-von-Wolfgang-Schaeuble-Update-193732.html

Kühn, S., Gleich, T., Lorenz, R. et al. (2014). Playing Super Mario induces structural brain plasticity: gray matter changes resulting from training with a commercial video game. Mol Psychiatry 19, 265–271 (2014). https://doi.org/10.1038/mp.2013.120

Kurz, C, Rieger, F. (2017): Autonomie und Handlungsfähigkeit in der digitalen Welt: Crossing the “creepy line”? In Augstein (2017).

Loideain, N; Adams, R (2020). From Alexa to Siri and the GDPR: The gendering of Virtual Personal Assistants and the role of Data Protection Impact Assessments; Computer Law & Security Review, Volume 36. https://doi.org/10.1016/j.clsr.2019.105366

Lobe, A. (2019). Speichern und strafen. Die Gesellschaft im Datengefängnis. München.

Lopez-Fernandez, O; Kuss, D. J. (2019). Harmful internet use – Part I: Internet addiction and problematic use; Scientific Foresight Unit (STOA), Directorate for Impact Assessment and European Added Value; European Parliament; Brussels. https://doi.org/10.2861/315951

Meidert, U.; Scheermesser, M.; Prieur, Y.; Hegyi, S.; Stockinger, K.; Eyyi, G.; Evers-Wölk, M.; Jacobs, M.; Oertel, B.; Becker, H. (2018). Quantified Self - Schnittstelle zwischen Lifestyle und Medizin. TA-SWISS 67, Zurich. https://doi.org/10.3218/3892-7

van Mensvoort, K. (2017). Antropomorphismus-Phobie. In Otto, Gräf (2017).

Meyer, B; Asrock, F (2018). Disabled or cyborg? How bionics affect stereotypes toward people with physical disabilities. Frontiers in Psychology, 9(2251), 1-13. https://doi.org/10.3389/fpsyg.2018.02251

Moll, R.; Schulze, A.; Rusch-Rodosthenous, R.; Kunke, C,; Scheibel, L. (2017). Wearables, Fitness-Apps und der Datenschutz: Alles unter Kontrolle?. Verbraucherzentrale NRW e. V. http://www.marktwaechter.de/digitale-welt/marktbeobachtung/wearables-und-fitness-apps

Mozilla Foundation (2019). Internet Health Report 2019. Bielefeld. https://www.transcript-verlag.de/978-3-8376-4946-8/internet-health-report-2019

Nocun, K. (2018). Die Daten, die ich rief – Wie wir unsere Freiheit an Großkonzerne verkaufen. Köln.

Otto, P.; Gräf, E. (2017). 3thics- die Ethik der digitalen Zeit. Berlin 2017.

Pariser, E. (2012). Filter Bubble: Wie wir im Internet entmündigt werden, München.

Pekka Raatikainen, M. J.; Arnar, D. O.; Zeppenfeld, K,; Merino, L. J.; Levya, F.; Hindriks, G.; Kuck, K. (EUROPACE 2015). Comparative analysis of EHRA White Book data 2009-2013: Statistics on the use of cardiac electronic devices and electrophysiological procedures in the ESC countries. 2014 report from the European Heart Rhythm Association (EHRA) In: Europace – 2015/01/23 17 Suppl 1. https://doi.org/10.1093/europace/euu300

Reinberger, S (2017). Digitale Medien. Neue Medien – Fluch oder Segen? In: Gemeinnützige Hertie Stiftung: G_AP Gehirn - Anwendung Praxis (project report). Fokus Schule. https://www.ghst.de/fileadmin/images/02_Formulare_und_Dokumente/Bericht_GAP_2017.pdf

Robinette, P.; Wenchen L., Allen, R; Howard, A. M.; Wagner, A. R.: Overtrust of Robots in Emergency Evacuation Scenarios, (2016). ACM/IEEE International Conference on Human-Robot Interaction) (HRI 2016). https://www.cc.gatech.edu/~alanwags/pubs/Robinette-HRI-2016.pdf

Royal Society for Public Health: #StatusOfMind - Social media and young people‘s mental health and wellbeing, London May 2017 https://www.rsph.org.uk/our-work/campaigns/status-of-mind.html

Eric Schmidt (2010). At the Washington Ideas Forum in Washington, D.C. on October 1, 2010. https://www.youtube.com/watch?v=CeQsPSaitL0 (from 14:10)

Selke, S. (2016-1). Lifelogging: Digitale Selbstvermessung und Lebensprotokollierung zwischen disruptiver Technologie und kulturellem Wandel, Berlin. https://doi.org/10.1007/978-3-658-13137-1

Selke S. (2016) Ausweitung der Kampfzone. In: Selke S. (eds) Lifelogging. Springer VS, Wiesbaden. https://doi.org/10.1007/978-3-658-10416-0_14

Solove, D. J. (2006). A Taxonomy of Privacy. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006. GWU Law School Public Law Research Paper No. 129. https://ssrn.com/abstract=667622

Spiekermann, S. (2010). About the “Idea of Man” in System Design – An enlightened version of the Internet of Things? In Architecting The Internet of Things, edited by D. Uckelmann, M, Harrison, F. Michahelles, Springer Verlag, 2010, p. 25-34. http://ssrn.com/abstract=2046497

Spiekermann-Hoff, S; Böhme, R.; Acquisti, A.; Hui, K-L. (2015). The Challenges of Personal Data Markets and Privacy. Electronic Markets (em), 25 (2). pp. 161167. ISSN 1422-8890. https://ssrn.com/abstract=3305307

Suarez, D. (2017). Wie die Technik unser Denken verändert in: Augstein (2017)

The Intercept (2015/11/12). Edward Snowden Explains How To Reclaim Your Privacy; Micah Lee; November 12 2015. https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/

US Food and Drug Association (US-FDA 2017/08/29). Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott‘s (formerly St. Jude Medical‘s) Implantable Cardiac Pacemakers: FDA Safety Communication. https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals

Vincent, D.: China used prisoners in lucrative internet gaming work in The Guardian 25/5/2011. https://www.theguardian.com/world/2011/may/25/china-prisoners-internet-gaming-scam

Wang, F.; Tong, Y.; Danovitch, J. (2014). Who do I believe? Children’s epistemic trust in internet, teacher, and peer informants. In Cognitive Development, Volume 50, 2019, Pages 248-260, ISSN 0885-2014. https://doi.org/10.1016/j.cogdev.2019.05.006

Weiser, M. (1991). The Computer for the 21st Century in: Scientific American 09/1991; 94-104.

Wilkens, A. (2015). Wir müssen Small Data werden. In Die Zeit 25.3.2015. https://www.zeit.de/kultur/2015-03/analog-digital-bio-essay/

Zeh, J. (2014/02/11). Schützt den Datenkörper! In Frankfurter Allgemeine Zeitung. https://www.faz.net/-hyt-7m8gw

Zhou, F., Montag, C., Sariyska, R., Lachmann, B., Reuter, M., Weber, B., Trautner, P., Kendrick, K. M., Markett, S., Becker, B. (2019). Orbitofrontal gray matter deficits as marker of Internet gaming disorder: converging evidence from a cross-sectional and prospective longitudinal design. Addiction Biology, 24: p. 100– 109. https://doi.org/10.1111/adb.12570

Zuboff, S.(2018). The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power. Profile Books, London 2019.

Zuboff, S (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization (April 4, 2015). Journal of Information Technology (2015) 30, 75–89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2016/03/05). Google as a Fortune Teller: The Secrets of Surveillance Capitalism (2016, published in German language as: Überwachungskapitalismus: Wie wir Googles Sklaven wurden) by: Frankfurter Allgemeine Zeitung. https://www.faz.net/-hzi-8eaf4.

Sharing is Caring

This series "Smart City, Smart Teaching: Understanding Digital Transformation in Teaching and Learning" is an Open Educational Resource (OER) supported by the European Commission.

If you copy or further distribute this publication, please always refer to "DARE network & AdB", the https://dare-network.eu website as source and acknowledge the "DIGIT-AL project" as authors.