Deutsches Institut für Menschenrechte

Institute for Business Ethics
University of St.Gallen

Analysis

Business and Human Rights in the Data Economy

A Mapping and Research Study

Isabel Ebert I Thorsten Busch I Florian Wettstein



The German Institute for Human Rights

The German Institute for Human Rights is the independent National Human Rights Institution of Germany. It is accredited according to the Paris Principles of the United Nations (A-status). The Institute's activities include the provision of advice on policy issues, human rights education, information and documentation, applied research on human rights issues and cooperation with international organizations. It is financed by the German Federal Parliament (Deutscher Bundestag). In addition, the Institute is specifically mandated to monitor the implementation of the UN Convention on the Rights of Persons with Disabilities and the UN Convention on the Rights of the Child and has established Monitoring Bodies for these purposes.

Authors

Isabel Ebert is a Research Associate and PhD Candidate at the Institute for Business Ethics, University of St. Gallen. Her PhD focusses on ethical questions regarding data disclosure by companies to governments. Since September 2019, Isabel is a visiting researcher at the Oxford Internet Institute. She is also part of a Swiss National Science Foundation research project on workplace monitoring and privacy in cooperation with the Institute for Work and Employment Research, University of St. Gallen. Isabel served as the EU Representative of the Business & Human Rights Resource Centre, based in London (2014-2018). She holds a M.A. in International Relations, Peace and Conflict Studies from Goethe University Frankfurt and a B.A. in Politics and Management from University of Konstanz and Sciences Po Paris.

Thorsten Busch teaches digital business ethics, responsible innovation, digital games, and digital marketing ethics at the University of St. Gallen, Switzerland, Trinity Business School, Ireland, and HEC Montréal, Canada. His award-winning research on a wide range of issues in digital ethics has been published in outlets such as the Journal of Business Ethics, Ethics and Information Technology, and Convergence, and it has been presented at leading international institutions, including MIT, University of Oxford, and McGill University. Among other positions, Thorsten was a Postdoctoral Fellow in game studies at Concordia University in Montréal, Canada, a Visiting Assistant Professor in corporate social responsibility at the University of Konstanz, Germany, and a Senior Research Fellow in data ethics at the University of St. Gallen, Switzerland. Thorsten holds an M.A. in political science, economics, and management from the University of Oldenburg, Germany, and a Ph.D. in organizational studies and cultural theory from the University of St. Gallen, Switzerland.

Florian Wettstein is a Professor and Director of the Institute for Business Ethics at the University of St. Gallen. Florian is Vice-President of the International Society of Business, Economics, and Ethics (ISBEE) and of the Global Business and Human Rights Scholars Association (BR2R). He is Editor-in-Chief of the Business and Human Rights Journal (BHRJ), published by Cambridge University Press, and the author of Multinational Corporations and Global Justice: Human Rights Obligations of a Quasi-Governmental Institution (Stanford University Press, 2009). He held previous positions at York University in Toronto and at University of St. Thomas in Minneapolis/St. Paul. He is a past fellow of Massachusetts Institute of Technology's "Program on Human Rights and Justice".

This analysis reflects the views of the German Institute for Human Rights.

Deutsches Institut für Menschenrechte

Institute for Business Ethics
University of St.Gallen

Analysis

Business and Human Rights in the Data Economy

A Mapping and Research Study

Isabel Ebert I Thorsten Busch I Florian Wettstein

Preface

Digitalization is a topic that is gaining importance rapidly. However, neither companies nor states have yet developed a thorough and systemic understanding of the data economy's human rights impacts. For instance, in what ways can algorithms impact human rights? Does the international human rights protection system provide the necessary means to deal with, e.g., racist or gender-biased analytics software that supports court decisions? To what extent are companies responsible if their services facilitate the spread of hate speech and violence? What should corporate human rights due diligence systems look like in the data economy? Do the existing frameworks provide adequate protection already, or do we need new ones? These are some of the questions the German Institute for Human Rights seeks to explore in its business and human rights work. For this purpose, it commissioned the Institute for Business Ethics at the University of St. Gallen to undertake this mapping study in 2019. Preliminary results were shared with stakeholders from academia, civil society and business in a workshop in March 2020 and incorporated in this analysis.

The UN Guiding Principles on Business and Human Rights, as endorsed by the UN Human Rights Council in 2011, have become the stepping stone for progressive company policies and practice on human rights respect. At the same time, the accelerating growth of the information society and data economy have created new challenges with regard to the corporate responsibility to respect human rights. It becomes apparent that by datafying a growing number of domains both in business and in society, data-driven business affects human rights on many levels and in a wide range of contexts.

The recent developments around the Covid-19 pandemic have demonstrated how technology can assist in rolling-out and implementing widespread measures to handle a public health emergency. At the same time, those same measures, often hastily decided upon and sometimes unchecked bya balance of powers, threaten to infringe on a plethora of human rights, such as privacy. It raises the question whether it may be more harmful than helpful to embark on unchartered territory at fast speed by applying means such as Covid-19 tracking apps that might infringe on digital rights. Often, such measures are implemented or facilitated by private organizations.

This study suggests that addressing the corporate responsibility of technology companies through a business and human rights lens has the benefit of anchoring the debate in internationally established norms and universally accepted human rights. Furthermore, discussing human rights in the data economy from this angle opens the possibility for companies to use or learn from managerial toolkits that have already been developed in this field. Business and human rights frameworks offer a clear corporate human rights due diligence procedure, which technology companies can and should adapt to their context and apply in their operations.

Prof. Dr. Florian Wettstein
Director, Institute for Business Ethics
at the University of St. Gallen

Michael Windfuhr
Deputy Director, German Institute
for Human Rights

Contents

Executive Summary 9

1 Introduction: Human Rights in the Data Economy 10

1.1 The Data Economy: Between Hype and “Techlash” 10

1.2 Opacity in Data-Driven Business Models 12

1.3 Rethinking Human Rights Along the Technological Lifecycle and Within Data Ecosystems 12

2 Privacy as the Gateway for Human Rights Protection in the Data Economy 14

3 Exploring Technologically Driven Human Rights Risks Through Vignettes 16

3.1 Connected Mobility and Autonomous Vehicles 16

3.2 Smart Cities 17

3.3 Privacy and Health 17

3.4 Labor and the Gig Economy 18

3.5 Workplace Monitoring and Worker Surveillance 18

3.6 Recruiting and Algorithmic Bias 18

3.7 Credit Scoring 19

3.8 Targeted Data Profiling of Human Rights Defenders 19

3.9 Predictive Policing 19

3.10 Public-Private Partnerships in Law Enforcement 19

3.11 Facial Recognition, Border Control and Drone Technology 20

4 The Responsibility to Respect Human Rights in the Data Economy 21

5 Ways Forward: Human Rights Due Diligence in the Data Economy 23

5.1 Identifying and Assessing Human Rights Impacts: Policy Commitment, Data Collection and Baseline Development 24

5.2 Acting on the Findings: Identify Existing Processes and Potential Gaps 24

5.3 Impact Mitigation and Management: Prioritize Measures and Agree on Next Steps 25

5.4 Reporting, Evaluation and Remedy: Anchor Human Rights Due Diligence in Business Practice to Enable Organizational Learning 26

6 Concluding Remarks 27

7 References 28

Executive Summary

This study identifies novel challenges for human rights protection emerging from data-driven business conduct. It offers an overview of the current policy debate and emerging best practices for business to mitigate the impacts of data-driven business on human rights. A strong emphasis lies on the dynamic interlinkages between human rights issues in a data ecosystem, in particular addressing systemic bias in data models and establishing genuine stakeholder engagement.

This mapping study serves as a conversation starter and aims at raising awareness regarding the data economy's impact on human rights. On the one hand, the study could be used in a public policy context, e.g. to convince ministerial staff that "digital" human rights issues should also be part of National Action Plans on Business and Human Rights, or why the EU Digital Strategy can benefit from a rights-based approach. On the other hand, companies can use the study to engage in a dialogue with senior management on why a rights-based approach is relevant and should be mainstreamed across business, e.g. for a product counsel or a public affairs specialist. The study thus provides exploratory guidance for human rights impact and risk assessments and human rights due diligence. It addresses some core phenomena and technologies of the data economy and situates them within the social, cultural, and political contexts that explain their effects on human rights.

The study presents the following key recommendations:

- Business needs a life cycle approach to capture emerging and systemic human rights problems. This would allow it to identify, address and eradicate systematic distortions that have negative impacts on human rights in datafied environments. "Data universalism" needs to be replaced with context-specific, robust human rights due diligence processes that keep companies' local embeddedness in mind.

- Civil society may need to develop new methods to hold companies accountable for "digital" human rights violations. This point is closely connected to the public policy debate on the state duty to protect human rights, including digital rights.

- Policymakers should take digital rights into account in policy proposals on human rights due diligence for business and revisit whether existing protection can still cover emerging digital issues. Legislators should strengthen digital rights in the coming years and strategically connect them to other legislative debates on human rights due diligence.

This mapping can serve as a basis for a deeper examination of what all actors-states, companies, civil society organizations, national human rights institutions-can do to guarantee that digitalization and technological progress go hand in hand with the enjoyment and protection of human rights.

1 Introduction: Human Rights in the Data Economy

1.1 The Data Economy: Between Hype and "Techlash"

For years now, data has been hailed as "the new oil" that organizations need to extract and monetize (Thorp 2012; Tarnoff 2017). Due to the "hype" (Crawford 2013) and "mythology" (Boyd & Crawford 2012) surrounding Big Data, transnational corporations continue to leave no stone unturned in their effort to uncover new ways of becoming ever more competitive and innovative. As a result, the data economy is driven by major corporations utilizing technologies that "render into data many aspects of the world that have never been quantified before" (Cukier & Mayer-Schönberger 2013: 29). Contrary to popular belief, however, this phenomenon is neither new nor a force of nature foisted upon us without any room for critical reflection or political intervention. Instead, today's data economy is the result of the "Californian ideology" (Barbrook & Cameron 1996), i.e. specific financial interests and decades of specific sociocultural developments, most of which center around the culture and business models of tech companies based in Silicon Valley. While not necessarily a new phenomenon, the "datafication" (Cukier & Mayer-Schönberger 2013) of the economy has intensified in recent years to such an extent that it increasingly has visible consequences far beyond the economic sphere itself. This has yielded ambiguous results in many ways, as optimistic narratives around the many potential benefits of new technologies in domains such as medicine and business have given way to profound concerns around potentially abusive uses of technology (Mittelstadt et al. 2016; Brooks 2017; Christl 2017a/b; Cohen 2017; Zuboff 2019). A recent report by Amnesty International (2019: 50) offered scathing criticism in this regard, claiming that companies "that depend on invasive data-driven operations amounting to mass corporate surveillance must find ways to transition to a rights-respecting business model." This issue has become all the more pressing in recent years because it is no longer just individual companies or industries that have become ever more dependent on data-driven business models. In addition to the private sector, it is also nation-states and political entities such as the European Union that try to walk the fine line between supporting the data economy on the one hand, and reining it in due to ethical concerns on the other.

One reason for this conflict between economic and ethical concerns is that over the past decade, most major US tech companies have been affected by scandals and 'moral panic' around their services. Facebook in particular has been in the spotlight of public concern, followed by Google and Amazon. In light of its many privacy violations, Facebook was called out by The Guardian as "the bad guy" as early as 2016 (Solon 2016). Various minor scandals followed until the so-called "Cambridge Analytica" scandal hit in 2018, which to a certain extent served as a wake-up call for the general public. The Cambridge Analytica scandal revealed that Facebook had been harvesting personal data of millions of its users without consent and that the data had been used for political purposes, such as influencing voter behavior through targeted advertising. These revelations led to public outcry and political hearings on both sides of the Atlantic (Confessore 2018). Moreover, Facebook was criticized for its complicity in fueling political conflicts in Myanmar (Roose & Mozur 2018). 2019 was an equally turbulent year for the company, with CEO Mark Zuckerberg testifying before both the US congress and EU parliament in the aftermath of the Cambridge Analytica revelations, along with an additional US congress hearing on Facebook's cryptocurrency, "Libra". As a result, the tech industry as a whole has since been caught up in a massive "techlash" (Sa-

casas 2018; Zimmer 2019), and public trust in technology companies' ability to responsibly navigate the many ethical risks inherent in their business models is at an all-time low (Deibert 2019). This "techlash" also illustrates the ever-increasing dependencies between the worlds of politics and business, both nationally and internationally (Scherer & Palazzo 2011), which will be discussed particularly intensely in 2020 due to the federal elections in the US. Aside from their influence on traditional political channels, scholars and critics alike have also called out tech companies' business practices and their role in establishing deeply problematic forms of modern "data capitalism" (Myers West 2019). In this context, Zuboff (2015, 2019) coined the term "surveillance capitalism," which describes a political economy that is driven by tech companies' virtually unlimited appetite for data extraction. Human beings in this system are relegated to an instrumental role as mere data subjects whose personal information is processed by Kafkaesque algorithmic "black boxes" for the financial gain of the data economy (Pasquale 2015; Srnicek 2017).

Against this background, it becomes apparent that by datafying as many aspects of business and society as possible, tech companies affect human rights on many levels and in a wide range of contexts (Reventlow 2019). That is why scholars, NGOs and increasingly also policymakers have been drawing attention to the human rights impact of new technologies, such as artificial intelligence and machine learning (Access Now 2018a/b; Andersen 2018; Whittaker et al. 2018).

Although definitions tend to differ quite a bit, the term "Artificial Intelligence" (AI) broadly summarizes computerized systems and/or processes that mimic human intelligence, including the ability to adapt, learn, and plan ahead automatically. The Alan Turing Institute, for example, explains AI as follows: "a machine or system performs tasks that would ordinarily require human (or other biological) brainpower to accomplish, such as making sense of spoken language, learning behaviours or solving problems. There are a wide range of such systems, but broadly speaking they consist of computers running algorithms, often drawing on data."

Machine learning (ML), on the other hand, is a predictive analytical process based on algorithms and statistical models that computer systems use to perform a specific task or to spot patterns and make inferences without using explicit instructions. Machine learning is a part of AI. Algorithms use a mathematical model based on sample data (training data) to make predictions and/or decisions. According to Article 19 and Privacy International, the lack of definitional clarity is a challenge, as different types of AI systems raise specific ethical and regulatory issues (Article 19 & Privacy International 2018). The discourse on ethical concerns about AI is often summarized as "AI ethics."

AI ethics discourse can be a good conversation starter, but the abundance of frameworks makes it unclear what the actual foundations of AI ethics are (Jobin, Ienca & Vayena 2019; Fjeld et al. 2020). Concepts centered around AI ethics, which are predominantly based on ethical guidelines, have been criticized for their voluntary nature and vague language (Hilligoss et al. 2018; Raso et al. 2018; Sloane 2018). Indeed, while some elements of the AI ethics discourse are relevant and useful when it comes to advancing and respecting human rights, others risk muddying the waters. For instance, Wagner (2018) argues that the vague language of corporate social responsibility (CSR) is frequently used by corporations to avoid regulation, and in a similar fashion, supposedly "ethical" principles can even be used to harm fundamental freedoms (Pirkova 2018).

On the other hand, discussing human rights in the data economy has turned out to be particularly fruitful from a business and human rights angle (Ruggie 2007, 2013; Wettstein 2015, 2016; Jorgensen 2019). That is because human rights-based approaches provide clarity and are based on commonly accepted standards. Addressing corporate responsibility through a business and human rights lens has the benefit of anchoring the debate in internationally established norms, universally accepted human rights, and managerial toolkits, as business and human rights frameworks offer a "do no harm" perspective as a minimum standard to avoid negative effects on human rights through business operations (Ruggie 2007, 2013; Wettstein 2015, 2016; Jorgensen 2019). This study will thus address some core phenomena and technologies of the data economy by situating them within the social, cultural, and political contexts that explain their effects on human rights.

1.2 Opacity in Data-Driven Business Models

As international tech companies, such as Google or Amazon, advance "surveillance capitalism" (Zuboff 2015, 2019), every aspect of modern business is put under close scrutiny to identify any and all untapped data extraction opportunities. Thus, the use of increasingly sophisticated technologies in the data processing economy creates ever more granular and scalable levels of information (Gasser & Almeida 2017). Formerly unsophisticated data analytics processes have evolved into new techniques explaining, inferring, interpreting, and extrapolating human action by consolidating a wide range of highly granular data points, often collected and submitted by users themselves on a voluntary basis (Cohen 2015; Neff & Nafus 2016). The enhanced quality of data obtained by using new technologies even enables prescriptive analytics for business purposes, which has many potential effects on human rights, for instance due to surveillance technology in the workplace or software for predictive policing.

Due to these new levels of complexity and the interconnectedness of data gathering and processing technologies, information asymmetries regarding data and its interpretation can become quite impactful, as more and more societal structures are now being governed through data-driven black boxes (Pasquale 2015). This is rendered particularly severe when we consider the power imbalance between the bodies collecting and processing data on the one hand and those who are relegated to the role of mere data subjects, i.e. the objects of data processing, on the other (Byrne 2019). Hence, there is a need for social learning among all involved stakeholders to respect human rights in light of the new information density and granularity enabled by new, data-driven technologies.

In many ways, surveillance capitalism is a dehumanizing process, and unfortunately, data-driven societal models are not immune to errors, biases, or wrong conclusions about human interaction (Monahan 2016; Whittaker et al. 2018). That is why scholars use drastic terms such as "data colonialism" (Couldry & Meijas 2018) to describe how a technologically driven economic logic increasingly views human traditions, norms, and values merely as an obstacle to doing business (Risse 2018; Risse & Stevenson 2019). Moreover, the assumed default position when rolling out data-driven business models often reflects a "data universalism" (Milan & Treré 2019) that fails to take into account multi-dimensional contextuality, which in turn can lead to cascading negative effects on affected individuals, particularly in the Global South (Graham 2019). For instance, platform-based work might produce new opportunities in the Global South and widen participation for some actors; yet at the same time, it might leverage and reinforce existing socio-cultural hierarchies, e.g. caste systems in India. Another example is algorithmic governance, which might enshrine precarity for informal workers unless there is situated reckoning of the unique historical and labor needs of Global South geographies, rather than a "blind adoption" of universal or Western AI futures (Global Information Society Watch 2019). In addition, using data-driven models in working with refugees might put people at risk if the authoritarian regimes or armed groups they are fleeing from get hold of their data (International Committee of the Red Cross & Privacy International 2018). Therefore, human rights play an increasingly vital role in setting contextual boundaries to surveillance capitalism and in enabling a digitally mediated life worth living for billions of individuals and their respective communities. When it comes to addressing these challenges in practice, this implies that human rights lawyers, policymakers, social scientists, computer scientists, and engineers need to work together to operationalize human rights into business models, workflows, and product design (Latonero 2018).

1.3 Rethinking Human Rights Along the Technological Lifecycle and Within Data Ecosystems

The new interlinkages between human rights impacts and business operations in the data economy require new, holistic methods to identify, mitigate, and eradicate negative impacts on human

rights. Suitable proposals require a certain degree of rethinking human rights along the technological lifecycle and within a data ecosystem. The "AI Blindspot" project at MIT outlines three such lifecycle stages:

- Planning: checking the intended purpose of a service or product, verifying whether data is representative, abusability is prevented, and privacy is respected;
- Building: prevent discrimination by proxy, uphold explainability, and optimize criteria;
- Deploying: check against generalization errors and integrate the right to contest resulting action (MIT Media Lab 2019).

Such an assessment will require a different mindset when thinking about concrete and potential human rights impacts, away from classic linear thinking and towards how we build processes in multi-disciplinary teams that can identify blindspots in AI and find systemic biases in context-specific environments along all lifecycle stages, starting in product development.

In the following, we will argue that privacy has a gateway function for human rights protection in the data economy. Yet, we would like to re-emphasize that all human rights can be affected by data-driven business and need to be taken into account, in particular those rights that might be affected as unintended consequences.

2 Privacy as the Gateway for Human Rights Protection in the Data Economy

As an intrusion into the private sphere of an individual lays bare the very data that data-driven business models require, upholding privacy can be seen as the gateway for human rights protection in the data economy. Importantly, this privacy gateway logic should not overlook the exploitation of data that had initially been shared voluntarily by users and/or that later was combined in Big Data ecosystems. Moreover, even if a user might have withheld consent in the first place, data can still be shared for other means without consent, or one user might be impacting non-users by sharing their data on their behalf and without their consent. These interdependencies between the use of individual data and interlinkages between users in a data ecosystem demonstrate that the right to privacy is a cornerstone in the discussion about digital ethics, as an ever-increasing number of rights are influenced by digital contexts (Mittelstadt et al. 2016; Reventlow 2019). Moreover, the challenge of identifying human rights risks is not only about individuals' rights, but instead about interconnected collective effects, as it touches upon a wide range of related rights (Bernal 2016).

The individual's right to the safeguarding of their private sphere against intrusion was first articulated in Article 12 of the UN Universal Declaration of Human Rights (UDHR 1948):

> "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."

The International Covenant on Civil and Political Rights (ICCPR), adopted by the UN General Assembly in 1966, takes up the notion of privacy in article 17, stating: "No one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation."

The European Convention on Human Rights (ECHR), adopted in 1950 and entered into force in 1953, defines privacy in Article 8 as an individual's right to respect for their private and family life, home and correspondence:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a publicauthority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

As detailed above, the right to privacy is a human right enshrined in the European Convention on Human Rights (ECHR): The right to a private life protects privacy within the fundamental rights system of the Council of Europe. The fundamental right to respect for one's private life has a catch-all function, since the ECHR does not contain a general right to freedom (Maus 2006: 172).

The European Court of Human Rights (ECtHR) has consistently refrained from giving a comprehensive definition of the notion of private life (Mowbray 2012: 488; Wildhaber 2017: 214). Instead, private life is a broad term that is not exhaustive (Rainey et al. 2017: 401). The scope of protection of the "right to privacy" according to the US Constitution and of the "right to respect for private life" based on Art. 8 ECHR is identical (Maus 2006: 161). Specific aspects of the right to respect for private life are, in particular, data protec-

tion (Grabenwarter 2014: 10), the protection of informational self-determination (Kälin & Künzli 2019: 12.8), and the protection of personal correspondence (Art. 8 para. 1 ECHR).

In addition to the right to privacy, a plethora of other human rights can be affected by the data economy (Raso et al. 2018; Reventlow 2019). Again, privacy has a gateway function, as violations of privacy can enable the abuse of other human rights through insights gained by privacy breaches. Three examples illustrate this connection:

(1) If a company uses personal data of job candidates for recruiting purposes, it might acquire data from data brokers without the data subject having had the chance to give consent. Based on this data, an algorithm might decide that a female candidate or a candidate of color might be less qualified for a position. This might be due to algorithmic bias, which can occur when an algorithm was trained using biased historical data from, for instance, a tech company that used to hire a lot of male, white staff in the past. Learning from this historical training data, the algorithm would conclude that white, male candidates are who the company should look for as suitable staff members. As a result, female candidates and candidates of color would be discriminated against.

(2) Another example is the use of health data acquired from self-tracking devices. A health insurance company might decide to use data from data brokers or other sources that reveal users' fitness levels. Hence, the insurer might choose not to offer an individual customer a competitive insurance policy based on data that the insurer obtained through breaching the privacy of the user. As a result, the right to health of the individual might be violated as rightsholders could face financial discrimination by having to pay a higher premium than those clients who willingly share their data with the insurance company, or they might be denied healthcare services altogether.

(3) Similarly, in the context of smart cities, users of various apps and technologies transmit valuable personal data on a daily basis, yet data sharing policies are opaque. It is often unclear who is allowed to use what kind of data, and for what purposes. As it is a grey zone, business actors might treat personal data as a proprietary technology, use it for services unrelated to the original use case that they sought consent for, or sell personal data to third parties, thus infringing on the privacy and property rights of rightsholders (Melendez & Pasternack 2019). Third parties in turn might use the data for their respective purposes, such as hiring and recruiting or health insurance schemes.

As shown above, even though the current discourse in business and human rights tends to focus on privacy in the data economy, a wide range of human rights beyond privacy can be affected by business activities. Due to the global nature of the data economy, this phenomenon is not limited by sector-specific boundaries, national borders or legal jurisdictions. Instead, the data economy is built on the use of new technologies that enable transnational data flows and are applied in a wide range of interconnected sectors ranging from healthcare, insurance, and construction to food, private security, and a wide range of services. The following chapter will illustrate what the human rights risks resulting from these dynamics can look like.

3 Exploring Technologically Driven Human Rights Risks Through Vignettes

This chapter explores a range of technologies affecting human rights in different contexts. Despite the fact that these technologies may differ greatly from one another, two key issues that most of the following examples have in common are (1) bias in the datasets they use, which frequently results in racist and/or gender discrimination (Crawford 2013; O'Neil 2016; Courtland 2018), and (2) a lack of genuine avenues for stakeholder engagement (Jorgensen 2019).

(1) The gender data gap affects a plethora of contexts, such as government policy and medical research, technology, workplaces, urban planning, and the media. It predominantly stems from data sets that are collected based on male features, making it potentially lethal due to blind spots regarding female representation. At work, for instance, occupational health and safety measures are often designed based on data that is targeted towards men, neglecting the physiognomy and consequential physical measures for the protection of women (Criado Perez 2019; Collett & Dillon 2019). Key demands regarding how to overcome these inherent biases can be found in the Feminist Manifest-No (Cifor et al. 2019). In a similar fashion, machine learning algorithms get trained to classify people into clear-cut (binary) categories, such as "male/female," but it is questionable how the rights of people whose physiognomy or identity does not fit these fixed categories could be respected when they are literally not seen at all by technology (Buolamwini 2018; Costanza-Chock 2020). IBM, for instance, was criticized for not addressing this problem in its apologetic, prominently placed "Dear Tech" ad during the 2019 Oscars (Selinger 2019). This problem is all the more frustrating as there are actually many highly qualified women working in the field of AI ethics, but their research still is ignored in too many cases (Dand 2018).

(2) Neglecting bias in data models is closely connected with stakeholder engagement: Often, affected individuals are not aware of human rights infringements as they lack knowledge or the digital literacy to understand the issues at hand. This is reinforced by the absence of structural avenues for strategic engagement with actual rightsholders. Partly, solutions that aim at overcoming bias, such as value-sensitive design or privacy-by-design, still neglect to provide structures for genuine, continuous rightsholder engagement (Spiekermann 2012; Koops & Leenes 2014). In one way or another, the technologies addressed in this section are all affected by the aforementioned biases as well as a lack of fair and comprehensive stakeholder engagement, and we will add details with regard to the respective examples in the vignettes discussed below.

3.1 Connected Mobility and Autonomous Vehicles

At first glance, autonomous vehicles seem to have little impact on human rights, as the big issue that has been discussed for years now is a mere variation of the classic "Trolley Problem" (Foot 1967): How should autonomous vehicles behave in moral dilemma situations, such as accidents? For instance, which human being should they hit if they have the choice between a grandmother and a young child? MIT scholars used a large-scale online experiment to find empirical answers on how people tend to think about such questions (Awad et al. 2018). However, while empirical research on attitudes and opinions may give us interesting insights into the social acceptance of certain engineering decisions in autonomous vehicles (Bergmann et al. 2018), there are no easy fixes or implementations that follow from it (Wolkenstein 2018). Instead, this technology actually raises fundamental ethical questions, not technical ones

(Bogost 2018). Many of these issues affect how social inclusion and discourse on human rights will develop in the future. For instance, who gets to determine what we mean by "progress" in the context of technology and mobility? Who gets to define what types of mobility can enable diverse communities across the globe to develop in ways that matter to them? And how would the needs of people with disabilities be taken into account? Closely connected to these questions around purpose are questions addressing how human rights can be protected against technologies mainly being developed by Western corporations, such as Uber, which are then used in a non-Western cultural or political contexts. As discussed above, such technologies often come with specific norms and use cases in mind that may turn out to be problematic for a wide range of stakeholders, even more so when applied to different cultural, social or political contexts (Koebler 2016; Chee 2018; Graham 2019). On the pathway to autonomous driving, the automotive industry sees itself confronted with issues arising from connected mobility and data sharing practices in the context of these new networked information systems (Continental 2020). Automotive companies and their suppliers need to assess what it actually means in terms of their human rights impacts when they integrate a certain off-the-shelf product into their mobility ecosystem.

3.2 Smart Cities

In a similar way to autonomous vehicles, this is a technology that brings to the fore questions about human rights when it comes to designing the infrastructure of the future. While smart cities hold the potential to improve many lives across the globe (World Bank 2016), their design and development raises serious questions: Who gets to have their voices heard, whose needs should be served, and who gets to define what "smart" is even supposed to mean with regard to an urban infrastructure that is plagued by gentrification and lack of affordable housing for many? The ongoing case of Google's smart city project in Toronto highlights these questions and the rights that are at stake (Wakefield 2020). The project led The Guardian (2018) to ask: "Is Google's future the one that the rest of us want?" While stakeholder groups were consulted in Toronto, conflicts broke out over human rights issues such as privacy and free, prior, and informed consent in the decision-making process over this alleged "smart city of surveillance" (Kofman 2018). Instead of allowing profit-driven stakeholders to dominate the conversation about smart cities, a better way to frame this entire debate is to ask what a "smart enough city" might look like if all stakeholder groups actually had their say in the design process (Green 2019). The Toronto case is thus an excellent predictor of conflicts between economic interests and human rights yet to come to many other parts of the globe.

3.3 Privacy and Health

Insurance companies are under increasing competitive pressure. Thus, managers often decide to mine customers' data at ever more granular levels in order to be able to offer better premiums and services. While many insurance customers do not seem to mind sacrificing their privacy rights in order to save some money, the real issue at hand is not merely a matter of consumer choice. Instead, trends in healthcare point to the fact that data from various sources will increasingly be combined and mined across individual services and companies, and even across sensitive databases run by governmental healthcare agencies. This trend threatens the privacy rights of citizens and non-citizens, such as refugees, with regard to some of their most sensitive and intimate data, for instance by way of workplace wellness programs that might leak data (Ajunwa 2017). This might ultimately affect the right to health when individuals are deprived of healthcare access altogether, as they might not be able to afford the premium for the risk group into which a data-driven system has put them. This might put vulnerable groups at risk, such as people with disabilities. Depending on national laws on access to health insurance, they might even be denied access to health coverage altogether due to overly broad diagnostic information, such as DNA testing (Raso et al. 2018).

3.4 Labor and the Gig Economy

Platforms such as ride sharing platform Uber, accommodation sharing marketplace AirBnB, or Amazon Mechanical Turk (AMT), a crowdsourcing market place for microtask labor, present themselves as convenient options for workers to generate some additional income in their spare time. However, they have been heavily criticized for a wide range of reasons (Chandler & Fuchs 2019). For instance, microtask labor for platforms like AMT takes a psychological toll (Geuss 2018), and jobs such as content moderation on social networks are particularly harsh on employees' mental health (Chen 2014). When it comes to gig economy labor for companies such as Uber, criticism includes the fact that these companies take advantage of weakened labor standards and protections or lack of support for people with disabilities, often by outsourcing remote labor to jurisdictions that are less strictly regulated, that they do not act responsibly when it comes to protecting their workers, that they do not pay benefits, that they limit workers' freedom of association, and that they even flat-out deny being employers in the first place, instead insisting that they are merely platforms which facilitate contact between independent agents and their clients (Farivar 2017; Scholz 2017; Graham 2019). Data-driven business models governing labor thus threaten to shrink workers' rights to collective bargaining or other forms of collective action by fragmenting the collective labor force into individual workers framed as being "self-employed," independent contractors.

3.5 Workplace Monitoring and Worker Surveillance

Contrary to popular belief, it is not only modern gig economy platforms that monitor their employees on a minute-by-minute basis. Instead, corporate surveillance has a long history at call centers and in other service industries, such as UPS package delivery services or Amazon warehouses, as observation has been an important factor in managing any business since the early 20th century (Bernstein 2017). The accelerated data economy now puts new pressures on traditional companies to monitor all of their employees in the workplace, moving the object of surveillance from "blue-collar" workers to "white-collar" office employees, and increasingly affecting "thinking work" (Kellogg, Valentine & Christin 2020). For instance, banks in the City of London need to determine how many of their offices are actually being used so that they can save rent on superfluous office space, and one way of getting data on this issue is to place surveillance technology in their offices to see whether employees are present or not (Morris, Griffin & Gower 2017). Moreover, technologies such as natural language processing and sentiment analysis can be used to determine employees' mood and predict their willingness to exert a task or to leave the company (Waddell 2016). And increasingly, companies will use more invasive methods of surveillance, such as microchip implants that connect employees to the company network (Astor 2017). This raises a wide range of human rights issues, including privacy and dignity.

3.6 Recruiting and Algorithmic Bias

Algorithmically reinforced biases such as racist and gender-related stereotypes are a major issue when it comes to human resources (HR) software. As everyone agrees that human decisions in organizations are likely to be biased, the need for objective decisions when it comes to hiring and promoting employees seems obvious. However, it turns out that algorithmic HR decisions can be just as biased as human ones, either because the historical data that algorithms are being trained on is deeply biased (DeBrusk 2018) or because the data and models being used are driven by a manager's agenda. Therefore, HR algorithms often recreate the biases found in the data that they were trained on (Raso et al. 2018). This means that instead of blindly trusting supposedly objective technologies, human beings need to address the underlying fundamental social problems such as racism and gender discrimination if they do not wish to perpetuate them by way of technology (O'Neil 2016; Prassl 2018).

3.7 Credit Scoring

Just like the above-mentioned forms of predictive machine learning, credit scoring sounds fair and transparent in theory, yet in practice turns out to be problematic from a business and human rights perspective. Even in the unlikely scenario that affected individuals were to participate in stakeholder engagement and consent to the processing of their data, part of the problem is biased training data, which could mean that an individual belonging to a group of people whose credit scores have historically been low might also get a low credit score not because of her own doing, but because of the overall performance of said group (O'Neil 2016). Individualized credit scoring promises a solution to this discriminatory logic, but it introduces new problems (Raso et al. 2018). For instance, if individuals are scored on their individual financial performance alone instead of being classified into risk groups for mathematical models, it seems likely that credit lines become unobtainable for a large portion of the population. This issue thus turns out to be a social and political challenge, as society needs to address difficult questions not just around individual privacy, but also around wealth distribution, participation in economic activity, and distributive justice. Lastly, when it comes to stakeholder engagement, how would a company ensure access to remedy if the credit scoring process is a "black box" based on a non-transparent technology, such as neural networks (Pasquale 2015)?

3.8 Targeted Data Profiling of Human Rights Defenders

Just a few years ago, social network sites such as Facebook and Twitter were praised as a liberation technology during the relatively peaceful political uprisings in countries such as Egypt (Diamond 2010; Busch & Shepherd 2014). In recent years, however, those same platforms have become a severe threat to activists and human rights defenders because their policies and design decisions can endanger activists (Choudry 2018). As a result, the "technology of repression" narrative emerged (Lynch 2011). For instance, Facebook's strict policing of its real-name policy and its group communication tools create privacy issues that make activists easy targets for police forces in oppressive regimes (MacKinnon 2012). In recent years, Silicon Valley companies have frequently demonstrated a thorough lack of understanding of how their platforms are being used internationally by a diverse range of actors that are not merely consumers in the Western sense (Tufekci 2017), such as authoritative governments requesting user data from companies (Ebert 2019). This presents a real threat to these allegedly atypical users, and the difficulties that companies like Facebook demonstrate when it comes to managing such situations point to a wide range of social, cultural, and political factors that are at play in this context (Tufekci 2018).

3.9 Predictive Policing

On paper, predictive policing seems like an excellent idea: After all, police forces are often understaffed, and data-driven policing could potentially lead to a more effective and efficient use of limited public resources (Access Now 2018a). However, as good as the idea might sound in theory, it does not work in practice. Criticism of this technology includes the fact that many software systems are black boxes produced by the private sector, and police have no transparency over the data collection and data analytics models being used to predict crime in any given community (Pasquale 2015). Moreover, racist bias often plays a role in the learning data used by predictive algorithms, which in turn increases the already problematic levels of racist bias in policing, especially in the US (AI Now 2019). Additionally, it is unclear who is ultimately to be held accountable for false outcomes of such a black-box system: the developer, the company or the police using it. A related issue is facial recognition used in law enforcement, which in the US is "unregulated and in many instances out of control" (Garvie, Bedoya & Frankle 2016).

3.10 Public-Private Partnerships in Law Enforcement

In 2016, Pro Publica reported on racist bias found in recidivism prediction software used by US judges (Angwin et al. 2016). This caused major public

outcry because algorithmic predictions might literally cost people their freedom. The case at hand centered on software used by US judges to help them make more accurate predictions about whether inmates should be granted parole based on whether they had a low or high likelihood of becoming an offender again. This type of recidivism prediction software turned out to be biased against blacks. From a human rights perspective, this case is highly relevant not just because of the obviously high stakes for each individual inmate, but also because it illustrates that public-private partnerships have increasingly become the norm in our justice systems, as private and public surveillance often go hand in hand (Bernal 2016). After all, it was a private-sector company that produced the software in question, and judges used it without knowing any details about how it worked and what kind of data it was based on. This raises serious concerns not only about the digital literacy skills of judges, but also about the purchasing decisions of justice departments. Similar to predictive policing, it is unclear who is to be held accountable: the developer, or the judge relying on a software solution (Access Now 2018a)?

3.11 Facial Recognition, Border Control and Drone Technology

On a similar note, public-private partnerships play an important role not only within the justice system, but also with respect to the increasingly widespread use of surveillance technologies in public contexts (Access Now 2018b). For instance, in a post-9/11 world, facial recognition software is now routinely used by many airports in order to perform background checks on travelers (Rudolph, Moy & Bedoya 2017). Moreover, major companies, such as Amazon, Google, and Microsoft, have been heavily criticized by both the media and their own employees for cooperating on morally questionable government projects, including facial recognition, border policing, and drone surveillance (Conger 2018; Wingfield 2018). Google employees, for instance, protested against both the company's complicity with censorship requirements in China and Project Maven, Google's machine learning algorithm that helps drones identify individuals for the US Department of Defense (Shane & Wakabayashi 2018). This is just one example of how employees at tech companies are now increasingly asking questions about the (mis-)uses of the products they are developing (Conger & Metz 2018). One reason for this is that many Western tech companies are directly or indirectly complicit in questionable government practices all across the globe, and many of these practices include obvious human rights violations. For instance, China uses DNA to track its people, with US companies providing technology for these practices (Wee 2019). Moreover, IBM was involved in building surveillance technology for Philippine authoritarian-ruling president Duterte (Joseph 2019). And given the fact that facial recognition is both a billion-dollar business and a tool for political control, China is now data-mining "African" faces to improve the accuracy of its algorithms (Hawkins 2018). In early 2020, based on information from a leaked white paper, the European Union was said to consider temporarily banning facial recognition in public spaces, acting in line with the recommendations by the Fundamental Rights Agency of the European Union (Euractiv 2020). However, the official white paper suggests otherwise, as the current EU approach appears to swing towards a risk-based approach, rather than prohibiting the use of certain technologies by default (European Commission 2020a). Meanwhile, the UK, as a future non-member of the EU, has recently launched a metropolitan police project in London that uses live facial recognition technology (Dodd 2020).

4 The Responsibility to Respect Human Rights in the Data Economy

The aforementioned new technologies and dynamics bear the potential to challenge conventional regulatory frameworks. Luckily, though, there are fundamental concepts that can be drawn upon from a business and human rights perspective. Thus far, privacy and freedom of speech have been the main issues that the telecommunications and tech sectors have been focusing on, governed mainly through bodies such as the Global Network Initiative (GNI), which tries to address human rights issues through a sector-specific multi-stakeholder approach. At the same time, there is a lack of approaches that address the fact that new technologies both connect and transcend traditional industrial sectors, thus creating wider systemic human rights issues beyond privacy and freedom of speech. Given the fact that the voluntary nature of corporate social responsibility (CSR) initiatives leaves a lot to be desired when it comes to the protection of human rights in the data economy, the following section investigates norms, guidelines, and frameworks that promise to provide paths towards a more hands-on, human rights-based approach in this context.

The corporate responsibility to respect human rights was laid down in the United Nations Guiding Principles on Business and Human Rights (UNGPs), as adopted by the United Nations Human Rights Council in 2011 (Alston 2005; Clapham 2006; Ruggie 2007, 2013; Wettstein 2015, 2016). Professor John Ruggie of Harvard University was appointed UN Special Representative of the Secretary-General on Human Rights and Transnational Corporations and Other Business Enterprises, and he embarked on a "fact finding mission" from 2005 to 2008 (UN Commission on Human Rights 2005). He led a global consultation process with relevant stakeholders (governments, business, civil society, trade unions, academics) that resulted in the Protect, Respect, Remedy Framework (Ruggie 2007, 2013). On the basis of this framework, the non-binding UNGPs emerged as a soft-law instrument (UN Human Rights Council 2011). The Guiding Principles are based on three pillars: the state duty to protect human rights, the corporate responsibility to respect human rights, and victims' access to effective remedy.

In line with the UNGPs, the duty to protect lies with the government, as formulated under pillar one, and is incorporated in international law. Companies, as described in pillar two, have the responsibility to respect human rights. Pillar two requires a company to carry out human rights due diligence throughout their operations as a continuous risk management process to identify, prevent, mitigate, and to be held accountable for addressing its human rights impacts. Pillars two and three in particular extend the traditional understanding of the state as the duty bearer to protect human rights under international law, and add the soft-law component of pillar two for businesses, and pillar three, access to remedy, that can be provided by judicial means by the state or by non-judicial means, such as company-level grievance mechanisms. The UNGPs can be applied not only throughout traditional corporate supply chains but also in the digital sphere (Samway 2016). With regard to the digital domain, for example, corporate actors must weigh their decisions on whether and which data to share very carefully to protect their users' privacy (Crawford & Schultz 2014). As a consequence, companies should perceive an increased awareness of the risks of human rights abuses, such as infringements of privacy.

In 2019, the Office of the High Commissioner for Human Rights carried out informal consultations with civil society, business, states, and other experts about its forthcoming project on Business and Human Rights in Technology (B-Tech). The project is set to focus on four areas: addressing human rights risks in business models, human

rights due diligence and end-use, accountability and remedy, and "a smart mix of measures" when it comes to exploring regulatory and policy responses to human rights challenges linked to digital technologies. According to the initial scoping paper, the project will entail conducting research, stakeholder consultations, and stakeholder-specific engagement sessions, along with an online portal (Office of the United Nations High Commissioner for Human Rights 2019). The B-Tech project aims at providing authoritative guidance and resources to enhance the quality of implementation of the UNGPs with respect to a selected number of strategic focus areas in the technology space.

In light of recent technological progress, it is of utmost importance to explore how business and human rights have become increasingly intertwined in the age of the data economy. In this context, bridging the many gaps between existing legal frameworks, social science approaches to the data economy, and the practical concerns of the "tech world" presents us with an enormous challenge. Against this background, how can we clarify what business and human rights mean in the "digital sphere"? In the following, we describe how the business and human rights lens could be adapted to include human rights risks that arise in the context of data-driven business conduct.

5 Ways Forward: Human Rights Due Diligence in the Data Economy

As argued in the previous chapter, the UNGPs remain the key framework for upholding human rights in the business realm. Their interpretation in the data economy needs to be implemented with the core demands from the original UNGPs in mind. Hence, policy demands should be in line with the UN Guiding Principles on Business and Human Rights, which state (UNGP 15):

> "In order to meet their responsibility to respect human rights, business enterprises should have in place policies and processes appropriate to their size and circumstances, including:
> (a) A policy commitment to meet their responsibility to respect human rights;
> (b) A human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights;
> (c) Processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute."

In order to ensure that business uphold its responsibility to respect human rights, the business and human rights lens proposes a human rights due diligence approach. Human rights due diligence, as both a management practice and ongoing process, offers a proactive, preventive approach towards human rights protection and stresses the importance to mitigate and remedy harm that has already occurred or is occurring currently. As it might not be possible to fully anticipate harmful effects of data-driven business before an impact has occurred, it is necessary to establish a continuous exchange among stakeholders and develop human rights due diligence as an on-going process with proper feedback loops. This also means that companies finding themselves in different positions within the value chain and development cycles of technology need to be part of these conversations. This applies not only to trans-national corporations but also to small and medium-sized enterprises, which need to be taken into account including their co-dependencies with larger players in the field.

Human rights due diligence builds upon a thorough human rights impact assessment. This assessment forms part of a due diligence process that is not static in nature. The UN Guiding Principles do not require that businesses conduct human rights impact assessments by using that exact terminology, but they indicate approaches that equal essential elements of a human rights impact assessment (Danish Institute for Human Rights 2016). This includes drawing on internal and/or independent human rights expertise, undertaking meaningful consultation with potentially affected rightsholders and other relevant parties. Attention should be paid to gender-sensitive language and a particular focus on any human rights impacts on individuals from groups that may be at heightened risk of vulnerability or marginalization. An assessment of impacts from the perspective of risk to people rather than risk to business, as well as repeated risk and impact identification and assessment at regular intervals is of high importance.

In the following sections, we describe how a company can enact human rights in a data economy business model, following a process of human rights due diligence as progressive company conduct that embraces a business and human rights lens in the data economy. It is important to note that there is no "one size fits all" approach, and each business needs to tailor its human rights due diligence process to its individual business model and respective socio-political context. As stressed previously, besides potential bias from data models, external stakeholder engagement is essential, yet it can be a challenging undertaking: How do businesses actually engage users or affected individuals? Can user testing sufficiently identify proxies? The following section addresses these questions, among others.

5.1 Identifying and Assessing Human Rights Impacts: Policy Commitment, Data Collection and Baseline Development

A solid understanding of the technological state of the art and its potential from a technical perspective is necessary in order to formulate effective policy demands from a business and human rights perspective. It is important to engage with a wide variety of different audiences to understand the full human rights footprint of a company. In many ways, decisions are not necessarily either right or wrong; instead they may be well-informed or ill-informed. For instance, one would assume that a tech company such as Google might take into account the rights of both its full-time employees as well as those of its contractors; this seems quite obvious due to the fact that both groups are staff operating on the premises. However, this does not yet always happen in practice because the company seems to be unaware that all of its hiring and recruiting processes need to be aligned with business and human rights. This holds true for many issues, such as bias in recruiting algorithms (see also the section on hiring, recruiting and algorithmic bias) and issues that were raised during the Google walkout, such as allegations of sexual misconduct by managers in the workplace, and broader representation of labor in the company's decision-making processes (Scheiber 2018). In the data economy, human rights due diligence increasingly also has to take product- and technology-focused human rights impact assessments into account in order to develop a better understanding of the policies, processes, and practices that different actors across the supply chain can use to mitigate and remediate adverse impacts.

An impact assessment could touch upon:

- high-risk markets or end-use by user/user groups (women, children, different political and cultural contexts) and possible unintended consequences
- consultation and involvement of users and affected stakeholder groups in the design and testing of data models or data-driven products
- identification of potential human rights risks and their severity in terms of risk to people (e.g. number of impacted users, seriousness of impact on the affected individual)

Companies in the data economy need to aim at fully grasping the human rights impact of their business. Key questions are: Who are the vulnerable groups affected by business operations and how, exactly, are they affected by business operations? To stick with the example of recruiting, a company should ensure that recruiting algorithms do not discriminate against vulnerable groups, such as women or people of color. Moreover, it needs to pay attention to its products' effects on privacy, including aspects such as user tracking through its apps, and whether it sells this data to third parties. This would help prevent problems such as "stalking apps" that endanger women (Brownlee 2012) or apps that record users' mobile phone screens without information or consent (Whittaker 2019).

5.2 Acting on the Findings: Identify Existing Processes and Potential Gaps

In this step, the business assesses whatever measures it already has in place, e.g. on privacy and data protection, and where gaps exist with regard to human rights protection. Some companies might follow a "privacy by design" ethos to address emerging privacy issues, for instance. Some authors point out that human rights by design could be an opportunity to incorporate human rights considerations into existing processes, in addition to other measures (Allison-Hope 2018). However, companies generally need to tread carefully, as human rights can only ever be protected to a certain extent by technical safeguards built into the settings and interfaces of new technologies. In many cases, tech companies tend to navigate unknown waters when it comes to technology in a business and human rights context, which is exacerbated further by legal liability issues.

Thus, in order to mitigate risks for both themselves and their stakeholders, companies should develop adequate avenues for engagement with rightsholders. BSR (2014) proposes eight princi-

ples for engagement with rightsholders, including being timely, inclusive to vulnerable groups, focused on relevant rights issues, and committed to the safety of all participants. Companies should also include relevant intermediary stakeholders in human rights discussions, for example local community members who represent their community's needs. In the data economy, one example could be the case of targeted advertising. Companies such as Facebook, including Instagram, analyze users' preferences in order to show them the most appealing adverts. One gap in the human rights impact assessment could be that this information about user preferences might reveal certain traits that should not be used for abusive practices. For instance, if a user preference profile might indicate that a person belongs to the LGBTI community, this can be very dangerous information in states where LGBTI people face oppression, prison time, or violence from either government actors or radical political groups. It thus becomes evident that the human rights due diligence process in the data economy needs more technology expertise than in a traditional one.

These questions demonstrate that human rights due diligence in the data economy requires more and more cross-functional collaboration to integrate rightsholder perspectives. Departments such as legal, procurement, human resources, public affairs, engineering, research and development, and data science might have to collaborate to find solutions. Ideally, this practice results in the erasure of blindspots and fosters preventive human rights due diligence approaches.

5.3 Impact Mitigation and Management: Prioritize Measures and Agree on Next Steps

This step is crucial for any business, but even more so for global data economy businesses due to their extensive scale and scope. The salience of risk to people should be a key priority (Global Reporting Initiative 2015). The prioritization step allows data businesses to focus on key questions of preventing, mitigating, and remedying the most salient impacts on rightsholders, such as: Where does the business have leverage to change behavior in order to avoid adverse effects on rightsholders? Where does the business need to form alliances with other businesses to change practices within data economy industries, such as adverse effects of targeted advertising? Where is the business unlikely to have leverage to change impacts on human rights? Can the company abandon certain business operations with adverse human rights impact in cases where it does not have leverage and find substitutes instead?

Lead questions could include the following:

- company-level mitigation measures (e.g., policies, controls) already in place and potential additional mitigation measures
- exchange within industry: companies that have released similar products or services share their experiences with arising human rights risks from product use and mitigatory management
- global policy implications: variation of risks, opportunities, and mitigation measures between different markets and countries, adaptation to local context

Examples in the tech sector include situations in which a company may find itself operating in a non-democratic country where international human rights and local laws are in conflict with one another. It might thus seek to form alliances with other affected businesses to speak out against restrictive government behavior on freedom of expression and identify ways forward with industry allies. Important cases in this context include the aforementioned Global Network Initiative (GNI) and, with respect to emerging technologies such as AI and machine learning, the Toronto Declaration (2018). It is important to note that for any international company, the prioritization of human rights risks needs to be in line with the UN Guiding Principles on Business and Human Rights, meaning that while all human rights are equal, the most severely affected rights need to be addressed and acted upon first (salient human rights issues). This also raises an important point regarding the vital role of professional codes of conduct and ethical guidelines across industries, e.g. for software engineers (see the sections on the ACM and IEEE in the annex): Addressing human rights due diligence

in tech requires every employee to have an understanding of both the technical and the human rights side of the issue. This is because isolated silos of tech-minded employees on the one hand and corporate CSR or legal departments on the other will not be able to address salient human rights issues in a holistic manner.

5.4 Reporting, Evaluation and Remedy: Anchor Human Rights Due Diligence in Business Practice to Enable Organizational Learning

In order to anchor human rights due diligence in everyday business practices, a data economy company needs to find ways to make the entire organization care about reporting, evaluating, and learning about its human rights impacts. This requires establishing a feedback loop to learn from past mistakes and improve business practices. It should also involve the integration of preventive and remedial mechanisms to deal with actual and potential human rights impacts.

This means that the company should offer company-level grievance mechanisms when violations result from decisions made by machines or algorithms, rather than humans. Such violations are often difficult to explain and may even be beyond the cognitive ability of human beings to understand. On a larger scale, this also implies that a company should ensure access to remedy when many companies, rather than just one single company, are linked to a human rights abuse through the interaction of different products and services – for example, developers, suppliers, and operators of AI solutions. It will be challenging to identify the principle actor in a violation and to determine who is thus accountable for remedy in the event of harm – for example, between the creator of an algorithm, the designer of the overall system, or the customer making use of it (Allison-Hope 2018).

The business and human rights community as a whole is currently in the midst of figuring out what access to remedy ought to look like in the machine age, and how innovations and new management approaches need to be designed to uphold human rights in the data economy. What should an operational grievance mechanism look like in this space? What would be a rights-respecting remedy? Different environments will require context-specific due diligence measures for remedy, and perhaps a patching and learning experience in cycles based on real-life experiences of how services are being used.

One current example: In order to make its governance and decision-making processes more transparent, Facebook has recently established an oversight board, with the bylaws being released in January 2020 (Facebook 2020, see also more on Facebook in the annex). It is to be welcomed that this body underwent a human rights review and is committed to taking the UNGPs into consideration in its decision-making processes (BSR 2020). As a result, ideally, impacts on all human rights, and not only freedom of expression as well as personal safety and security, can be taken into account by content decisions made by Facebook and its oversight board. Critics have pointed out an increased need for transparency reporting about the disclosure of cases by which community standards were violated, cases clustered by format or content at issue (e.g., text, image, video, livestream), number of accounts and pieces of content covered by the cases considered by the board, and number of accounts/pieces of content taken down or otherwise actioned as a result of a board. Other improvements called for by civil society are increased transparency about the nomination of board members, relationship between Facebook, the trust of the oversight board, and the oversight board itself, as well as government orders that threaten human rights (Ranking Digital Rights 2020). Summing up, the degree of independence of the oversight board, along with its efficacy, is yet to be seen in practice. It could at the same time provide strategic insights into how accountability structures need to be set up in order to be provide effective remedy for rightsholders.

However, one crucial aspect is clear at this point already, which is that tech companies, both individually and collectively, need to find answers to the question of who is to be held accountable for adverse impacts on human rights caused by technology. This cannot happen in a vacuum but rather needs to take into account a wide range of aspects, including affected stakeholders' needs, civil society and public policy recommendations, as well as regulatory frameworks.

6 Concluding Remarks

Summing up the findings of this analysis, we have shown several positive developments, such as the plethora of guidelines, codices, and reports on human rights and technology that are available already (see also Jobin, Ienca & Vayena 2019; Fjeld et al. 2020). Many of the materials detailed in this analysis and its annex provide useful guidance and orientation regarding what human rights due diligence in the data economy could look like. On a somewhat more pessimistic note, however, it also has become abundantly clear that many of the existing guidelines are vague and lacking in context- and industry-specific guidance. It would thus be beneficial for the business and human rights community as a whole to develop more case-specific assessment tools and share lessons learned as they emerge. Guidance materials need to be tested in full practice, as complex scenarios are hard to predict and cannot be sufficiently anticipated.

As this analysis has shown, when it comes to upholding the human rights responsibilities of companies in the data economy, it is not enough to hide behind technological black boxes and to merely blame anonymous algorithms every time things go wrong (Angwin 2016). Instead, companies should follow a proactive approach by working with technological solutions while at the same time reflecting upon their potential adverse effects on human rights, using human rights due diligence management practices, and consulting with a wide range of affected stakeholders about the interplay between tech solutions and actual human beings.

As Powles & Nissenbaum (2018) point out, many of the challenges posed by technologies such as AI and machine learning need societal checks and balances, and they may eventually need to be regulated thoroughly rather than just voluntarily:

> "Which systems really deserve to be built? Which problems most need to be tackled? Who is best placed to build them? And who decides? We need genuine accountability mechanisms, external to companies and accessible to populations. Any A.I. system that is integrated into people's lives must be capable of contest, account, and redress to citizens and representatives of the public interest. And there must always be the possibility to stop the use of automated systems with appreciable societal costs, just as there is with every other kind of technology."

In the meantime, however, while we build upon the useful suggestions made by voluntary initiatives, we should ask those questions that really address the broader political, economic, and cultural implications of technology, and not merely its technical aspects.

7 References

Access Now (2018): Human rights in the age of AI. A case study examining law enforcement use of AI-powered facial recognition. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights-Case-Study.pdf (access: 09.04.2020)

ACM (1992): ACM Code of Ethics and Professional Conduct. https://ethics.acm.org/code-of-ethics/ (access: 09.04.2020)

Access Now (2018): Human rights in the age of artificial intelligence. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf (access: 09.04.2020)

ACM (2018): ACM Code of Ethics and Professional Conduct. https://www.acm.org/code-of-ethics (access: 09.04.2020)

ACM (2019): Association for Computing Machinery: About Us. https://www.acm.org/about-acm (access: 09.04.2020)

ACM SIGCAS (2020): ACM Special Interest Group Computers & Society. http://www.sigcas.org/about-sigcas/ (access: 09.04.2020)

AI Ethics Initiative (2019): The Ethics and Governance of AI Initiative. https://aiethicsinitiative.org/ (access: 09.04.2020)

AI HLEG (2018): Draft ethics guidelines for trustworthy AI. European Commission High-Level Expert Group on AI, December 18. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57112 (access: 09.04.2020)

AI HLEG (2019): Ethics guidelines for trustworthy AI. European Commission High-Level Expert Group on AI, April 8. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 (access: 09.04.2020)

AI Now (2018): After a Year of Tech Scandals, Our 10 Recommendations for AI. https://medium.com/@AINowInstitute/after-a-year-of-tech-scandals-our-10-recommendations-for-ai-95b3b2c5e5 (access: 09.04.2020)

AI Now (2019): Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. New York University Law Review Online. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423 (access: 09.04.2020)

Ajunwa, Ifeoma (2017): Workplace Wellness Programs Could Be Putting Your Health Data at Risk. In: Havard Business Review 2017 (01). https://hbr.org/2017/01/workplace-wellness-programs-could-be-putting-your-health-data-at-risk (access: 09.04.2020)

Algorithmic Justice League (2019). https://www.ajlunited.org/ (access: 09.04.2020)

Allison-Hope, Dunstan / Hodge, Mark (2018): Artificial Intelligence. A Rights-Based Blueprint for Business. Papers 1-3. https://www.bsr.org/en/our-insights/report-view/artificial-intelligence-a-rights-based-blueprint-for-busines (access: 09.04.2020)

Amnesty International (2019): Surveillance giants: How the business model of Google and Facebook threatens human rights. London. https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF (access: 09.04.2020)

Andersen, Lindsey (2018): Human rights matter in the AI debate. Let's make sure AI does us more good than harm. Access Now, November 8. https://www.accessnow.org/human-rights-matter-in-the-ai-debate-lets-make-sure-ai-does-us-more-good-than-harm/ (access: 10.04.2020)

Angwin, Julia (2016): Make algorithms accountable. In: The New York Times, 01.08.2016. https://www.nytimes.com/2016/08/01/opinion/make-algorithms-accountable.html (access: 10.04.2020)

Angwin, Julia et al. (2016): Machine bias. There's software used across the country to predict future criminals. And it's biased against blacks. Pro Publica, May 23. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (access: 10.04.2020)

Article 19 / Privacy International (2018): Privacy and Freedom of Expression in the Age of Artificial Intelligence. London. https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf (access: 10.04.2020)

Asher-Shapiro, Avi (2019): Move Fast and Build Solidarity Activism at Google and Amazon paid off. But can the emerging "tech left" forge long-term alliances between janitors, drivers, and engineers? In: The Nation, 06.03.2019. https://www.thenation.com/article/tech-workers-google-facebook-protest-dsa/ (access: 10.04.2020)

Astor, Maggie (2017): Microchip Implants for Employees? One Company Says Yes. In: The New York Times, 25.07.2017. https://www.nytimes.com/2017/07/25/technology/microchips-wisconsin-company-employees.html (access: 10.04.2020)

Australian Human Rights Commission & World Economic Forum (2019): Artificial Intelligence: governance and leadership. https://tech.humanrights.gov.au/sites/default/files/2019-02/AHRC_WEF_AI_WhitePaper2019.pdf (access: 10.04.2020)

Awad, Edmond et al. (2018): The moral machine experiment. In: Nature 563, pp. 59–64

Banisar, David / Davies, Simon (1999): Global trends in privacy protection. An international survey of privacy, data protection, and surveillance laws and developments. In: The John Marshall Journal of Information Technology and Privacy Law 18 (1), pp. 1–112

Barbrook, Richard / Cameron, Andy (1996): The Californian Ideology. In: Science as Culture 6 (1), pp. 44–72

Barney, Darin et al. (eds.) (2016): The Participatory Condition in the Digital Age. Minnesota: University of Minnesota Press

Baumann-Pauly, Dorothée/Nolan, Justine (eds.) (2016): Business and human rights. From principles to practice. New York: Routledge

Bayamlioglu, Emre et al. (eds.) (2018): Being Profiled: Cogitas Ergo Sum. 10 Years of Profiling the European Citizen. Amsterdam: Amsterdam University Press

Bennett, Colin J. (1992): Regulating privacy. Data protection and public policy in Europe and the United States. Ithaca: Cornell University Press

Beras, Erika (2018): When AI misclassified her face, she started a movement for accountability. MIT Technology Review 35 Innovators Under 35. 2018 edition. https://www.technologyreview.com/lists/innovators-under-35/2018/pioneer/joy-buolamwini/ (access: 10.04.2020)

Bergmann, Lasse T. et al. (2018): Autonomous Vehicles Require Socio-Political Acceptance–An Empirical and Philosophical Perspective on the Problem of Moral Decision Making. In: Frontiers in Behavioral Neuroscience 12 (31), pp. 1–12

Bernal, Paul (2016): Data gathering, surveillance and human rights. Recasting the debate. In: Journal of Cyber Policy 1 (2), pp. 243–264

Bernstein, Ethan S. (2017): Making Transparency Transparent. The Evolution of Observation in Management Theory. In: Academy of Management Annals 11 (1), pp. 217–266

Boyd, Danah / Crawford, Kate (2012): Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. In: Information, communication & society 15 (5), pp. 662–679

Brooks, David (2017): How Evil Is Tech? In: The New York Times, 20.11.2017. https://www.nytimes.com/2017/11/20/opinion/how-evil-is-tech.html (access: 10.04.2020)

Brownlee, John (2012): This Creepy App Isn't Just Stalking Women Without Their Knowledge, It's A Wake-Up Call About Facebook Privacy [Update]. https://www.cultofmac.com/157641/this-creepy-app-isnt-just-stalking-women-without-their-knowledge-its-a-wake-up-call-about-facebook-privacy/ (access: 10.04.2020)

BSR – Business for Social Responsibility (2012): Applying the Guiding Principles on Business and Human Rights to the ICT Industry. Version 2.0. Ten Lessons Learned. San Francisco. https://www.bsr.org/reports/BSR_Guiding_Principles_and_ICT_2.0.pdf (access: 10.04.2020)

BSR – Business for Social Responsibility (2014): Legitimate and Meaningful: Stakeholder Engagement in Human Rights Due Diligence. San Francisco. https://www.bsr.org/en/our-insights/report-view/engaging-with-rights-holders (access: 10.04.2020)

BSR – Business for Social Responsibility (2020): A Human Rights Review of the Facebook Oversight Board. Blog post, December 12. https://www.bsr.org/en/our-insights/blog-view/a-human-rights-review-of-the-facebook-oversight-board (access: 10.04.2020)

Buolamwini, Joy (2018): When the Robot Doesn't See Dark Skin. In: The New York Times, 21.06.2018. https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html (access: 10.04.2020)

Busch, Thorsten / Shepherd, Tamara (2014): Doing well by doing good? Normative tensions underlying Twitter's corporate social responsibility ethos. In: Convergence 20 (3), pp. 293–315

Business and Human Rights Resource Centre (2020). https://www.business-humanrights.org/ (access: 10.04.2020)

Byrne, Ciara (2019): Trading privacy for survival is another tax on the poor. In: Fast Company, 18.03.2019. https://www.fastcompany.com/90317495/another-tax-on-the-poor-surrendering-privacy-for-survival (access: 10.04.2020)

Carlson, Nicholas (2010): At last – the full story of how Facebook was founded. In: Business Insider, 05.03.2010. https://www.businessinsider.de/how-facebook-was-founded-2010-3?op=1 (access: 10.04.2020)

Cath-Speth, Corinne / Kaltheuner, Frederike (2020): Risking everything: where the EU's white paper on AI falls short. In: New Statesman, 03.03.2020. https://tech.newstatesman.com/guest-opinion/eu-white-paper-on-artificial-intelligence-falls-short (access: 10.04.2020)

Chakravorti, Bhaskar (2019): Facebook's fake pivot to Privacy. Forbes, March 11. https://www.forbes.com/sites/bhaskarchakravorti/2019/03/11/facebooks-fake-pivot-to-privacy/ (access: 10.04.2020)

Chan, Tara (2018): These Chinese Workers' Brain Waves are Being Monitored. World Economic Forum, May 1. https://www.weforum.org/agenda/2018/05/china-is-monitoring-employees-brain-waves-and-emotions-and-the-technology-boosted-one-companys-profits-by-315-million/ (access: 10.04.2020)

Chandler, David / Fuchs, Christian (eds.) (2019): Digital Objects, Digital Subjects. Interdisciplinary perspectives on capitalism, labour and politics in the age of Big Data. London: University of Westminster Press

Chee, Florence M. (2018): An Uber ethical dilemma. Examining the social issues at stake. In: Journal of Information, Communication and Ethics in Society 16 (3), pp. 261–274

Chen, Adrian (2014): The Laborers Who Keep Dick Pics and Beheadings Out of Your Facebook Feed. In: Wired, 23.10.2014. https://www.wired.com/2014/10/content-moderation/ (access: 10.04.2020)

Choudry, Aziz (2019): Activists and the surveillance state. Learning from repression. London: Pluto Press

Christl, Wolfie / Kopp, Katharina / Riechert, Patrick U. (2017a): Corporate surveillance in everyday life. How companies collect, combine, analyze, trade and use personal data on billions. Working Paper. Vienna: Cracked Labs - Institute for Critical Digital Culture

Christl, Wolfie / Kopp, Katharina / Riechert, Patrick U. (2017b): How Companies Use Personal Data Against People. Automated disadvantage, personalized persuasion, and the societal ramifications of the commercial use of personal information. Vienna: Cracked Labs – Institute for Critical Digital Culture

Cifor, Marika et al. (2019): Feminist Data Manifest-No. https://www.manifestno.com/ (access: 10.04.2020)

Clapham, Andrew (2006): Human rights obligations of non-state actors. Oxford: Oxford University Press

Cohen, Julie E. (2016): The surveillance-innovation complex. The irony of the participatory turn. In: Barney, Darin et al. (eds.): The Participatory Condition in the Digital Age. Minnesota: University of Minnesota Press

Cohen, Noam (2017): Silicon Valley is not your friend. In: The New York Times, 13.10.2017.https://www.nytimes.com/interactive/2017/10/13/opinion/sunday/Silicon-Valley-Is-Not-Your-Friend.html (access: 10.04.2020)

Collett, Clementine / Dillon, Sarah (2019): AI and Gender. Four Proposals for Future Research. Cambridge. http://lcfi.ac.uk/media/uploads/files/AI_and_Gender___4_Proposals_for_Future_Research.pdf (access: 10.04.2020)

Confessore, Nicholas (2018): Cambridge Analytica and Facebook. The Scandal and the Fallout So Far. In: The New York Times, 04.04.2018. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (access: 10.04.2020)

Conger, Kate (2018): Amazon Workers Demand Jeff Bezos Cancel Face Recognition Contracts With Law Enforcement. In: Gizmondo, 21.06.2018. https://gizmodo.com/amazon-workers-demand-jeff-bezos-cancel-face-recognitio-1827037509 (access: 10.04.2020)

Conger, Kate / Metz, Cade (2018): Tech Workers Now Want to Know. What Are We Building This For? In: The New York Times, 07.10.2018. https://www.nytimes.com/2018/10/07/technology/tech-workers-ask-censorship-surveillance.html (access: 10.04.2020)

Continental (2020): Automated driving. https://www.continental.com/en/products-and-innovation/innovation/automated-driving/automated-driving-10556 (access: 10.04.2020)

Costanza-Chock, Sasha (2020): Design Justice. Community-Led Practices to Build the Worlds We Need. Cambridge/MA: MIT Press

Costanza-Chock, Sasha et al. (2018): #More than Code. Practitioners reimagine the landscape of technology for justice and equity. https://morethancode.cc/T4SJ_fullreport_082018_AY_web.pdf (access: 10.04.2020)

Couldry, Nick / Mejias, Ulises A. (2019): Data Colonialism. Rethinking Big Data's Relation to the Contemporary Subject. In: Television & New Media 20 (4), pp. 336–349

Council of Europe (1950): Convention for the Protection of Human Rights and Fundamental Freedoms, CoE Doc. ETS 005

Council of Europe (2018): Algorithms and human rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications. Council of Europe study DGI(2017)12. Prepared by the

Committee of Experts on Internet Intermediaries (MSI-NET). Strasbourg. https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory- implications.html (access: 10.04.2020)

Council of Europe (2019): Responsibility and AI. A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework. Council of Europe study DGI(2019)05. Prepared by the Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT). Strasbourg. https://rm.coe.int/responsability-and-ai-en/168097d9c5 (access: 10.04.2020)

Council of Europe, MSI-AUT (2018): Draft Recommendation of the Committee of Ministers to member States on human rights impacts of algorithmic systems. Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT). November 12. Strasbourg, EU Doc. MSI-AUT(2018)06. https://rm.coe.int/draft-recommendation-on-human-rights-impacts-of-algorithmic-systems/16808ef256 (access: 13.04.2020)

Courtland, Rachel (2018): Bias detectives. The researchers striving to make algorithms fair. In: Nature 558 (7710), pp. 357–360

Crawford, Kate (2013): The hidden biases in big data. In: Havard Business Review 2013 (1). https://hbr.org/2013/04/the-hidden-biases-in-big-data (access: 10.04.2020)

Crawford, Kate / Schultz, Jason (2014): Big data and due process. Toward a framework to redress predictive privacy harms. In: Boston College Law Review 55 (1), pp. 93–128

Criado Perez, C. (2019): Invisible Women. Exposing Data Bias in a World Designed for Men. New York City: Vintage Publishing

Cukier, Kenneth / Mayer-Schoenberger, Viktor (2013): The rise of big data. How it's changing the way we think about the world. In: Foreign Affairs 92, pp. 28–40

Dand, M. (2018): 100 Brilliant Women in AI Ethics to Follow in 2019 and beyond. Blog post, October 29. https://becominghuman.ai/100-brilliant-women-in-ai-ethics-to-follow-in-2019-and-beyond-92f467aa6232 (access: 10.04.2020)

Danezis, George et al. (2015): Privacy and Data Protection by Design – from policy to engineering. http://arxiv.org/pdf/1501.03726v2 (access: 10.04.2020)

Danish Institute for Human Rights (2016): Human rights impact assessment. Guidance and toolbox. Copenhagen. https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/business/hria_toolbox/hria_guidance_and_toolbox_final_may22016.pdf_223795_1_1.pdf (access: 10.04.2020)

Däubler, Wolfgang et al. (eds.) (2018): EU-Datenschutz-Grundverordnung und BDSG-neu. Kompaktkommentar. Frankfurt am Main: Bund-Verlag

DeBrusk, Chris (2018): The Risk of Machine-Learning Bias (and How to Prevent It). In: MIT Sloan Management Review 2018 (March 26). https://sloanreview.mit.edu/article/the-risk-of-machine-learning-bias-and-how-to-prevent-it/ (access: 10.04.2020)

Deibert, Ronald J. (2019): The Road to Digital Unfreedom. Three Painful Truths About Social Media. In: Journal of Democracy 30 (1), pp. 25–39

Dencik, L. / Jansen, Fieke / Metcalfe, Philippa (2018): A conceptual framework for approaching social justice in an age of datafication. Data Justice Project, August 30. https://datajusticeproject.net/2018/08/30/a-conceptual-framework-for-approaching-social-justice-in-an-age-of-datafication/ (access: 13.04.2020)

Diamond, Larry (2015): Liberation technology. In: Diamond, Larry and Plattner, Marc F. (eds.): Liberation Technology. Social Media and the Struggle for Democracy. Baltimore: The Johns Hopkins University Press, pp. 3–17

Diamond, Larry / Plattner, Marc F. (eds.) (2015): Liberation Technology. Social Media and the Struggle for Democracy. Baltimore: The Johns Hopkins University Press

Dodd, Vikram (2020): Met police to begin using live facial recognition cameras in London. In: The Guardian, 24.01.2020. https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras (access: 13.04.2020)

Ebert, Isabel (2019): The Tech Company Dilemma. Ethical Managerial Practice in Dealing with Government Data Requests. In: Zeitschrift für Wirtschafts- und Unternehmensethik 20 (2), pp. 264–275

Editorial (2018): The Guardian view on Google and Toronto. Smart city, dumb deal. In: The Guardian, 05.02.2018. https://www.theguardian.com/commentisfree/2018/feb/05/the-guardian-view-on-google-and-toronto-smart-city-dumb-deal (access: 13.04.2020)

Elish, Madeleine C. / Boyd, Danah (2018): Don't Believe Every AI You See. The Ethical Machine blog, November 13. https://ai.shorensteincenter.org/ideas/2018/11/12/dont-believe-every-ai-you-see-1 (access: 13.04.2020)

Epstein, Greg (2019): Silicon Valley's inequality machine. A conversation with Anand Giridharadas. Inequality, tech as religion, billionaire identity politics, and Winners Take All. Tech Crunch, March 2. https://techcrunch.com/2019/03/02/silicon-valleys-inequality-machine-anand-giridharadas/ (access: 13.04.2020)

EQUALS (2019): About Us. https://www.equals.org/about-us (access: 13.04.2020)

EU, European Commission (2019): Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising. Brussels, press release of 20 March 2019. http://europa.eu/rapid/press-release_IP-19-1770_en.htm (access: 13.04.2020)

EU, European Commission (2020): A European strategy for data. COM(2020) 66 final. Brussels, February 19. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf (access: 13.04.2020)

EU, European Commission (2020a): White Paper. On Artificial Intelligence – A European approach to excellence and trust. COM(2020) 65 final. Brussels, February 19. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (access: 13.04.2020)

EU, European Commission (2020b): Shaping Europe's digital future. Brussels, February 19. https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf (access: 13.04.2020)

European Commission (2020c). A European strategy for data. COM (2020) 66 final. Brussels, February 19. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf (access: 13.04.2020)

EU, European Commission Directorate General for Competition (2017): Antitrust/Cartel Cases. 39740 Google Search (Shopping). http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740 (access: 13.04.2020)

EU, European Commission Directorate General for Competition (2018): Antitrust/cartel cases. Google Android. http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_40099 (access: 13.04.2020)

EU, European Commission Directorate General for Competition (2019): Antitrust/cartel cases. 40411 Google Search (AdSense). http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_40411 (access: 13.04.2020)

EU, European Parliament and Council of the European Union: 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)., EU Doc. 2016/679. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679 (access: 13.04.2020)

Eubanks, Virginia (2018): A Hippocratic Oath for data science. Blog post, February 21. https://virginia-eubanks.com/2018/02/21/a-hippocratic-oath-for-data-science/ (access: 13.04.2020)

Euractiv (2020): Structure for the White Paper on artificial intelligence – a European approach. Leaked EU document draft. https://www.euractiv.com/wp-content/uploads/sites/2/2020/01/AI-white-paper-EURACTIV.pdf (access: 13.04.2020)

Facebook (2020): Preparing the Way Forward for Facebook's Oversight Board, press release of 28 January 2020. https://about.fb.com/news/2020/01/facebooks-oversight-board/ (access: 13.04.2020)

Farivar, Cyrus (2017): Uber really doesn't want its drivers to be considered employees. Ars Technica, September 21. https://arstechnica.com/tech-policy/2017/09/uber-really-doesnt-want-its-drivers-to-be-considered-employees/ (access: 13.04.2020)

Farrell, Henry / Levi, Margaret / O'Reilly, Tim (2018): Mark Zuckerberg runs a nation-state, and he's the king. Vox.com, April 10. https://www.vox.com/the-big-idea/2018/4/9/17214752/zuckerberg-facebook-power-regulation-data-privacy-control-political-theory-data-breach-king (access: 13.04.2020)

Fiesler, Casey (2018): What Our Tech Ethics Crisis Says About the State of Computer Science Education. If you work in tech and you're not thinking about ethics, you're bad at your job. Blog post, December 5. https://howwegettonext.com/what-our-tech-ethics-crisis-says-about-the-state-of-computer-science-education-a6a5544e1da6 (access: 13.04.2020)

Finlay, Steven (2014): Predictive Analytics, Data Mining and Big Data. Myths, Misconceptions and Methods. New York: Palgrave Macmillan

Fjeld, Jessica et al.: Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI. Berkman Klein Center for Internet & Society. http://nrs.harvard.edu/urn-3:HUL.InstRepos:42160420 (access: 13.04.2020)

Foot, Philippa (1967): The problem of abortion and the doctrine of double effect. In: Oxford Review 5, pp. 5–15

Frenkel, Sheera (2018): Microsoft Employees Protest Work With ICE, as Tech Industry Mobilizes Over Immigration. In: The New York Times, 19.06.2018. https://www.nytimes.com/2018/06/19/technology/tech-companies-immigration-border.html (access: 13.04.2020)

Garvie, Clare / Bedoya, Alvaro M. / Frankle, Jonathan (2016): The Perpetual Line-Up. Unregulated Police Face Recognition in America. Washington D.C. https://www.perpetuallineup.org/ (access: 13.04.2020)

Gasser, Urs / Almeida, Virgilio af (2017): A layered model for AI governance. In: IEEE Internet Computing 21 (6), pp. 58–62

Geuss, Megan (2018): Low pay, poor prospects, and psychological toll. The perils of microtask work. Ars Technica, September 23. https://arstechnica.com/information-technology/2018/09/in-most-cases-online-microtask-work-can-be-a-raw-deal-un-study-finds/ (access: 13.04.2020)

Global Information Society Watch (2019): Artificial intelligence. Human rights, social justice and development. https://giswatch.org/sites/default/files/gisw2019_artificial_intelligence.pdf (access: 13.04.2020)

Global Network Initiative (2017): GNI Principles on Freedom of Expression and Privacy. Global Network Initiative, May 2017. https://globalnetworkinitiative.org/wp-content/uploads/2018/04/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf (access: 13.04.2020)

Global Reporting Initiative (2015): Linking G4 and the UN Guiding Principles. Amsterdam. https://www.globalreporting.org/resourcelibrary/GRI-UNGP_LinkageDoc.pdf (access: 13.04.2020)

Grabenwarter, Christoph (2014): European Convention on Human Rights. Commentary. Munich: CH Beck

Grabenwarter, Christoph / Pabel, Katharina (2016): Europäische Menschenrechtskonvention. Munich: CH Beck

Graham, Mark (ed., 2019): Digital Economies at Global Margins. Cambridge, M.A. https://www.idrc.ca/sites/default/files/sp/Images/idl-57429_2.pdf (access: 13.04.2020)

Green, Ben (2019): The Smart Enough City. Putting Technology in Its Place to Reclaim Our Urban Future. Camebridge, MA: MIT Press

Harris, Shane (2014): @ War. The rise of the military-internet complex. New York: Eamon Dolan

Hawkins, Amy (2018): Beijing's Big Brother Tech Needs African Faces. July 24. https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/ (access: 13.04.2020)

Hern, Alex (2016): 'Partnership on AI' formed by Google, Facebook, Amazon, IBM and Microsoft. In: The Guardian, 28.09.2016. https://www.theguardian.com/technology/2016/sep/28/google-facebook-amazon-ibm-microsoft-partnership-on-ai-tech-firms (access: 13.04.2020)

Hern, Alex (2018): Italian regulator fines Facebook £8.9m for misleading users. In: The Guardian, 07.12.2018. https://www.theguardian.com/technology/2018/dec/07/italian-regulator-fines-facebook-89m-for-misleading-users (access: 13.04.2018)

Hidvegi, Fanny (2019): Experts are finished, politicians to deliver – the Council of Europe publishes expert recommendations on the human rights impacts of algorithmic systems. Access Now, November 12. https://www.accessnow.org/experts-are-finished-politicians-to-deliver-the-council-of-europe-publishes-expert-recommendations-on-the-human-rights-impacts-of-algorithmic-systems/ (access: 13.04.2020)

Hilligoss, Hannah / Raso, Filippo A. / Krishnamurthy, Vivek (2018): It's not enough for AI to be "ethical"; it must also be "rights respecting". Berkman Klein Center blog post, October 9. https://medium.com/berkman-klein-center/its-not-enough-for-ai-to-be-ethical-it-must-also-be-rights-respecting-b87f7e215b97 (access: 13.04.2020)

Hirsh, Jesse (2018): One City's Endeavour for Ethical AI. Centre for International Governance Innovation, December 14. https://www.cigionline.org/articles/one-citys-endeavour-ethical-ai (access: 13.04.2020)

House of Commons Digital, Culture, Media and Sport Committee (2019): Disinformation and 'fake news': Final report. Eighth report of session 2017-19. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf (access: 13.04.2020)

IEEE (2019): Ethically Aligned Design. Versions 1 and 2. https://standards.ieee.org/industry-connections/ec/ead-v1.html (access: 13.04.2020)

International Committee of the Red Cross (2018): Digital trails could endanger people receiving humanitarian aid, ICRC and Privacy International find. December 7. https://www.icrc.org/en/document/digital-trails-could-endanger-people-receiving-humanitarian-aid-icrc-and-privacy. (access: 13.04.2020)

Jobin, Anna / Ienca, Marcello / Vayena, Effi (2019): The global landscape of AI ethics guidelines. In: Nature Machine Intelligence 2 (1), pp. 389–399

Johnson, Bobbie (2010): Privacy no longer a social norm, says Facebook founder. In: The Guardian, 11.01.2010. https://www.theguardian.com/technology/2010/jan/11/facebook-privacy (access: 13.04.2020)

Jorgensen, Rikke F. (ed., 2019): Human rights in the age of platforms. Cambridge, MA: MIT Press. https://direct.mit.edu/books/book/4531/Human-Rights-in-the-Age-of-Platforms (access: 13.04.2020)

Joseph, George (2019): Inside the Video Surveillance Program IBM Built for Philippine Strongman Rodrigo Duterte. The Intercept, March 20. The Intercept. https://theintercept.com/2019/03/20/rodrigo-duterte-ibm-surveillance/ (access: 13.04.2020)

Kälin, Walter / Künzli, Jörg (2013): Universeller Menschenrechtsschutz. Basel: Helbing Lichtenhahn Verlag

Kelley, Jason (2019): If It Really Wants To Restore Debate, Facebook Should Update Its Ad Policy. Electronic Frontier Foundation. https://www.eff.org/fa/deeplinks/2019/03/if-it-really-wants-restore-debate-facebook-should-update-its-ad-policy (access: 13.04.2020)

Kellogg, Katherine C. / Valentine, Melissa A. / Christin, Angèle (2020): Algorithms at work. The new contested terrain of control. In: Academy of Management Annals 14 (1), pp. 366–410

Kim, Pauline T. (2016): Data-driven discrimination at work. In: William & Mary Law Review 58 (3), pp. 587–936

Kim, Pauline T. (2017): Auditing algorithms for discrimination. In: University of Pennsylvania Law Review Online 166, pp. 189–203

Koebler, Jason (2016): Uber Begins Its Endgame. Replacing Humans. Motherboard, August 18. https://motherboard.vice.com/en_us/article/9a3n93/uber-begins-its-endgame-replacing-humans (access: 13.04.2020)

Kofman, Ava (2018): Google's "smart city of surveillance" faces new resistance in Toronto. The Intercept, November 13. https://theintercept.com/2018/11/13/google-quayside-toronto-smart-city/ (access: 13.04.2020)

Koops, Bert-Jaap / Leenes, Ronald (2014): Privacy regulation cannot be hardcoded. A critical comment on the 'Privacy by Design' provision in data-protection law. In: International Review of Law, Computers & Technology 28 (2), pp. 159–171

Kroll, Joshua A. et al. (2016): Accountable algorithms. In: University of Pennsylvania Law Review Online 165, pp. 633–705

Labowitz, Sarah / Posner, Michael (2016): Why We're Leaving the Global Network Initiative. NYU Stern Center for Business and Human Rights, February 1. https://bhr.stern.nyu.edu/blogs/why-were-leaving-the-gni (access: 13.04.2020)

Latonero, Mark (2018): Governing Artificial Intelligence: Upholding human rights & dignity. New York: Data & Society research report. https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf (access: 13.04.2020)

Lynch, Marc (2011): After Egypt. The limits and promise of online challenges to the authoritarian Arab state. In: Perspectives on Politics 9 (2), pp. 301–310

MacKinnon, Rebecca (2007): Shi Tao, Yahoo!, and the lessons for corporate social responsibility. https://rconversation.blogs.com/YahooShiTaoLessons.pdf (access: 13.04.2020)

MacKinnon, Rebecca (2012): Consent of the networked. The worldwide struggle for Internet freedom. New York: Basic Books

Markkula Center for Applied Ethics (2019): Readings in AI ethics. Santa Clara University. https://www.scu.edu/ethics/internet-ethics-blog/readings-in-ai-ethics/ (access: 13.04.2020)

Martini, Beatrice (2017): Decolonizing technology. A reading list. Blog, May 10. https://beatricemartini.it/blog/decolonizing-technology-reading-list/ (access: 13.04.2020)

Maus, Moritz (2006): Der grundrechtliche Schutz des Privaten im europäischen Recht. Dissertation. Giessen: Justus-Liebig-Universität Giessen

Mazzetti, Mark et al. (2019): A New Age of Warfare. How Internet Mercenaries Do Battle for Authoritarian Governments. In: The New York Times, 21.03.2019. https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html (access: 13.04.2020)

Melendez, Steven / Pasternack, Alex (2019): Here are the data brokers quietly buying and selling your personal information. Fast Company, March 2. https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information (access: 13.04.2020)

Milan, Stefania / Treré, Emiliano (2019): Big Data from the South(s): Beyond data universalism. In: Television & New Media 20 (4), pp. 319–335

MIT Media Lab (2019): AI Blindspot. A discovery process for spotting unconscious biases and structural inequalities in AI systems. https://aiblindspot.media.mit.edu/ (access: 13.04.2020)

Mittelstadt, Brent D. et al. (2016): The ethics of algorithms. Mapping the debate. In: Big Data & Society 3 (2), pp. 1–21

Monahan, Torin (2016): Built to lie. Investigating technologies of deception, surveillance, and control. In: The Information Society 32 (4), pp. 229–240

Montréal Declaration (2018): Official launch of the Montréal Declaration for Responsible Development of Artificial Intelligence, press release of 04 December 2018. https://www.declarationmontreal-iaresponsable.com/blogue/d%C3%A9voilement-de-la-d%C3%A9claration-de-montr%C3%A9al-pour-un-d%C3%A9veloppement-responsable-de-l-ia (access: 13.04.2020)

Montréal Declaration (2019): Montréal Declaration for a Responsible Development of Artificial Intelligence. https://www.montrealdeclaration-responsibleai.com/the-declaration (access: 13.04.2020)

Morris, Stephen / Griffin, Donal / Gower, Patrick (2017): Barclays Puts in Sensors to See Which Bankers Are at Their Desks. Bloomberg, August 18. https://www.bloomberg.com/news/articles/2017-08-18/barclays-puts-in-sensors-to-see-which-bankers-are-at-their-desks (access: 13.04.2020)

Mowbray, Alastair (2012): Cases, materials, and commentary on the European Convention on Human Rights. Oxford: Oxford University Press

Myers West, Sarah (2019): Data capitalism. Redefining the logics of surveillance and privacy. In: Business & Society 58 (1), pp. 20–41

Necessary & Proportionate (2014): International Principles on the Application of Human Rights to Communications Surveillance. https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf (access: 13.04.2020)

Neff, Gina / Nafus, Dawn (2016): Self-tracking. Camebridge, MA: MIT Press

NOYB (2018): Complaint against Google under art. 77(1) GDPR. https://noyb.eu/en/project/national-implementation-gdpr (access: 13.04.2020)

NOYB (2018): GDPR: noyb.eu filed four complaints over “forced consent” against Google, Instagram, WhatsApp and Facebook., press release of 25 May 2018. https://noyb.eu/en/project/forced-consent-dpas-austria-belgium-france-germany-and-ireland (access: 13.04.2020)

NOYB (2019): CNIL fines Google € 50 Mio based on noyb complaint, press release of 21 January 2019. https://noyb.eu/en/breaking-cnil-fines-google-eu-50-mio-based-noyb-complaint (access: 13.04.2020)

OECD (2019): OECD AI Principles. https://www.oecd.org/going-digital/ai/principles/ (access: 13.04.2020)

O'Neil, Cathy (2017): Weapons of math destruction. How big data increases inequality and threatens democracy. New York: Broadway Books

PAI (2019): Partnership on AI: Meet the partners. https://www.partnershiponai.org/partners/ (access: 13.04.2020)

Pardes, Arielle (2018): Silicon Valley Writes a Playbook to Help Avert Ethical Disasters. A new guidebook for tech companies helps them imagine future scenarios where their tech might end up causing societal harm. Wired, August 7. https://www.wired.com/story/ethical-os/ (access: 13.04.2020)

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

Pasquale, Frank (2015): The black box society. Camebridge, MA: Harvard University Press

Penney, Jonathon et al. (2018): Advancing Human-Rights-by-Design in the Dual-Use Technology Industry. In: Journal of International Affairs 71 (2), pp. 103–110

Pichai, Sundar (2018): AI at Google: our principles. Blog post by Google CEO Sundar Pichai. https://www.blog.google/technology/ai/ai-principles/ (access: 13.04.2020)

Pielemeier, Jason (2019): AI & Global Governance: The Advantages of Applying the International Human Rights Framework to Artificial Intelligence. United Nations University Centre for Policy Research, February 26. https://cpr.unu.edu/ai-global-governance-the-advantages-of-applying-the-international-human-rights-framework-to-artificial-intelligence.html (access: 13.04.2020)

Pilkington, Ed (2019): 'Digital welfare state': big tech allowed to target and surveil the poor, UN is warned. In: The Guardian, 16.10.2019. https://www.theguardian.com/technology/2019/oct/16/digital-welfare-state-big-tech-allowed-to-target-and-surveil-the-poor-un-warns (access: 13.04.2020)

Piper, Kelsey (2019): Exclusive: Google cancels AI ethics board in response to outcry. Vox.com, April 4. https://www.vox.com/future-perfect/2019/4/4/18295933/google-cancels-ai-ethics-board (access: 13.04.2020)

Pirkova, Eliska (2018): How the Use of 'Ethical' Principles Hijacks Fundamental Freedoms: The Austrian Social Media Guidelines on Journalists' Behaviour. Privacy & Sustainable Computing Lab, August 8. https://privacylab.at/1083/how-the-use-of-ethical-principles-hijacks-fundamental-freedoms-the-austrian-social-media-guidelines-on-journalists-behaviour/ (access: 13.04.2020)

Powles, Julia / Nissenbaum, Helen (2018): The Seductive Diversion of 'Solving' Bias in Artificial Intelligence. Trying to "fix" A.I. distracts from the more urgent questions about the technology. Blog post, December 7. https://medium.com/s/story/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53 (access: 13.04.2020)

Prassl, Jeremias (2018): Humans as a service. The promise and perils of work in the gig economy. Oxford: Oxford University Press

Rainey, Bernadette / Wicks, Elizabeth / Ovey, Clare (2014): Jacobs, White and Ovey. The European convention on human rights. Oxford: Oxford University Press

Ranking Digital Rights (2020): Ranking Digital Rights' response to Facebook on the Oversight Board bylaws, trust, and human rights review, press release of 28 January 2020. https://rankingdigitalrights.org/wp-content/uploads/2020/01/RDR-Response-Facebook-Oversight-Board.pdf (access: 13.04.2020)

Raso, Filippo A. et al. (2018): Artificial Intelligence & Human Rights: Opportunities & Risks. Berkman Klein Center Research Publication no. 2018-6. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3259344 (access: 13.04.2020)

Redeker, Dennis / Gill, Lex / Gasser, Urs (2018): Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights. In: International Communication Gazette 80 (4), pp. 302–319

Reventlow, Nani J. (2019): Digital rights are *all* human rights, not just civil and political. Berkman Klein Center blog series, February 27. https://medium.com/berkman-klein-center/digital-rights-are-all-human-rights-not-just-civil-and-political-daf1f1713f7a (access: 13.04.2020)

Richards, Neil M. (2012): The dangers of surveillance. In: Harvard Law Review 126 (7), pp. 1934–1965

Risse, Mathias (2018): Human Rights and Artificial Intelligence: An Urgently Needed Agenda. HKS Faculty Research Working Paper Series RWP18-015. Harvard Kennedy School, May 18. https://dx.doi.org/10.2139/ssrn.3180741 (access: 13.04.2020)

Risse, Mathias / Livingston, Steven (2019): The Future Impact of Artificial Intelligence on Humans and Human Rights. In: Ethics and International Affairs 33 (2), pp. 141–158

Roose, Kevin / Muzur, Paul (2018): Zuckerberg was called out over Myanmar violence. Here's his apology. In: The New York Times, 09.04.2018. https://www.nytimes.com/2018/04/09/business/facebook-myanmar-zuckerberg.html (access: 13.04.2020)

Rubinstein, Ira (2012): Big data. the end of privacy or a new beginning? In: International Data Privacy Law 3 (2), pp. 12–56

Rudolph, Harrison / Moy, Laura / Bedoya, Alvaro M. (2017): Not ready for takeoff. Face scans at airport departure gates. Georgetown Law Center on Privacy & Technology. Washington, D.C. https://www.airportfacescans.com/ (access: 13.04.2020)

Ruggie, John G. (2007): Business and human rights. The evolving international agenda. In: American Journal of International Law 101 (4), pp. 819–840

Ruggie, John G. (2013): Just business. Multinational corporations and human rights. New York: WW Norton & Company

Samway, Michael A. (2016): The Global Network Initiative. How can companies in the information and communications technology industry respect human rights. In: Baumann-Pauly, Dorothée and Nolan, Justine (eds.): Business and human rights. From principles to practice. New York: Routledge, pp. 136–146

Sander, Matthias (2016): Datenschutz allein reicht nicht aus. In: Neue Zürcher Zeitung, 21.04.2016. https://www.nzz.ch/wirtschaft/unternehmen/ethik-aussschuss-fuer-big-data-datenschutz-allein-reicht-nicht-aus-ld.15168 (access: 13.04.2020)

Scheiber, Noam (2018): Google Workers Reject Silicon Valley Individualism in Walkout. In: The New York Times, 06.11.2018. https://www.nytimes.com/2018/11/06/business/google-employee-walkout-labor.html (access: 13.04.2020)

Scheiber, Noam / Conger, Kate (2020): The Great Google Revolt. In: The New York Times, 18.02.2020. https://www.nytimes.com/interactive/2020/02/18/magazine/google-revolt.html (access: 13.04.2020)

Scherer, Andreas G. / Palazzo, Guido (2011): The new political role of business in a globalized world. A review of a new perspective on CSR and its implications for the firm, governance, and democracy. In: Journal of Management Studies 48 (4), pp. 899–931

Schneier, Bruce (2015): Data and Goliath. The hidden battles to collect your data and control your world. New York: WW Norton & Company

Scholz, Trebor (2017): Uberworked and underpaid. How workers are disrupting the digital economy. Cambridge et al.: MA: Polity Press

Selinger, Evan (2019): Why IBM's "Dear Tech" ad is so enraging. Slate, February 26. https://slate.com/technology/2019/02/ibm-dear-tech-oscars-ad.html (access: 13.04.2020)

Shane, Scott / Wakabayashi, Daisuke (2018): 'The Business of War': Google Employees Protest Work for the Pentagon. In: The New York Times, 04.04.2018. https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html (access: 13.04.2020)

Singer, Natasha (2018): Tech's ethical 'dark side': Harvard, Stanford and others want to address it. In: The New York Times, 12.02.2018. https://www.nytimes.com/2018/02/12/business/computer-science-ethics-courses.html (access: 13.04.2020)

Sloane, Mona (2018): Making artificial intelligence socially just: Why the current focus on ethics is not enough. LSE blog, July 6. https://blogs.lse.ac.uk/politicsandpolicy/artificial-intelligence-and-society-ethics/ (access: 13.04.2020)

Solon, Olivia (2016): The year Facebook became the bad guy. In: The Guardian, 12.12.2016. https://www.theguardian.com/technology/2016/dec/12/facebook-2016-problems-fake-news-censorship (access: 13.04.2020)

Spiekermann, Sarah (2012): The challenges of Privacy by Design. In: Communications of the ACM 55 (7), pp. 38–40

Srnicek, Nick (2017): Platform capitalism. Cambridge: Polity

Stack Overflow (2018): Developer survey 2018. https://insights.stackoverflow.com/survey/2018/ (access: 13.04.2020)

Strasbourg Observers (2019): López Ribalda and Others v. Spain – covert surveillance in the workplace: attenuating the protection of privacy for employees. Blog, December 6. https://strasbourgobservers.com/2019/12/06/lopez-ribalda-and-others-v-spain-covert-surveillance-in-the-workplace-attenuating-the-protection-of-privacy-for-employees/ (access: 13.04.2020)

Swisher, Kara (2019): Facebook's Biblically Bad Week. In: The New York Times, 14.03.2019. https://www.nytimes.com/2019/03/14/opinion/facebook-criminal-investigation.html (access: 13.04.2020)

Tarnoff, Ben (2017): Silicon Valley siphons our data like oil. But the deepest drilling has just begun. In: The Guardian, 23.08.2017. https://www.theguardian.com/world/2017/aug/23/silicon-valley-big-data-extraction-amazon-whole-foods-facebook (access: 13.04.2020)

Tene, Omer / Polonetsky, Jules (2011): Privacy in the age of big data. A time for big decisions. In: Stanford Law Review Online 64, pp. 63–69

Thorp, Jer (2012): Big data is not the new oil. In: Havard Business Review 2012 (November). https://hbr.org/2012/11/data-humans-and-the-new-oil (access: 13.04.2020)

Toronto Declaration (2018): The Toronto Declaration: Protecting the Rights to Equality and Non-discrimination in Machine Learning Systems. https://www.intgovforum.org/multilingual/sites/default/files/webform/toronto-declaration-final.pdf (access: 13.04.2020)

Tufekci, Zeynep (2014): How social media took us from Tahrir Square to Donald Trump. In: MIT Technology Review 2014 (August). https://www.technologyreview.com/s/611806/how-social-media-took-us-from-tahrir-square-to-donald-trump/ (access: 13.04.2020)

Tufekci, Zeynep (2017): Twitter and tear gas. The power and fragility of networked protest. New Haven & London: Yale University Press

UN, General Assembly (1948): Universal Declaration of Human Rights (UDHR), adopted on 10 December 1948, UN Doc. A/RES/217

UN, General Assembly (1966): International Covenant on Civil and Political Rights, UN Doc. A/RES/2200 (XXI)

UN, Office of the United Nations High Commissioner for Human Rights (2019): UN Human Rights Business and Human Rights in Technology Project (B-Tech). Applying the UN Guiding Principles on Business and Human Rights to digital technologies. November 2019. Geneva. https://www.ohchr.org/Documents/Issues/Business/B-Tech/B_%20Tech_Project_revised_scoping_final.pdf (access: 13.04.2020)

UN, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (2018): Report of the Special Rapporteur to the General Assembly on AI and its impact on freedom of opinion and expression. New York, UN Doc. A/73/348

Universal Guidelines for AI (2018): International Data Protection and Privacy Commissioners Conference. https://thepublicvoice.org/ai-universal-guidelines/ (access: 13.04.2020)

Vaidhyanathan, Siva (2018): Antisocial media. How Facebook disconnects us and undermines democracy. Oxford: Oxford University Press

Vaidhyanathan, Siva (2019): Facebook's new move isn't about privacy. It's about domination. In: The Guardian, 07.03.2019. https://www.theguardian.com/commentisfree/2019/mar/07/facebook-privacy-domination (access: 13.04.2020)

Vaidhyanathan, Siva (2019): Facebook's privacy meltdown after Cambridge Analytica is far from over. In: The Guardian, 18.03.2019. https://www.theguardian.com/uk-news/commentisfree/2019/mar/18/cambridge-analytica-chernobyl-privacy (access: 13.04.2020)

Waddell, Kaveh (2016): The Algorithms That Tell Bosses How Employees Are Feeling. In: The Atlantic, 29.11.2016. https://www.theatlantic.com/technology/archive/2016/09/the-algorithms-that-tell-bosses-how-employees-feel/502064/ (access: 13.04.2020)

Wagner, Ben (2018): Ethics as an Escape from Regulation. From ethics-washing to ethics-shopping? In: Bayamlioglu, Emre et al. (eds.): Being Profiled: Cogitas Ergo Sum. 10 Years of Profiling the European Citizen. Amsterdam: Amsterdam University Press

Wagner, Ben / Kettemann, Mathias C. / Vieth, Kilian (eds.) (2019): Research handbook on human rights and digital technology. Global politics, law and international relations. Cheltenham, UK et al.: Edward Elgar Publishing

Wakefield, Jane (2020): Google asked to justify Toronto 'digital-city' plan. BBC News, February 27. https://www.bbc.com/news/technology-51658116 (access: 13.04.2020)

Wedde, Peter (2018): Art. 25 DSGVO. In: Däubler, Wolfgang et al. (eds.): EU-Datenschutz-Grundverordnung und BDSG-neu. Kompaktkommentar. Frankfurt am Main: Bund-Verlag, pp. FEHLEN

Wee, Sui L. (2019): China Uses DNA to Track Its People, With the Help of American Expertise. In: The New York Times, 21.02.2019. https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html (access: 13.04.2020)

West, Sarah M. (2019): Data capitalism. Redefining the logics of surveillance and privacy. In: Business & Society 58 (1), pp. 20–41

Wettstein, Florian (2015): Normativity, ethics, and the UN guiding principles on business and human rights. A critical assessment. In: Journal of Human Rights 14 (2), pp. 162–182

Wettstein, Florian (2016): From Side Show to Main Act. Can Business and Human Rights Save Corporate Responsibility. In: Baumann-Pauly, Dorothée and Nolan, Justine (eds.): Business and human rights. From principles to practice. New York: Routledge, pp. 77–87

Whittaker, Meredith et al. (2018): AI Now Report 2018. AI Now Institute, New York University. https://ainowinstitute.org/AI_Now_2018_Report.pdf (access: 13.04.2020)

Whittaker, Zack (2019): Many popular iPhone apps secretly record your screen without asking. And there's no way a user would know. Techcrunch.com, February 6. https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots/ (access: 13.04.2020)

Wikipedia (2019): Criticism of Facebook. https://en.wikipedia.org/wiki/Criticism_of_Facebook (access: 13.04.2020)

Wildhaber, Isabelle (2017): Robotik am Arbeitsplatz. Robo-Kollegen und Robo-Bosse. In: Aktuelle Juristische Praxis 26 (2), pp. 213–224

Wingfield, Nick (2018): Amazon Pushes Facial Recognition to Police. Critics See Surveillance Risk. In: The New York Times, 22.05.2018. https://www.nytimes.com/2018/05/22/technology/amazon-facial-recognition.html (access: 13.04.2020)

Wolkenstein, Andreas (2018): What has the Trolley Dilemma ever done for us (and what will it do in the future)? On some recent debates about the ethics of self-driving cars. In: Ethics and Information Technology 20 (3), pp. 163–173

World Bank (2016): World Development Report 2016: Digital Dividends. Washington D.C.: World Bank. https://doi.org/10.1596/978-1-4648-0671-1 (access: 13.04.2020)

Zimmer, Ben (2019): 'Techlash': Whipping up criticism of the top tech companies. The increasingly sharp rebukes of Facebook, Google and others now have a term of their own. In: The Wall Street Journal, 10.01.2019. https://www.wsj.com/articles/techlash-whipping-up-criticism-of-the-top-tech-companies-11547146279 (access: 13.04.2020)

Zuboff, Shoshana (2015): Big other. surveillance capitalism and the prospects of an information civilization. In: Journal of Information Technology 30 (1), pp. 75–89

Zuboff, Shoshana (2019): The age of surveillance capitalism. The fight for the future at the new frontier of power. New York: Public Affairs

Zuckerberg Files (2019): An archive of all public utterances of Facebook's founder and CEO, Mark Zuckerberg. https://www.zuckerbergfiles.org/ (access: 13.04.2020)

Imprint

PUBLISHER
German Institute for Human Rights
Zimmerstraße 26/27 | 10969 Berlin, Germany
Tel.: +49 30 25 93 59-0
info@institut-fuer-menschenrechte.de
www.institut-fuer-menschenrechte.de

Institute for Business Ethics
University of St. Gallen (HSG)
Girtannerstrasse 8
CH-9010 St.Gallen
Tel.: +41 71 224 21 11
ethik@unisg.ch
https://iwe.unisg.ch/de

Analysis I May 2020
ISBN 978-3-946499-69-5 (PDF)

CITATION
Ebert, Isabel / Busch, Thorsten / Wettstein, Florian (2020): Business and Human Rights in the Data Economy. A Mapping and Research Study. Berlin: German Institute for Human Rights

LICENCE

https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de

TITLE IMAGE
metamorworks/istock

TYPESETTING
www.avitamin.de

Gefördert durch:

Bundesministerium für Arbeit und Soziales

aufgrund eines Beschlusses des Deutschen Bundestages

German Institute for Human Rights

Zimmerstraße 26/27
10969 Berlin

www.institut-fuer-menschenrechte.de