Digital Future Society

Towards better data governance for all:

Data ethics and privacy in the digital era

A programme of

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

MOBILE WORLD CAPITAL BARCELONA

Digital Future Society

About Digital Future Society

Digital Future Society is a non-profit transnational initiative that engages policymakers, civil society organisations, academic experts and entrepreneurs from around the world to explore, experiment and explain how technologies can be designed, used and governed in ways that create the conditions for a more inclusive and equitable society.

Our aim is to help policymakers identify, understand and prioritise key challenges and opportunities now and in the next ten years under key themes including public innovation, digital trust and equitable growth.

Visit digitalfuturesociety.com to learn more

A programme of

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

MOBILE WORLD CAPITAL BARCELONA

Published
July 2019

Disclaimer
The information and views set out in this report are those of the author(s) and do not necessarily reflect the official opinion of Mobile World Capital Foundation. The Foundation does not guarantee the accuracy of the data included in this report. Neither the Foundation nor any person acting on the Foundation's behalf may be held responsible for the use which may be made of the information contained herein.

Digital Future Society

Contents

Executive Summary

Digital Future Society

From the wake of today's rapid technological development, human and ethical dilemmas emerge. Societies worldwide are undergoing what has come to be known as the Fourth Industrial Revolution, marked by the elimination of boundaries between the physical and digital worlds, and the outsourcing of human activities and decisions to machines — all ultimately fueled by data.

While undoubtedly serving as an asset, data can also pose ethical risks. Threats of privacy erosion and growing public awareness around data misuse have sparked heated debates around the need for more transparency, accountability and inclusiveness. With profit-driven interests leveraging increasingly sophisticated technologies, data users — and more broadly, citizens — are sounding the alarm on the pernicious outcomes of unethical data use.

In a world increasingly reliant on data-driven algorithms to shape choices and make decisions on behalf of humans, policymakers have a responsibility to ensure that appropriate regulatory frameworks and data governance mechanisms are in place so that data practitioners and users understand, respect, and can exercise fundamental human rights. Policymakers also have a critical role in ensuring all members of society possess the skills needed to benefit from increasingly prevalent data-driven systems.

The Digital Future Society programme is engaging with experts and policymakers to expand the boundaries of the debate around digital ethics and data privacy by creating space to reflect and act on questions such as:

- How can organisations prevent unethical outcomes of data-driven technologies?
- How can public administrations undertake ethically responsible oversight of data-driven technologies?
- How can governments support the involvement of citizens in the development of data-driven systems that will directly impact their lives?

At the heart of our inquiry is a desire to establish an inclusive digital society in which data ethics and privacy are embedded as norms rather than exceptions or afterthoughts. Having explored the current views of public and private organisations around the opportunities and challenges of privacy and ethics in the context of data-driven technologies, we propose the following set of recommendations to help policymakers improve data governance efforts:

1 **Lead by example in good data governance**
Policymakers can set the bar for good data governance by implementing Privacy by Design in public service delivery, going open source by default and experimenting with emerging data governance models.

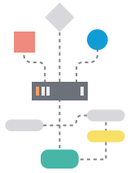
2 **Push for accountability and regulatory reform that operationalises ethical principles**
Concrete actions beyond commitment are needed to ensure ethical data collection, use, and governance in the public and private sectors.

3 **Take an inclusive and transparent approach to data governance beyond consent and transparency fallacies**
Policymakers can address inclusion and transparency gaps by improving digital literacy and promoting diversity in the tech sector.

Glossary

Digital Future Society

Glossary

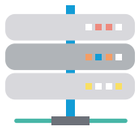


Algorithm

An algorithm is an unambiguous specification of a process describing how to solve a class of problems that can perform calculations, process data and automate reasoning.[1]

Artificial intelligence (AI)

In its most basic form, artificial intelligence is a system that makes autonomous decisions. AI is a branch of computer science in which computers are programmed to do things that normally require human intelligence. This includes learning, reasoning, problem solving, understanding language and perceiving a situation or environment.[2]



Automated decision-making systems (ADMS)

Procedures or processes that gather data, analyse data, interpret the results of this analysis (based on a human-defined interpretation model), and act automatically based on that interpretation (without any human involvement or intervention). These decisions can be based on factual data, as well as on digitally created profiles or inferred data. While ADMS have proven to be extremely efficient in improving data and information flow, these systems are only as ethically robust as the data that is fed to them.

Data breach

The unauthorised acquisition of computerised data that compromises the security, confidentiality, or integrity of personal information maintained by a data collector.[3]

[1] Figure-eight.com 2019

[2] Webb et al. 2019

[3] Nytimes.com 2019

Data brokers

Entities that collect, aggregate and sell individuals' personal data, derivatives, and inferences from disparate public and private sources.[4]

Data ethics

Data ethics is the branch of ethics that studies and evaluates moral problems related to data use (including generation, recording, curation, processing, dissemination, sharing), algorithms (including artificial intelligence, artificial agents, machine learning and robots) and corresponding practices (including responsible innovation, programming, hacking and professional codes), in order to formulate and support morally desirable solutions (e.g. good conduct or ethical values).[5]

General Data Protection Regulation (GDPR)

The General Data Protection Regulation replaced the Data Protection Directive in 2018. The aim of the GDPR is to provide one set of data protection rules for all European Union member states and the European Economic Area (EEA).[6]

[4] Nytimes.com 2019

[5] Floridi and Taddeo 2016

[6] Iapp.org 2019

Privacy

A right to be left alone. The right to privacy means that each individual has the right to choose to share or not to share information about his or her private life, habits, acts, and relations with others.[7] Four main areas of privacy are relevant to discussions of data protection, privacy laws and practices: information privacy, bodily privacy, territorial privacy, and communications privacy.[8] At the core of informational privacy is the notion that data subjects have the right and the ability to shield personal data from third parties.[9]

Privacy by Design

Developed by Dr. Ann Cavoukian in the 1990s, Privacy by Design is a framework that addresses the ever-growing and systemic effects of information and communication technologies, business practices, and of large-scale networked data systems.[10]

Transparency

In the field of information ethics, transparency is generally defined as the availability of information, the conditions of accessibility and how the information may support the user's decision-making processes.[11]

[7] Warren and Brandeis 1890

[8] Iapp.org 2019

[9] Schermer 2011

[10] Caroukian 2019

[11] Turilli and Floridi 2009

Introduction

Digital Future Society

About this report

The promise of more efficient services and improved quality of life brought by data-driven technologies like automated decision-making systems comes with concerns regarding the ethical practices of the public and private entities to which we freely provide our data every day. By identifying common challenges, opportunities and imagining scenarios within the data ethics landscape writ large, this report maps alternative pathways through ongoing, collaborative discussions centered on a vision for a digital future in which society can benefit from data-driven technologies while mitigating harm.

Our ultimate aim is to inform policymakers — anyone working within governments worldwide who must carry out rules, governing frameworks, and regulations that intersect with data-driven technologies — of actionable outcomes that can be implemented now to build more inclusive and equitable digital societies.

Audience

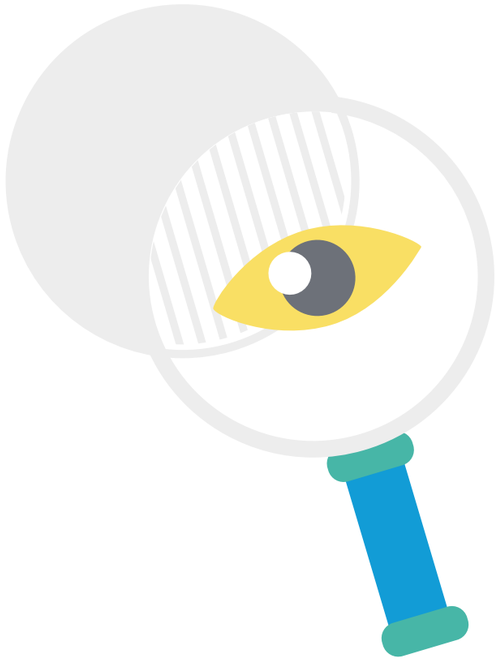
Moral reasons to protect personal data including avoiding harm, preventing exploitation in data markets and preventing inequality and discrimination through data misuse place the responsibility on governments and policymakers to set up appropriate laws and regulations. For this reason, we direct our inquiry to individuals and organisations who are able to drive change in a policymaking context.

Beyond informing policymakers of the challenges and opportunities of transforming societies by deploying data-driven technologies, we aim to influence current data governance efforts undertaken by public and private entities so that the digital economies of today and tomorrow benefit all.

Scope

As data-driven technologies become increasingly prevalent in critical societal infrastructures in business and government, they bring direct consequences to our social, cultural, and economic futures. For this reason, our focus rests on how to ensure data is used for ethical decision-making that respects the privacy of individuals and social groups, especially those at risk of exclusion.[12]

As no one-size-fits-all model to tackling data ethics issues exists, we echo leaders in the field who have advocated for a 'sector-specific approach' to questions of data ethics.[13] The global scope of this report also draws upon trans-regional contexts in Europe, Latin America and Africa to continue developing our inquiry with case studies across the world. This will ensure that the findings and recommendations in this report are widely applicable.



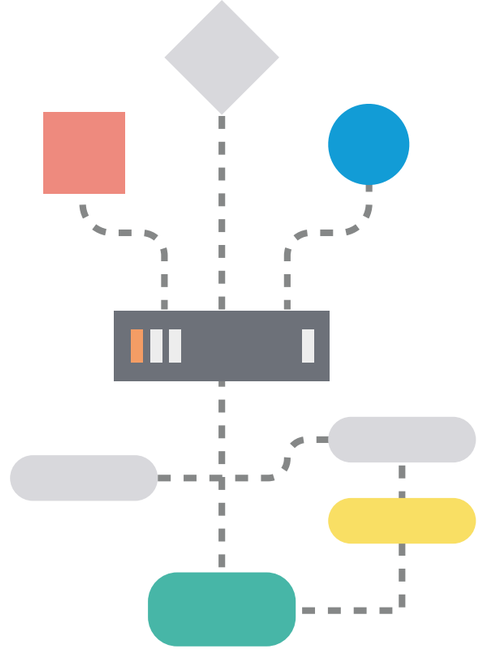
[12] Algorithm Watch 2018

[13] Whittaker et al. 2018

Structure

This report presents the insights and recommendations the Digital Future Society programme has gained through a combination of desk research and consultation with our community of experts, leaders, civil society organisations and policymakers with experience in the implementation of data governance.

The first chapter introduces the concept of data ethics and traces its evolution in recent years. Section 2 focuses on the opportunities and challenges faced by public and private organisations in ensuring ethical data collection, use, and governance. In Section 3 we introduce the concept of futures as tools which is based on the analysis of key uncertainties that will shape our societies in the coming years. Drawing on the analysis of preceding chapters, Section 4 shares and explains key recommendations for policymakers to improve and operationalise ethical data governance structures through focused transparency, accountability, and educational efforts.



1

Tracing the development of data ethics

Digital Future Society

What is data ethics?

In recent years, public policy discussions on the collection and use of personal information by third parties have focused mainly on privacy issues. While a great deal of work has been done on privacy regulation, it is important to bring data ethics into public policy discourse, especially in the context of data-driven technologies such as artificial intelligence, in order to clarify and address impacts of third-party data use not covered by privacy discussions. These include the potential for discrimination, biased decision-making, as well as the amplification of risks to fairness, equality and due process.[14]

Data ethics refers to the branch of ethics that studies and evaluates moral problems related to data (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including artificial intelligence, artificial agents, machine learning and robots) and corresponding practices (including responsible innovation, programming, hacking and professional codes), in order to formulate and support morally good solutions, right conduct or values.[15]

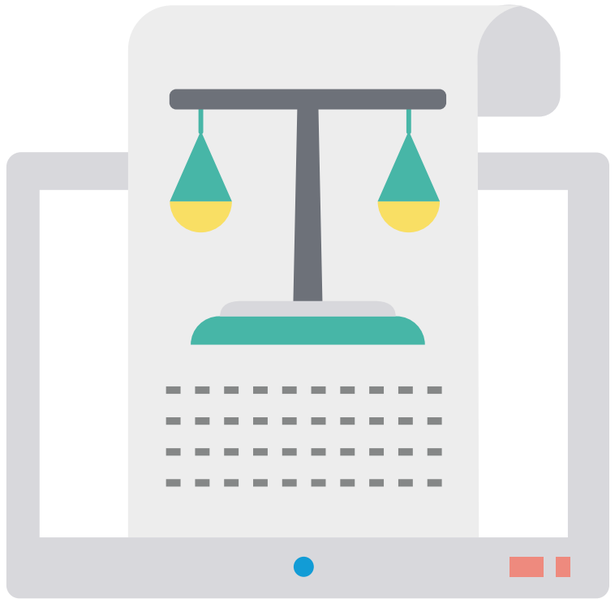
The ethics of data relates to issues such as the possible re-identification of individuals from large data sets, group privacy and the risk of discrimination. The ethics of algorithms addresses the many issues arising from increasingly complex and automated systems, from setting the goals of a system to developing it to selecting training data to system implementation.[16] The ethics of practices addresses questions around the responsibility of organisations and data professionals such as data scientists, researchers, and programmers, that specify the operational parameters of algorithms and their training data inputs.

[14] Building Data Ethics into Privacy Frameworks for Big Data and AI 2018

[15] Floridi and Taddeo 2016

[16] Müller-Eiselt 2018

These three areas (data, algorithms and practices) are deeply intertwined and can be thought of as three axes defining the conceptual space onto which ethical problems related to privacy can be mapped.[17] For instance, an algorithm used in a disaster relief context such as matching lost persons with their families might create a conflict between individual privacy interests on one hand — reflected in purpose limitation and data minimisation principles — and the broader interests of society on the other — served by predicting outcomes based on observed patterns. Data ethics is at the core of reconciling competing public goods: in this case, individual privacy protection vs. the broader societal benefits that may be derived from expedited reunification.[18]



[17] Floridi and Taddeo 2016

[18] Building Data Ethics into Privacy Frameworks for Big Data and AI 2018

Mapping the data ethics landscape

The landscape of data ethics is complex and many challenges emerge when trying to define and engage with it, especially when digital technologies such as artificial intelligence are involved. At the same time, working group experts pointed out that ethical guidelines and codes of conduct have long been present in industries like medicine, finance, and biotechnology, as weel as in the academic world.

Data protection officers, institutional review boards and validation teams are starting to appear in research institutes and even in private organisations that are innovating with big data and artificial intelligence, such as retail banks. In cities, new transparency initiatives and participatory processes based on open data strive to balance citizens' privacy with delivering on promised benefits of digital decision-making processes. Universities around the world have implemented open science and innovation policies, while ethics committees and other bodies work to ensure research is replicable, transparent and respectful of subject privacy. Research groups and educational programmes are becoming increasingly interdisciplinary, with science and engineering tracks including courses on ethics. The scientific research community is another key player in the data ethics landscape, driving this process of raising awareness and changing practices, especially in the emerging field of AI.

However, such practices are not the norm across all sectors and are insufficient given the ubiquity of data and the associated risks of misuse and other potentially harmful impacts, including discrimination and algorithmic bias. Data breaches, hacks, and privacy abuse scandals have become increasingly commonplace around the world, as shown by the following visualisation:

DATA BREACHES vs. CODES OF DATA ETHICS

Digital Future Society

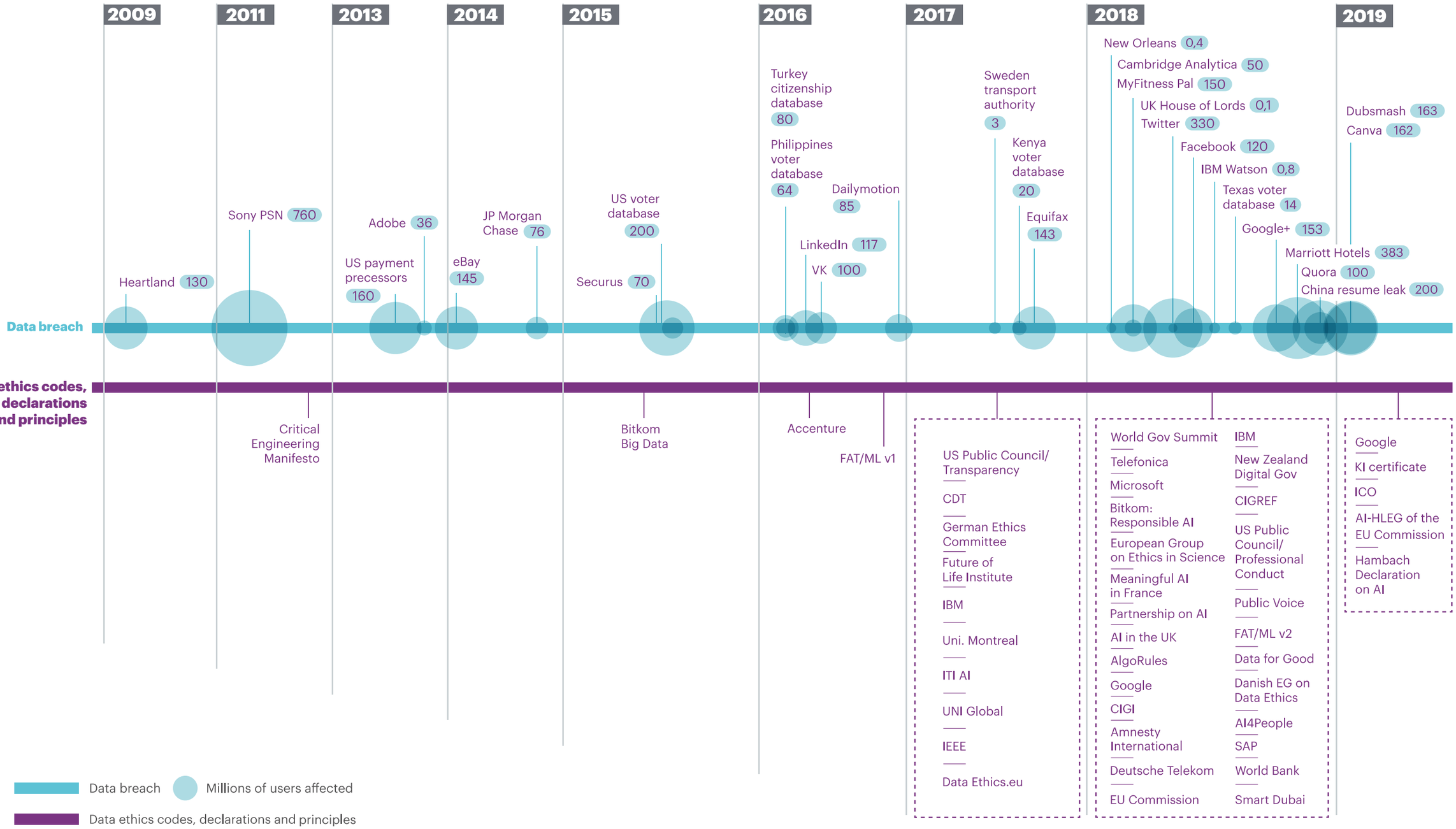


Image source: Digital Future Society

Applying data ethics in supercomputing research

Supercomputing is at the core of AI development. From deep learning to neural network training and feeding big data into massive networks, ethical practices for the collection and processing of data is critical to many research activities at the Barcelona Supercomputing Centre (BSC). For instance, although the BSC does not collect data, it has nonetheless appointed an external ethical committee to provide oversight and approve all research projects. Scientific Manager of the High-Performance Artificial Intelligence Group Ulises Cortes explains how ethics are put into practice at the BSC: "An external ethical committee is consulted to assess all experiments that include personal and/or sensitive data ensuring compliance with an ethical code that prevails in the academic and scientific environment."

Aside from regulatory compliance, the BSC has also taken steps to transform ethical principles into action through its involvement in the European AI project AI4EU. The BSC is currently working on piloting the operationalisation of the guidelines for trustworthy AI in several private and public organisations. In addition to AI4EU project coordinating activities to promote the use of these guidelines, the BSC is contributing to the creation of an observatory to study the use of AI ethics in Europe.

Second, data practices are becoming increasingly sophisticated, surreptitious and invasive. This trend, resulting in a loss of privacy, is summarised below by science fiction author, computer science professor and tech activist Cory Doctorow:

> **"[...] platforms leverage both their users' behavioural data and the ability to lock their users into "walled gardens" to drive growth and profits. The customers for these systems are treated as though they have entered into a negotiated contract [...] trading privacy for service, or vendor lock-in for some kind of subsidy or convenience. [Data collectors claim] that their customers negotiated a deal in which they surrendered their personal information to be plundered and sold, or their freedom to buy service and parts on the open market. But it's obvious that no such negotiation has taken place. Your browser invisibly and silently hemorrhages your personal information as you move about the web."**[19]

In parallel, a new data protection regulatory framework was enacted in Europe that encourages the development of a Privacy by Design infrastructure.[20] Enacted in 2018, the European General Data Protection Regulation (GDPR) provides a regulatory framework around informational privacy, consent, transparency and explainability, the right to erasure or to be forgotten, data portability and Privacy by Design. To date, the GDPR serves as a model for many organisations and governments in terms of data governance and privacy, placing Europe at the vanguard of ethical digital design. Similar frameworks around the world are being developed or revised, with most sharing common underlying privacy principles such as transparency, meaningful choice, accountability and security. Examples include Brunei in 2015,[21] China[22] and Kenya in 2018,[23] and Thailand in 2019.[24]

Beyond evolving legal and regulatory frameworks for data and privacy protection, the past two years alone have seen a growing number of principles, voluntary commitments and frameworks for the ethical use of data, especially where AI is concerned.[25]

In summary, the landscape of data ethics has expanded beyond academia and clinical research domains to the broader public sphere, driven by questionable data practices and leading to raised consciousness around the issues of privacy and data ethics. Despite this heightened awareness, many nuanced challenges and opportunities remain before ethical data-driven systems are deployed universally. These are presented in the next section with a view to proposing policy-relevant recommendations for improved data governance.

[19] Doctorow 2019
[20] See Annex II
[21] Salleh Rahaman 2015
[22] Liao 2018
[23] Privacy and Data Protection Policy 2018
[24] Inside Privacy 2019
[25] See Annex I

2

Challenges and opportunities

Digital Future Society

Weighing the complexities of data governance

The rapid growth of datafication and the digitalisation of nearly all aspects of modern society make citizens more vulnerable to data misuse. This can range from algorithmic and systematic bias embedded within digital technologies that are designed — consciously or not — to discriminate against certain social, gendered, and ethnic groups, to breaches in personal data through online platforms. While accountability and transparency are climbing higher on the agendas of private and public institutions alike, the following challenges must be overcome before data-driven technologies can be implemented safely and ethically.

Challenges of the data-driven era

Data can be an asset, but it can also pose risks. While a growing dialogue to negotiate global standards, roles, rights and responsibilities to handle such risks is ongoing, tensions and clashes between laws and cultural values are being amplified as illustrated in the challenges below.

Algorithmic bias

Business leaders, governments, and academics agree about the potential of AI and other data-driven technologies to improve our lives. But they also agree that these systems have a problem: bias and the risk of discrimination.[26] Algorithms are value-laden by nature, reflecting the life and background of the engineers who build them — typically white males from high income countries.[27] They are then configured by users with desires and moral frameworks that privilege some values and interests over others. It is harder to avoid the involuntary introduction of bias in algorithms when teams of developers lack a minimum degree of diversity and interdisciplinarity to model different realities and complexities into decisions that are being automated.

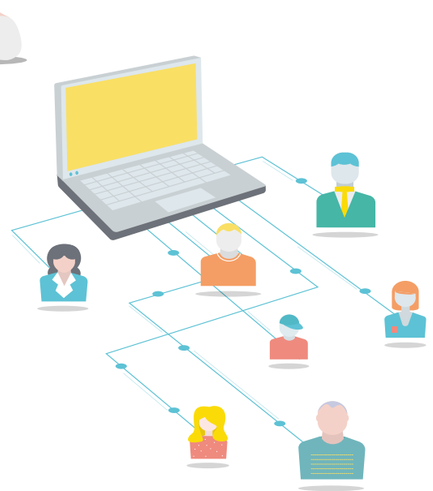
[26] Powles and Nissenbaum 2018

[27] Vincent 2019

Take for example the case of Amazon's same-day delivery service, where action from the public sector was necessary to ensure people from all neighbourhoods were offered the same-day delivery option instead of targeting postal codes that correlated with higher income levels.[28]

Not only can algorithm design engender bias, but the transfer of services and the emergence of new digital products can also end up replicating or amplifying existing inequalities. For example, a new study of the most popular object-recognition algorithms found that 10 percent more errors were made when the algorithms were tasked to identify items from a household with a lower monthly income.[29] Moreover, these algorithms were 15 to 20 percent better at recognising objects from the United Kingdom or the United States than those from Burkina Faso, Somalia, or Nepal.[30]

> **"All algorithms are biased because data is in itself biased and the criteria used in algorithms are culturally defined, so bias is being embedded. That, or there is missing data and proxies are introduced that can also be a source of bias."** [31]
> **-Cathy O'Neil, mathematician and author**



Data concentrations

Many of the world's largest companies rely on data to drive their business models. Alphabet, Amazon, Apple, Facebook, and Microsoft in the United States and Alibaba, Baidu, and Tencent in China enjoy significant competitive advantages that come from owning massive data sets. However, this concentration of data within a limited number of corporations poses a challenge by limiting possibilities for the extraction of public value from data. Furthermore, a lack of market competition has given consumers few alternative choices for the protection of privacy, and none are likely to appear.[32]

[28] Ingold and Soper 2016
[29] Vincent 2019
[30] Vincent 2019
[31] VPRO 2018
[32] Doctorow 2019

Ethical data use carries multiple costs

In the absence of a market for ethical data use, governments face challenges in creating conditions in which ethical behaviours do not come at a cost of competitiveness for large and small firms. Consider AI systems that rely on labelled data in the health technology innovation sector. While the process of ethical data collection is understood and legally defined, labelling tasks risk disproportionately affecting vulnerable groups. However, considerable costs are associated with using ethical sources for labels. While ethical providers are emerging, they are not yet competitive as they operate mainly as non-profits for education and other social programmes. As the challenge of ethical data collection and labelling evolves, the emergence of large data farms in Asia and Africa leaves many questioning the working conditions of these new jobs. "We must be careful to avoid creating a new generation of sweatshops," one expert cautioned.

Overcoming a lack of data literacy

Although awareness of the consequences of sharing data with public and private organisations is on the rise, possible secondary uses of data are not well understood by most. For instance, justifications for collecting and selling data — otherwise known as privacy policies — tend to be excessively verbose and full of jargon, making them nearly impossible for the average internet user to understand. The data market that the internet has become is largely fuelled by citizens who agree to but don't fully understand privacy policies. Working group experts noted a major challenge in boosting data literacy — ensuring individuals and organisations not only understand the consequences of data collection and use, but also its value.

Avoiding the transparency fallacy

As AI becomes more sophisticated, it will become more difficult to explain in an understandable way. As the complexity of algorithms increases, rights to greater transparency might turn counterproductive if citizens lack sufficient data literacy to exercise those rights. The problem is not only faced by citizens; even programmers struggle to understand or explain the decisions taken by some neural networks. As one working group member explains:

> **"Relying on individual rights to explanation as a means for the user to take control of algorithmic systems risks creating a transparency fallacy. Individuals are not empowered to make use of the kind of algorithmic explanations they are likely to be offered; they are mostly too time-poor, resource-poor, and lacking in the necessary expertise to meaningfully make use of these individual rights."**[33]

Security and increased risk of data breaches

Cyberattacks and threats of "massive data fraud" have consistently ranked among the top five global risks listed by the World Economic Forum (WEF).[34] According to the WEF's latest annual survey, theft of money and/or data as well as the disruption of operations and/or infrastructure are expected to increase year on year.[35] The advancement of artificial intelligence is likely to increase the sophistication and difficulty of predicting cyberattacks.

Assigning accountability

Some argue that machine learning algorithms must be considered moral agents with some degree of responsibility.[36] Traditional models of accountability tend to fail since in most cases, no one person has enough control over an automated decision-making system to assume responsibility for its decisions. Implementing workable accountability mechanisms to assure that the decisions of these systems are fair and nondiscriminatory remains a major challenge.

Digital twins and the erosion of moral autonomy

Moral autonomy refers to one's capacity to present one's own identity to others and to resist attempts to stereotype one's choices and biography. A human is morally autonomous when he or she is the author of his or her own moral career.[37] In other words, when we can choose how we want to be and work towards that identity, we can resist external pressures that try to categorise us. However, this effort to shape one's own identity based on moral values becomes threatened when data collectors have already profiled us based on data points gathered about us — sometimes referred to as our "digital twin."

[33] Edwards and Veale 2017

[34] The Age of Digital Interdependence 2019

[35] The Global Risks Report 2019

[36] Mittelstadt et al. 2016

[37] van den Hoven 2008

A second Sorine

The year is 2030, and Sorine is digging through her purse for an ibuprofen on her way home from her new design job. Sorine takes the painkiller and settles into a seat on the driverless tram. "It's that time of the month again," she thinks, Facebook-logging into her period tracking app and inputting a few symptoms. Reaching home, Sorine checks her email. Surprised to see the name of the period tracker app she was just using, she opens the message to discover that her account has been compromised. Startled and annoyed, Sorine quickly deletes the app from her phone and resolves to find a more secure period tracker later. Weeks later, Sorine still cannot be sure that her personal health data will not be sold to insurance companies. It has already been sold to marketers – she knows that because pregnancy test ads keep showing up on her YouTube videos and as she scrolls through Instagram. But if her company should somehow get a hold of it, could it put her new job at risk?

In fact, the data about Sorine's menstrual cycle is not what these companies are after, but rather the "digital debris" that she leaves behind when she reads articles or watches videos, posts about her new job or even searches for recipes. This metadata is used to make inferences that combined create a profile of Sorine – her "digital twin" – whose potential behaviour is carefully tracked, analysed and tagged accordingly. Companies betting on how "digital Sorine" will behave in such markets are profiting from Sorine without her knowledge or consent. It is these secondary uses of metadata over which Sorine – and the rest of us using apps and "free" online platforms and services – have no control.

Problematic data governance models based on ownership and consent

Consent- and ownership-based models of data governance fail to protect the public against certain privacy violations and the unethical collection and use of personal data. Working group experts suggest that even milestone privacy legislation like the GDPR falls short in sufficiently guaranteeing the ethical use of data in a scenario of ubiquitous algorithmically-driven systems. They observe that our collective conception of consent seems to have shifted from providing any informational self-determination to merely legitimising the extraction of personal data in most cases.

> **"Both users and tech providers seem to treat consent as an unnecessary given right," observes one working group member. "More worrying is the possibility of re-identifying individuals from large data sets. The challenge is to ensure the right to be forgotten is understood and respected by public and private entities."**

Similarly, the concept of ownership — widely touted as a solution to data governance issues — is not easily applicable to data and fails to address important questions around access, use, and impact of outcomes, especially in the context of technologies like automated decision-making systems.

Finally, the right to portability in which data subjects have the right to receive their data in a machine-readable format is problematic. While obtaining the data might be easy, using it to obtain a similar service from a different provider could be rendered impossible. Portability is therefore an inadequate substitute for the ability to migrate to a different service to manage data as demonstrated by the case in which a Flickr user's meticulously organised photo collection could only be downloaded in randomised sets of unlabeled files.[38]

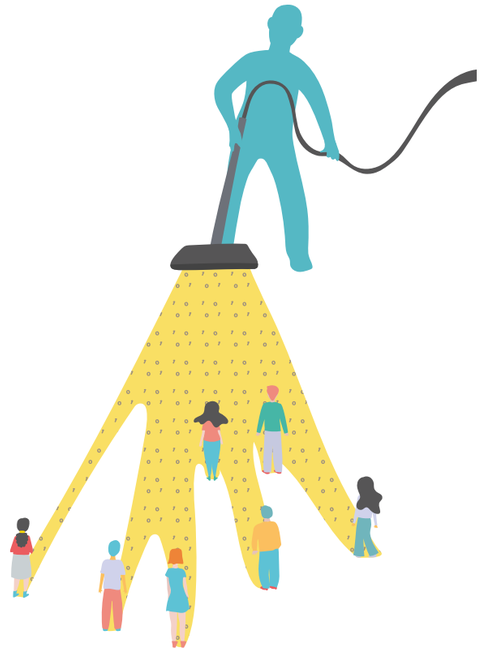
The challenge of global data governance

The fact that attitudes toward privacy, data governance approaches, and technological development strategies differ widely across regions poses a challenge to the development of transnational data governance mechanisms. For example, while China's AI plan focuses on boosting the international competitiveness of its private sector, the United States lets market forces define its data governance approach with the public sector supporting research and entrepreneurship, whereas the EU takes a position where all AI development must place humans at the centre, using data ethics as a guiding approach in both the public and private sectors. Other countries have yet to implement data governance mechanisms altogether, which can raise new sets of challenges.

[38] Furseth 2019

Too much information: The case of Kenya's voter register

Kenyan law requires the voter register to be published prior to elections. In a bid for efficiency and lower costs ahead of the 2017 election, the Kenyan electoral management body (IEBC) published the register online. The data included voters' national identity card number, date of birth and gender alongside their full name and voting area. One could query the database using the national ID number or send a national ID number to a designated SMS.



The Kenya ICT Action Network (KICTANet) noted with concern that the online portal revealed unnecessary information for the purpose of publishing the voter register. Exposure of national ID numbers was of particular concern since the same number is linked to multiple government and private registries. It could therefore be used to link people's data using relational database mining technologies. In addition, the weak security measures of the online portal opened it to the risk of automated data mining. In discussions on a KICTANet online forum, users shared their experiences with querying the IEBC voter register portal. Many explained how they were able to query random numbers. Other reports claimed one could send identity card numbers to the SMS number an infinite number of times.

This sparked debates on how to accomplish the statutory requirement of publishing the voter register without compromising voters' personal data. An IEBC representative was invited to the online forum, where he explained the basis for publishing the register and the issues raised by the public, including the presence of dead voters, mixed up ID numbers and multiple registrations – all concerns that had not been anticipated by the IEBC.

KICTANet made several recommendations for removal of information that was not necessary to comply with the publication requirement, such as date of birth and gender. The publication of ID card number was debatable. While some forum users expressed concerns with using ID information to relate voter data with other databases, others thought that it was the surest way for the public to identify inaccuracies in the voter register. Voter number was suggested as an alternative identifier.

To prevent automated data mining, KICTANet forum users recommended the use of robot deterrents such as captcha. IEBC immediately added the robot deterrent feature. In a matter of days, they also reduced the personal information visible on querying the database. Months after the election, reports indicated that political actors had obtained voter register data and used it to send targeted messages to voters, in some cases manipulating them. Reports also pointed to political parties having obtained the entire voter register.

KICTANet has been undertaking policy research and advocacy for a comprehensive data protection framework for Kenya. The work involved research on the state of data protection in Kenya and engagement with parliamentary committees on ICT. The network gave substantive input to two data protection bills, the status of which KICTANet is monitoring. Although the IEBC eventually improved its privacy practices, it was an ad hoc response to data privacy concerns with the voter register that could have been avoided if a comprehensive data protection framework had been in place.

The Kenyan case illustrates the challenge of public sector digitalisation without privacy impact assessments underpinning technology deployment. However, it can also be interpreted as an opportunity for public interest organisations to advocate for better privacy practices, if public sector organisations are open to critique from the public. Public sector organisations must have the political will to engage meaningfully with those who give input.

Applying ethics beyond virtue signalling

As shown in Annex I, a significant number of ethical codes and principles for the development and use of AI have emerged during the last two years, coming from public and private entities as well as the third sector. Though a promising step, most declarations come in the form of statements (such as "we will ensure our data sets are not biased") and lack actionable recommendations, governance and accountability mechanisms or examples of how to operationalise ethical principles in a way that preserves human rights.

As one working group member observed, this is understandable given that "not all human rights can be translated to digital rights and not all aspects of the digital world fit into a human rights framework." Similarly, the costs of infrastructure needed to secure ethical data treatment (such as paying for alternatives to data giants) could be prohibitive for smaller organisations. The question of how to implement high-level privacy legislation and ethical data guidelines in SMEs and other organisations with fewer resources is one of the key challenges the Digital Future Society programme is working to address. Still, when organisations of any size commit to ethics guidelines without indicating how they will follow them, ethics declarations risk dismissal as window dressing or virtue signalling.

A second challenge of this proliferation of ethical principles is the need for increased coordination or "digital cooperation". A skewed or atomised distribution of effort makes it difficult to assess the scope and effectiveness of data ethics principles in practice. Beyond regulation around data ethics and digital privacy, one of the main challenges that remain is the ethical training of programmers and those designing AI systems. New evidence shows that codes of ethics may have a negligible effect on behaviour change, at least among software developers who are crucial in the design and delivery of automated decision-making systems.[39]

[39] McNamara et al. 2018

Opportunities for more responsible data use

Data, personal data included, can have many positive uses and outcomes. The fact that automated decision-making is becoming central to the technologies we use in our everyday lives is not inherently negative; any individual using a cellphone, or making a bank transaction, or booking a flight has benefitted from them. Similarly, the synchronisation of traffic lights in any city, or the controlled speed of its underground trains, requires ADMS to run smoothly and safely. In addition to the benefits of efficiency gains and lower costs of products and services that result from data-driven systems, several opportunities can be found in ensuring data collection, use and governance is ethical and respectful of privacy.

Competitive advantage of privacy

According to the 2019 Internet Trends report, privacy is steadily becoming a bigger selling point as consumer demand for safer digital communication options increases. Today, 87 percent of global web traffic is encrypted, up from 53 percent three years ago.[40] In markets where consumers progressively set the bar and increasingly value privacy, a company's degree of data ethics awareness and action presents a compelling case to develop ethical products and services, despite the potential costs.

Consensus around explicability

There is an emerging global consensus that autonomous intelligent systems should be designed so that their decisions can be explained. In cases of so-called "black box" algorithms, other explicability measures (traceability, auditability, and transparent communication on system capabilities) may be required, provided that the system as a whole respects fundamental human rights. However, the degree to which explicability is needed is highly dependent on the context and the severity of the consequences if that output is erroneous or otherwise inaccurate.

[40] Molla 2019

Interoperability

Interoperability allows data to flow for commercial, research and government purposes and is an essential ingredient of innovation. According to the United Nations Secretary General's High-Level Panel on Digital Cooperation, there is scope to launch collaborative projects to test the interoperability of data, standards and safeguards across the globe.[41]

Interoperability has the potential to be used not only for data cooperation, but also as a competitive lever that can counteract data concentrations and allow new data market entrants to arrogate network effects.[42] In low-and middle-income countries where limited resources strengthen the promise of digitalisation to improve public service delivery, it is vital that lessons and improvements are shared between cities and other governmental entities nationally and internationally. fAIr LAC is an ambitious project in Latin America and the Caribbean that strives to harness the benefits of AI while working to dispel society's distrust towards automation. For the Inter-American Development Bank who is leading this initiative, the opportunity lies in collaboration through three main activities: sharing predictive models for social policies, strengthening the impact of local entrepreneurship, and building capacity and standards for interoperable AI systems in the region.

[41] The Age of Digital Interdependence 2019

[42] Doctorow 2019

Emergence of new data governance models and tools

The debate on data governance is now moving towards the notion of ecosystems of institutions collaborating under different conditions of consent, and updated conceptualisations of private and public value to maximise public benefits from data. For instance, the Platform for Big Data Agriculture was launched in 2017 by the Colombia-based International Center for Tropical Agriculture after consultation with public, private and non-profit stakeholders.[43] By providing new ways to share agricultural data, this collaboration seeks to transform research and innovation in food security, sustainability and climate change.[44] Another example of an emerging data governance model that employs a collaborative ecosystem approach is that of the data trust.[45]

[43] The Age of Digital Interdependence 2019

[44] CGAIR Platform for Big Data in Agriculture 2019

[45] Mulgan and Straub 2019

Case study: Pooling individual rights to data privacy through data trusts

Data trusts are gaining interest and acceptance as models to steward, maintain, and manage data so that public and private entities benefit from it as a shared resource. Borrowing from the finance field, the idea is to transfer the governance structures of fiduciary trusts that are used to maintain shared resources, such as public land and pension funds, to the governance of data.[46] Data trusts bring opportunities to balance conflicting views and incentives about data access and enable collaboration on common challenges to create new products and services. They can also reduce data sharing costs and create new opportunities for companies innovating with data.[47]

Together with the Open Data Institute, the Office for Artificial Intelligence and Innovate UK are currently piloting the model of data trusts as legal structures that provide independent stewardship of data in three different use cases: urban space data, image and acoustic data at borders to tackle illegal wildlife trade, and sales data to reduce global food waste.[48] In each case, a data trust serves as an independent entity that decides how to use and share data for an agreed purpose. Implementing these pilots involved engagement of stakeholders, legal analysis and advice for a requisite legal structure, design of a decision-making process, assessment of the technical architecture to allow access to data via a data trust, and a viability study.
The experience shows that there is no one single legal structure that fits all data trusts and that each requires its own design and decision making approach that is reflected in its legal model.[49] The pace of decision making processes, for example, will be faster for data trusts for private organisations than for those that steward data for private and public sectors.

Though appetites to pilot this model for data access and sharing are on the increase, the definition of the term data trust remains open as its configuration is not exactly analogous to that of a financial trust. For this reason, it is advisable for public organisations to consider using another term such as data cooperative or data sharing contract. Governments and other actors interested in improving their own data governance models can approach the growing constellation of organisations around the world that are working openly to share experiences and lessons including the Governance Laboratory, the Royal Society, the British Academy, the Data Stewards Network, Element AI, Nesta, and the Centre for International Governance Innovation.

[46] Wylie and McDonald 2018

[47] Hardinges 2018

[48] Theodi.org 2018

[49] Reed et al. 2019

The challenges and opportunities encountered in the implementation of the three pilots enabled the identification of a data trust life cycle that offers useful guidance to public entities looking to test this model of data governance, showing the activities, risks and stakeholders that must be involved at each stage of the implementation process.
It should be noted that security and sustainability are paramount in this data governance model.

The data trust life cycle

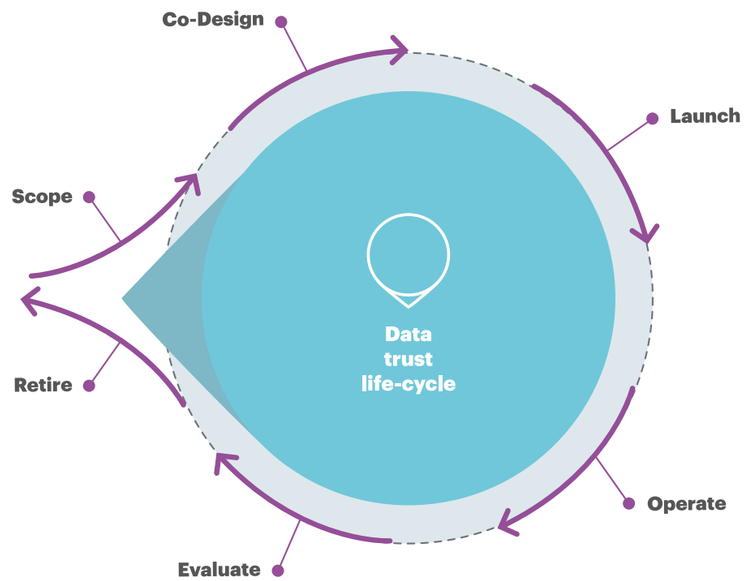


Image source: The odi.org 2018

Impact assessments

Data protection impact assessments (DPIAs) are voluntary measures typically undertaken by public bodies bound to compliance and audits in the healthcare sector. However, applying DPIAs more widely could have positive implications for the design of algorithmic systems and could become a required norm, especially where sensitive personal of data ethics, exploring probable futures that enable us to propose data governance recommendations for the now.

Certifications

Voluntary measures present another set of opportunities to operationalise ethics in the form of certifications for algorithms themselves or for the entire person or process used to make decisions. Fairness and discrimination issues could be considered in certification criteria, as well as the opportunity to proactively incentivise the creation of more scrutable algorithms. The fAIr LAC project sees an opportunity in building local capacity and ethical standards in Latin American countries by working with local firms and governments to provide certificates of excellence in responsible AI.

In this section we have discussed the main challenges and opportunities of ethical data governance as identified by working group experts. The list is non-exhaustive, as more are sure to emerge as digitalisation and AI progress. As concerns around data use and governance build, private and public entities are beginning to show more commitment to tackle the challenges of data ethics and digital privacy. Yet, concrete actions beyond commitment are needed to ensure ethical data collection and use, which must be paramount to policymakers in the coming years. In the next section we consider factors that are likely to determine the landscape of data ethics, exploring probable futures that enable us to propose data governance recommendations for the now.

3

Looking ahead to act now

Digital Future Society

Futures as tools

Futures as tools

The methodology used in Digital Future Society working groups applies the concept of futures as tools to inform the discussion, collective analysis, and strategic anticipation of key challenges and opportunities that could emerge over the next decade.

This concept should not be confused, misused, or misunderstood with the mindset of "predicting the future." In using this approach, our purpose is not to try to predict what will happen in 2030, but rather to apply collective long-term thinking and avoid common hindsight bias when it comes to exploring the impact of data-driven technologies on society. By combining the perspectives of experts from the public, private, academic, and third sectors, we create a holistic vision and narratives to build a deeper, more informed, and strategically valuable understanding of the broader theme of digital trust and security.

The futures as tools methodology creates a space to cultivate a greater and future-proofed value of the actionable recommendations gathered in the working groups, informed by the drivers, trends, and key uncertainties shaping the near futures of emerging technologies and society from multiple perspectives. Each imagines a world in 2030.

Why 2030?

By using the 2030 time horizon, Digital Future Society aims to deliver recommendations in a shared framework that connects to existing transnational narratives, particularly the United Nations Secretary General High-Level Panel on Digital Cooperation and, more broadly, the Sustainable Development Goals (SDGs). 2030 is a temporal reference used by many other governments, international organisations, and transnational initiatives within entities such as the World Economic Forum, the World Bank, and the European Commission.

Our aim is to encourage policymakers use the SDGs as a guiding framework to build a common shared vision of desirable futures when faced with ethical and data governance decisions, especially in light of the goals that are designed to promote stronger institutions, quality education, gender equality, decent work, reduced inequalities and innovation in industry and infrastructure. By looking ahead and explaining what possible futures of a data-driven world might look like, and how it could affect key social, economic and environmental factors, we can catalyse action-oriented policy responses now.

A note on scenario building

Building on the discussion about current challenges and opportunities for public and private entities, the exercise is focused on creating consensus around the likelihood and magnitude of the uncertainties that experts consider will have a greater impact in the coming years. The aim is to anticipate game-changing developments in order to come up with relevant recommendations that address the wide range of challenges and opportunities around data ethics and governance. The expert working group participants identified citizen vs. corporate-owned data and algorithms and high vs. low social involvement in data ethics issues as the uncertainties most critical to explore in order to anticipate and respond to the challenges of the coming decade.

Scenario A: My data, my rules

Engaged citizens drive the data governance agenda

Following a series of critical data breaches and privacy scandals global in scope, citizens care deeply about data and have secured mechanisms for access and ownership of data and algorithms. Hungry for debate and action, civil society groups have organised and mobilised against public and private entities using their personal data for private gain, and have successfully influenced governments to implement laws that support this model. Citizens are largely empowered in this scenario as they have gained full control over how their data is used and to what extent their lives are affected by algorithms. With strengthened capacity for mobilisation and recourse, citizens have unprecedented agency in a data-driven world.

Beyond strong privacy laws at the national level, there is an international alignment around citizens' data rights based on landmark GDPR legislation, "copies" of which have now been adopted globally. The result is a more highly concentrated market as citizens have more power over algorithms and own their data, thereby reducing the chances for some companies to collect and use personal data.

This scenario opens several opportunities for governments to both use and regulate data ethically, not only to improve public services but also to set an example for the private sector. By funding algorithm creation and using ethical principles by default, governments could lead by example in innovative Privacy by Design efforts. The public sector also has the opportunity to redesign the relationship between private and public entities and increase autonomy by reducing the concentration of data and algorithm ownership in private hands.

The challenges that governments will have to face in this scenario include finding ways to operationalise transparency and craft updated policy responses as highly engaged citizens continue to hold them accountable in the ethical collection and use of data. More public investment will be needed to fund entities that conduct non-partisan data ethics research and third party oversight.

Scenario B: Vulnerability by indifference

While enshrined by law, data ethics and privacy are taken for granted

This scenario is characterised by a kind of data fatigue. While legislation exists that ascribes data ownership to citizens and algorithms are open, citizens do not understand and do not care about the consequences of companies using their data, resulting in the practical foregoing of digital rights.

Again in this scenario, landmark GDPR legislation has become an international benchmark, even for previously divergent governments in North America and Asia. Not only have policy attitudes shifted, but compliance and changed practices around data ownership have become the norm in the private sector as well. Namely, it has become standard business practice to state the purpose and specific usage of data while minimising collection. This has resulted in increased technical complexity, a greater need for auditing and higher software prices. Larger companies with more resources to implement data ethics and privacy regulations see significant gains and outcompete smaller startups and SMEs. Lowering the cost of doing business presents a major challenge to both the private and public sectors in this scenario.

Another challenge arises in using data for social good, which becomes more difficult due to “overcorrecting” regulation. While users of technology are focused on the personal, short-term benefits, the role of citizens remains passive. In this scenario, it falls to governments to use data to improve public services in an ethical and privacy-first manner, which can also be viewed as an opportunity for governments to implement participatory data governance policies.

Scenario C: Data as currency for a better society

High social involvement and data ownership concentrated in big corporations

In this scenario, the benefits of digital systems are enjoyed by society. Citizens want to know who has their data and how it is being used. It is widely understood that data is actively owned and collected by a handful of dominant public and private entities. People generally accept that governments and corporations own and use their personal data as the situation is one of a clear and well-enforced regulatory framework around data governance.

Following years of “techlash”, citizens now demand more responsible use of digital platforms and social media from government and business. Strong movements against lack of transparency and misuse of data have led to an increase in the number of class-action lawsuits against companies abusing people’s data and privacy. Now required by law, the explainability of algorithms has made the implementation of automated digital technologies more costly.

A new and necessary understanding of privacy and data ethics has taken hold in business and across society. Organisations use Privacy by Design in their products and services to collect as little data as possible. Citizens like Sorine regularly exercise data rights through subject access requests and portability. Not only can citizens visit a consolidated platform to see which companies have collected their data, but they can actually cancel and erase unwanted transactions. While technically daunting, this type of tool plays an important role in fighting the surreptitious tracking, collection and sale of metadata and other unethical data handling practices. There is also an option to see where the data has gone, the value of its having been shared or sold, together with the ability to seek recourse and even compensation enforced by a global data ethics council.

While there is less room for governments and corporations to misuse data, monetisation is still allowed and data markets have grown around the world. New opportunities for growth arise in the creation of new data economies, markets and income sources. On the other hand, governments face regulatory hurdles at the supranational level, as coordinating a global response to data ethics and privacy challenges proves difficult, especially when it comes to dealing with transnational monopolies in data ownership and handling.

While a handful of companies with high volumes of data and algorithm power have the opportunity to develop a wider range of cheaper products, policymakers face challenges in regulatory enforcement.

Scenario D: Winners take all

Data monopolies meet social indifference

In this scenario, data reaches peak concentration in the hands of what futurist Amy Webb calls The Big Nine: Amazon, Apple, Google, Facebook, IBM, Microsoft, Baidu, Tencent and Alibaba. There is no transparency regarding data use and people are content with digital platforms without giving much thought to data ethics or privacy.

Beyond the now obsolete GDPR, no further efforts to increase digital literacy, data ethics or privacy have been made by governments in Europe or elsewhere. Externalisation of public services is commonplace, with easy-to-use digital applications ubiquitous in public and private services.

Unable to compete with data giants, local shops and small businesses have closed at unprecedented rates and are now exceedingly rare, even in non-digital hubs. Having influenced policy through lobbying and now directly, The Big Nine now have an impact on drafting legislation and regulations to secure their own dominance.

In this scenario, both citizens and government take a passive role in how data is used, leaving regulation completely up to the private sector. Decision-making power over data has been externalised in the public sector, including the electoral process. Privacy protection is designed in the context of intellectual property rights rather than human rights, and all forms of data are considered the property of corporations who use it, not the citizens who supply it. This presents a major barrier for governments who seek to improve public services as they now lack access and ownership to data and must rely on private firms.

4

From analysis to action

Digital Future Society

Toward better data governance

Our increasing reliance on data-driven technologies and systems on a personal and public level has translated to growing ethical concerns tied to data governance, especially in terms of privacy and transparency. The new data ethics landscape requires a multi-faceted and multi-disciplinary approach to addressing the challenges and opportunities described in Section 2.

Recognising that the conversation initiated by this report will be ongoing, we have identified the following set of recommendations that are meant to serve as a starting point for ethical data governance and more broadly, the construction of more equitable digital futures.

Lead by example

1.1 Champion Privacy by Design: toward moral autonomy of digital citizens

Moral autonomy is understood as having control over the way one is seen: a fundamental right that must be respected to the same extent in the digital world as in the physical. With increasing demands for transparency regarding the uses of the data people provide online, governments can gain trust by clearly communicating their actions to citizens.

To action this now, governments can consider adding “What we do with your data” information boxes on public websites and incentivise private entities that want to work with them to do the same. Public entities should strive to deliver public services according to the principles of Privacy by Design.[50] Governments in Estonia, Austria, and India are implementing design features and regulatory frameworks based on principles and practices that aim to ensure data privacy in their national digital ID systems.[51]

[50] See Annex II

[51] World Bank Group 2018

1.2 Choose to go open source by default

Open data policies are one way to promote ethical data use in the delivery of public services. While private companies are not obliged to share details of data collection and algorithm design, they can promote trust by being transparent about known vulnerabilities in software and communicating data breaches in a timely manner. Other values-based digital cooperation efforts can be directed to address specific ethical and transparency-related challenges.

Policymakers can lead by example by using alternatives to dominant data collection platforms. The concentration of data can be reduced through the use of alternative services and solutions, such as those listed by the Danish think tank Data Ethics.[52] The city of Barcelona offers a practical example of how to apply this recommendation in their Ethical Digital Standards policy toolkit.[53]

1.3 Experiment with new data governance models

Governments should collaborate with industry, civil society organisations and academia to pilot new data governance models such as data trusts that improve upon consent-based models of privacy, particularly in departments using or planning to use automated decision-making systems.

When experimenting with new data governance models, policymakers should aim for a sustainable, voluntary, and participatory approach to collecting and using personal data as they deploy data-driven technologies for the delivery or enhancement of public services. Opening up the technological field to include citizens in the creation of algorithms can ensure a more diverse and simultaneously ethical approach to algorithm design and AI deployment.

[52] Dataethics.eu 2018

[53] Barcelona.cat 2018

Operationalise ethics through accountability

2.1 Enforce accountability mechanisms for unethical data use

There must be consequences for data misuse by public and private entities. European efforts to lead regulatory changes toward more stringent data protection practices and Privacy by Design have succeeded in raising awareness around data ethics globally. However, challenges remain regarding the implementation of robust accountability mechanisms.

One sample action that could be implemented immediately is the creation and maintenance of a public list of data brokers. Something as simple as a list of companies that purchase and use personal information could go a long way toward setting a higher bar for privacy-conscious behaviour and accountable data governance.

Policymakers could also compile and publish a compendium of case examples demonstrating how their government or department is operationalising data ethics, together with a plan for regular revisions and updates. In cases of AI deployment, the document should clearly explain the severity level of the consequences of each system, as well as indicate which individual will remain in control of the system.

2.2 Create favourable conditions for a private sector shift toward ethical technology development

Governments have a key role in creating conditions in which ethical data governance does not detract from the competitiveness of small and medium-sized firms. Policymakers need to consider the competitiveness of their local tech sector and introduce mechanisms and measures that support growth in an ethical manner. Regulation must be flexible enough to avoid stifling entrepreneurship and innovation, while serving as a source of new possibilities for trust to be valued by consumers. Public sector support toward private sector compliance with data regulations and ethical principles, such as a subsidy for firms innovating with ethically certified data, could contribute positively to this shift.

Take an inclusive and transparent approach

Transparent data governance is not simply about communicating data ownership or consent, but more crucially when, how, and why data is being used by public and private entities. The working group agreed that public and private entities have an obligation to be transparent, especially when relying on the use of citizen data for public service delivery.

3.1 Address gaps in data literacy by developing and distributing educational programming for online and offline users

In collaboration with stakeholders from the public and private sector, governments should undertake a public education initiative focused on data ethics and privacy to improve data literacy. Such a programme must take into account people's search for a public self and how to exercise one's digital rights, and ensure availability is inclusive (available online as well as offline). Upon finishing the programme, users should understand what organisations do with their data and how to ensure their digital twin has moral autonomy. The case of Finland provides an instructive example with their free online course Elements of AI, from which over 10,000 people have graduated. The country plans to reach 1 percent of its population with the course, or 55,000 citizens.[54]

3.2 Promote a diverse and interdisciplinary AI workforce

The output quality and ethical integrity of an algorithm depends on the assurance that the inherent bias of programmers has not transferred to code. A diverse group of programmers reduces the risk of embedding bias into algorithms and enables a fairer and higher quality output.

To reach representational parity, and to ensure digital rights are considered from multiple perspectives, it is crucial to promote a diverse workforce that includes underrepresented groups (most notably along gendered, racial, and economic lines). Policymakers also have a role in ensuring an interdisciplinary approach to increasing transparency and accountability. Lawyers, interface designers, sociologists, and ethicists must work alongside computer engineers if we are to operationalise ethics and the rule of law in algorithmic system design.

[54] Decker 2019

A call to action

Throughout history, societies have always somehow managed to act when faced with globally far-reaching risks. Public and private entities have had to adapt to these requirements not only with targeted risk assessment and accountable management, but by innovating and evolving in new ways. They will have to do the same in a data-saturated environment. Through new regulations, global standards, formal accountability systems that citizens can trust, and slow but steady cultural adaptation, we can continue to reach new levels of awareness, education, data literacy and better data governance when it comes to the design and deployment of data-driven technologies.

We conclude this report by challenging policymakers to test the recommendations proposed in this report, whether through regulatory sandboxes, pilot zones, trial periods or prototyping. Only through experimentation and evidence-based policy can we move from reflection to action in our quest for a more equitable and inclusive digital future.

References and acknowledgements

Digital Future Society

References

Algorithm Watch. (2018). *Automating Society Taking Stock of Automated Decision-Making in the EU*. Available at: https://algorithmwatch.org/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf

Barcelona.cat. (n.d.). *Ethical Digital Standards: Executive Summary*. [online] Available at: https://www.barcelona.cat/digitalstandards/en/data-management/0.1/summary

Building Ethics Into Privacy Frameworks For Big Data and AI. (2018). [PDF] United Nations Global Pulse and the International Association of Privacy Professionals. Available at: https://iapp.org/media/pdf/resource_center/BUILDING-ETHICS-INTO-PRIVACY-FRAMEWORKS-FOR-BIG-DATA-AND-AI-UN-Global-Pulse-IAPP.pdf

Cavoukian, A. (n.d.). *Privacy by Design: The Seven Foundational Principles*. [PDF] Privacy and Big Data Institute. Available at: https://www.ryerson.ca/content/dam/pbdce/seven-foundational-principles/The-7-Foundational-Principles.pdf

CGIAR Platform for Big Data in Agriculture. (2019). *CGIAR Platform for Big Data in Agriculture*. [online] Available at: https://bigdata.cgiar.org/

Dataethics.eu. (2018). *Data Ethics Tools for Companies and Organisations - Dataethical Thinkdotank*. [online] Available at: https://dataethics.eu/tools/

Delcker, J. (2019). *Finland's grand AI experiment*. [online] POLITICO. Available at: https://www.politico.eu/article/finland-one-percent-ai-artificial-intelligence-courses-learning-training

Doctorow, C. (2019). *Adversarial Interoperability: Reviving an Elegant Weapon From a More Civilized Age to Slay Today's Monopolies*. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2019/06/adversarial-interoperability-reviving-elegant-weapon-more-civilized-age-slay

Edwards, L. and Veale, M. (2017). Slave to the Algorithm? *Why a Right to Explanation is Probably Not the Remedy You are Looking for. SSRN Electronic Journal*.

Figure Eight. (2019). *The Artificial Intelligence (AI) Glossary*. [online] Available at: https://www.figure-eight.com/resources/the-artificial-intelligence-glossary

Floridi, L. and Taddeo, M. (2016). *What is data ethics?* Philosophical Transactions A, Royal Society Publishing. [PDF] Available at: https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2016.0360

Furseth, J. (2019). *The big picture: What we lost in the wilderness years of photo storage*. [online] Findingctrl.nesta.org.uk. Available at: https://findingctrl.nesta.org.uk/in-the-wilderness-years-of-photo-storage

Hardinges, J. (2018). *What is a data trust? – The ODI*. [online] Theodi.org. Available at: https://theodi.org/article/what-is-a-data-trust/

Hardinges, J. and Wells, P. (2018). *Defining a data trust*. [online] Theodi.org. Available at: https://theodi.org/article/defining-a-data-trust/

Iapp.org. *General Data Protection Regulation*. [online] Available at: https://iapp.org/resources/article/general-data-protection-regulation/#

Ingold, D. and Soper, S. (2016). *Amazon Doesn't Consider the Race of Its Customers. Should It?*. [online] Bloomberg.com. Available at: https://www.bloomberg.com/graphics/2016-amazon-same-day/

Inside Privacy. (2019). *Thailand Adopts Personal Data Protection Act*. [online] Available at: https://www.insideprivacy.com/data-privacy/thailand-passes-personal-data-protection-act/

Katwala, A. (2018). *How to make algorithms fair when you don't know what they're doing*. [online] Wired.co.uk. Available at: https://www.wired.co.uk/article/ai-bias-black-box-sandra-wachter

Liao, T. (2018). *China Publishes National Standard for Personal Data Protection*. [online] Morganlewis.com. Available at: https://www.morganlewis.com/pubs/china-publishes-national-standard-for-personal-data-protection

McNamara, A., Smith, J. and Murphy-Hill, E. (2018). Does ACM's code of ethics change ethical decision making in software development?. *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering - ESEC/FSE 2018*.

Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S. and Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2).

Molla, R. (2019). *Mary Meeker's most important trends on the internet*. [online] Vox. Available at: https://www.vox.com/recode/2019/6/11/18651010/mary-meeker-internet-trends-report-slides-2019

Mulgan, G. and Straub, V. (2019). *The new ecosystem of trust*. [online] nesta. Available at: https://www.nesta.org.uk/blog/new-ecosystem-trust/

Müller-Eiselt, R. (2018). *An Ethics for Algorithmists – Lessons Learned from Effective Professional Ethics*. [online] Ethics of Algorithms. Available at: https://ethicsofalgorithms.org/2018/09/24/an-ethics-for-algorithmists-lessons-learned-from-effective-professional-ethics

Nytimes.com. (2019). *The New Terminology for Privacy*. [online] Available at: https://www.nytimes.com/interactive/2019/04/10/opinion/internet-privacy-terms.html

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

Powles, J. and Nissenbaum, H. (2018). *The Seductive Diversion of 'Solving' Bias in Artificial Intelligence*. [online] Medium. Available at: https://medium.com/s/story/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53

Privacy and Data Protection Policy 2018 - Kenya. (2018). [PDF] The Government of Kenya. Available at: http://www.ict.go.ke/wp-content/uploads/2018/08/Kenya-Data-Protection-Policy-2018-15-8-2018.pdf

Reed, C., BPE Solicitors, Pinsent Masons (2019). *Data trusts: legal and governance considerations*. [PDF] Available at: http://theodi.org/article/data-trusts-legal-report/

Salleh Rahaman, A. (2015). *Data Protection Policy*. [PDF] E-Government National Centre of Brunei. Available at: http://www.information.gov.bn/PublishingImages/SitePages/New%20Media%20and%20IT%20Unit/Data%20Protection%20Policy%20V.2.2.pdf

Schermer, B. (2011). The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, 27(1), pp.45-52.

Theodi.org. (2018). *UK's first 'data trust' pilots to be led by the ODI in partnership with central and local government – The ODI*. [online] Available at: https://theodi.org/article/uks-first-data-trust-pilots-to-be-led-by-the-odi-in-partnership-with-central-and-local-government/

The World Bank Group. (2018). *Privacy by Design: Current Practices in Estonia, India, and Austria. Identification of Development (ID4D)*. [PDF] Available at: https://id4d.worldbank.org/sites/id4d.worldbank.org/files/PrivacyByDesign_112918web.pdf

Turilli, M. and Floridi, L. (2009). The ethics of information transparency. *Ethics and Information Technology*, 11(2), pp.105-112.

United Nations Secretary General's High-Level Panel on Digital Cooperation. (2019). *The Age of Digital Interdependence*. [PDF] Available at: https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf

van den Hoven, J. (2008). *Information technology, privacy, and the protection of personal data, in Information technology and moral philosophy*, J. Van Den Hoven and J. Weckert (eds.), Cambridge: Cambridge University Press, pp. 301–322.

Vincent, J. (2019). *AI is worse at identifying household items from lower-income countries*. [online] The Verge. Available at: https://www.theverge.com/2019/6/11/18661128/ai-object-recognition-algorithms-bias-worse-household-items-lower-income-countries

VPRO (2018). *Algorithms Rule Us All*. [video] Available at: https://www.youtube.com/watch?v=NFF_wj5jmiQ

Warren, S. and Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), p.193.

Webb A., Giralt, E., Palatucci, M. & Perez, K. (2019). Tech Trends Report. [PDF] Future Today Institute.

Wendy, D. & Pesenti, J. (2017). Growing the Artificial Intelligence Industry in the UK. [PDF] GOV.UK. Available at: https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk

Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., Myers West, S., Richardson, R., Schultz, J. and Schwartz, O. (2018). AI Now Report 2018. [PDF] New York: AI Now Institute. Available at: https://ainowinstitute.org/AI_Now_2018_Report.pdf

World Economic Forum. (2019). *The Global Risks Report*. 14th ed. [PDF] Geneva: World Economic Forum. Available at: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Wylie, B. and McDonald, S. (2018). *What Is a Data Trust?*. [online] Centre for International Governance Innovation. Available at: https://www.cigionline.org/articles/what-data-trust

Acknowledgements

Lead author

- **Adriana Diaz** – Researcher, Digital Future Society Think Tank

Co-author

- **Nicole Harper** – Editor, Digital Future Society Think Tank

Expert contributors

This report draws on the expertise and inputs of the following expert contributors:

- **Aimee van Wynsberghe** – Co-Director, Foundation for Responsible Robotics and Assistant Professor, Ethics and Philosophy of Technology, Delft University of Technology
- **Arran Riddle** – Content Director for Policy and Regulation, GSMA
- **Artur Serra** – Deputy Director, i2cat and Leadership Member, European Network of Living Labs
- **Atia Cortes** – Computer Science Engineer and Artificial Intelligence Researcher, Polytechnic University of Catalonia
- **Cesar Buenadicha** – Chief Discovery Officer, Inter-American Development Bank
- **Fabro Steibel** – Executive Director, Institute for Technology and Society of Rio de Janeiro
- **Grace Mutung'u** – Associate, Kenya ICT Action Network (KICTANet)
- **Jade Nester** – Director of Consumer Policy, GSMA
- **Joan Roses** – Editor, Collateralbits
- **Lavinia Marin** – Ethics and Philosophy of Technology Lecturer, Delft University of Technology
- **Marc Blasi** – Big Data Project Manager, CaixaBank
- **Marc Torrent –** Big Data Analytics Director, Eurecat and Director, Big Data Center of Excellence Barcelona
- **Sandra Alvaro** – Researcher, Centre de Cultura Contemporània de Barcelona
- **Tarek Besold** – Artificial Intelligence Lab Lead, Alpha Health and Chair, German National Standards Working Group on Artificial Intelligence
- **Ulises Cortes** – Scientific Coordinator, High-Performance Artificial Intelligence, Barcelona Supercomputing Center
- **Victoria Anderica** – Transparency Project Lead, Madrid City Council

Digital Future Society Think Tank team

Thank you to the following Digital Future Society Think Tank colleagues for their input and support in the production of this report:

- **Carina Lopes** – Head of the Digital Future Society Think Tank

Citation

Please cite this report as:

- Digital Future Society. (2019). Towards better data governance for all: Data ethics and privacy in the digital era. Barcelona, Spain.

Appendices

Digital Future Society

Annex I: Global inventory of data ethics frameworks and principles

There is no shortage of suggestions for how data-driven technologies should be ethically governed, as demonstrated by this non-exhaustive list. From governmental initiatives to supranational efforts, the past three years alone have seen a growing number of principles, declarations, voluntary commitments and framework proposals for the ethical use of data and AI.

Organisation	Year	Principles	Sector	Source
Datenschutzkonferenz	Apr 2019	Hambach Declaration on Artificial Intelligence (in German)	Private	Algorithm Watch
European Commission (AI-HLEG)	Apr 2019	Ethics guidelines for trustworthy AI	Public	Rathenau Instituut
Bundesverband KI	Mar 2019	KI certificate (in German)	Private	Algorithm Watch
Information Commissioner's Office (ICO)	Mar 2019	AI auditing framework blog	Public	UK Government
Google	Jan 2019	AI Governance	Private	Rathenau Instituut
Smart Dubai	Dec 2018	Artificial Intelligence Ethics and Principles	Public	Algorithm Watch
Atomium – EISMD (AI4People)	Nov 2018	AI4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations	NGOs	Algorithm Watch

Organisation	Year	Principles	Sector	Source
Danish Expert Group on Data Ethics (DATAETIK)	Nov 2018	Data for the Benefit of the People	Public	Algorithm Watch
DataforGood	Nov 2018	Hippocratic Oath for the Data Scientist (in French)	Private	Algorithm Watch
World Bank	Nov 2018	Privacy by Design: current practices in Estonia, India and Austria	Multilateral development bank	The World Bank
CIGREF	Oct 2018	Digital Ethics	Private - Public	Algorithm Watch
Privacy Commissioner and Government Chief Data Steward, New Zealand	Oct 2018	Principles for safe and effective use of data and analytics	Public	NZ Government
The Public Voice	Oct 2018	Universal Guidelines for Artificial Intelligence	NGOs	Rathenau Instituut
Association for Computing Machinery - US Public Policy Council	Sep 2018	ACM Code of Ethics and Professional Conduct	Private	Rathenau Instituut
European Commission	Sep 2018	Code of Practice on Disinformation	Public	Algorithm Watch
IBM	Sep 2018	Ethics for AI: A practical guide for designers and developers	Private	Rathenau Instituut

Organisation	Year	Principles	Sector	Source
SAP	Sep 2018	Guiding principles for AI	Private	Rathenau Instituut
Deutsche Telekom	Aug 2018	Digital Ethics Guidelines on AI	Private	Algorithm Watch
Amnesty International and Access Now	Jul 2018	The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems	NGOs	Rathenau Institut/ Algorithm Watch
Centre for International Governance Innovation (CIGI)	Jul 2018	Toward a G20 Framework for Artificial Intelligence in the Workplace	Public	Algorithm Watch
Google	Jun 2018	Artificial Intelligence at Google: Our Principles	Private	Rathenau Instituut
Bertelsmann Foundation, iRights.lab	May 2018	Algo.Rules	Private	Algorithm Watch
Partnership on AI	Apr 2018	Tenets	Private - NGOs	Rathenau Instituut
UK House of Lords	Apr 2018	AI in the UK: Ready, willing and able?	Public	Rathenau Instituut
Cédric Villani, Mathematician and Member of the French Parliament	Mar 2018	For a meaningful artificial intelligence: Towards a French and European strategy	Public	Rathenau Instituut
European Group on Ethics in Science and New Technologies	Mar 2018	Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems	Public	Rathenau Instituut

Organisation	Year	Principles	Sector	Source
Bitkom	Feb 2018	Recommendations for Responsible Use of AI and Automated Decisions Corporate Digital Responsibility and Decision Making (in German)	Private	Algorithm Watch
World Government Summit 2018 (Dubai)	Feb 2018	Summary Report 2018 (AI)	Public	Rathenau Instituut
Microsoft	Feb 2018	The Future Computed	Private	Rathenau Instituut
Telefonica	Feb 2018	AI principles of Telefonica	Private	Rathenau Instituut
Data Ethics	Dec 2017	Data Ethics Principles	Private	Algorithm Watch
IEEE	Dec 2017	Ethically aligned design	Private	Rathenau Instituut
Information Technology Industry Council	Nov 2017	ITI AI Policy Principles	Private	Rathenau Instituut
UNI Global Union	Nov 2017	Top 10 Principles for Ethical Artificial Intelligence	NGOs	Rathenau Instituut
University of Montreal - Forum on the socially responsible development of AI	Nov 2017	The Montreal Declaration for a Responsible Development of Artificial Intelligence: A participatory process	Private	Rathenau Instituut

Organisation	Year	Principles	Sector	Source
IBM	Oct 2017	IBM data responsibility	Private	Rathenau Instituut
Future of Life Institute	Aug 2017	Asilomar AI principles	Private - NGOs	Rathenau Instituut
Federal Ministry of Transport and Digital Infrastructure Ethics Committee	Jun 2017	Automated and Connected Driving (in German)	Public	Algorithm Watch
Center for Democracy & Technology (CDT)	May 2017	Digital Decisions	Public	Algorithm Watch
Association for Computing Machinery US Public Policy Council	Jan 2017	Statement on Algorithmic Transparency and Accountability	Private	Rathenau Instituut/ Algorithm Watch
Fairness , Accountability, and Transparency in Machine Learning	Nov 2016	Principles for Accountable Algorithms and a Social Impact Statement for Algorithms	Private	Algorithm Watch
Accenture	Jun 2016	Universal Principles of Data Ethics	Private	Algorithm Watch
Bitkom	Sep 2015	Guidelines for big data applications (in German)	Private	Algorithm Watch
Critical Engineering Working Group	Oct 2011	The Critical Engineering Manifesto	Private	Algorithm Watch

Annex II: Privacy by Design - Core Principles and Practices

Developed by Dr. Ann Cavoukian in the 1990s, Privacy by Design is a framework that addresses the ever-growing and systemic effects of information and communication technologies, business practices, and of large-scale networked data systems. Seven core principles inform the foundation of eleven fair information practices, both of which are listed below.[55]

- **Principle 1:** Proactive not reactive: preventative not remedial
- **Principle 2:** Privacy as the default setting
- **Principle 3:** Privacy embedded into design
- **Principle 4:** Full functionality: positive-sum, not zero-sum
- **Principle 5:** End-to-end security: full lifecycle protection
- **Principle 6:** Visibility and transparency: keep it open
- **Principle 7:** Respect for user privacy: keep it user-centric

Eleven Fair Information Practices	
Purpose specification	The purposes for which personal information is collected, used, retained, and disclosed shall be communicated to the individual (data subject) at or before the time the information is collected. Specified purposes should be clear, limited, and relevant to the circumstances.
Collection limitation	The collection of personal information must be fair, lawful, and limited to that which is necessary for the specified purposes.
Data minimization	The collection of personally identifiable information should be kept to a strict minimum. The design of programs, information and communications technologies, and systems should begin with non-identifiable interactions and transactions, as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimised.
Use, retention and disclosure limitation	The use, retention, and disclosure of personal information shall be limited to the relevant purposes identified to the individual, for which he or she has consented, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.
Security	Entities must assume responsibility for the security of personal information (generally commensurate with the degree of sensitivity) throughout its entire life cycle, consistent with standards that have been developed by recognised standards development bodies.
Accountability	The collection of personal information entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual. When transferring personal information to third parties, equivalent privacy protection through contractual or other means shall be secured.
Openness	Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.
Consent	The individual's free and specific consent is required for the collection, use, or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.
Accuracy	Personal information shall be as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes.
Access	Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
Compliance	Organisations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal.

[55] The World Bank Group 2018


Digital
Future Society