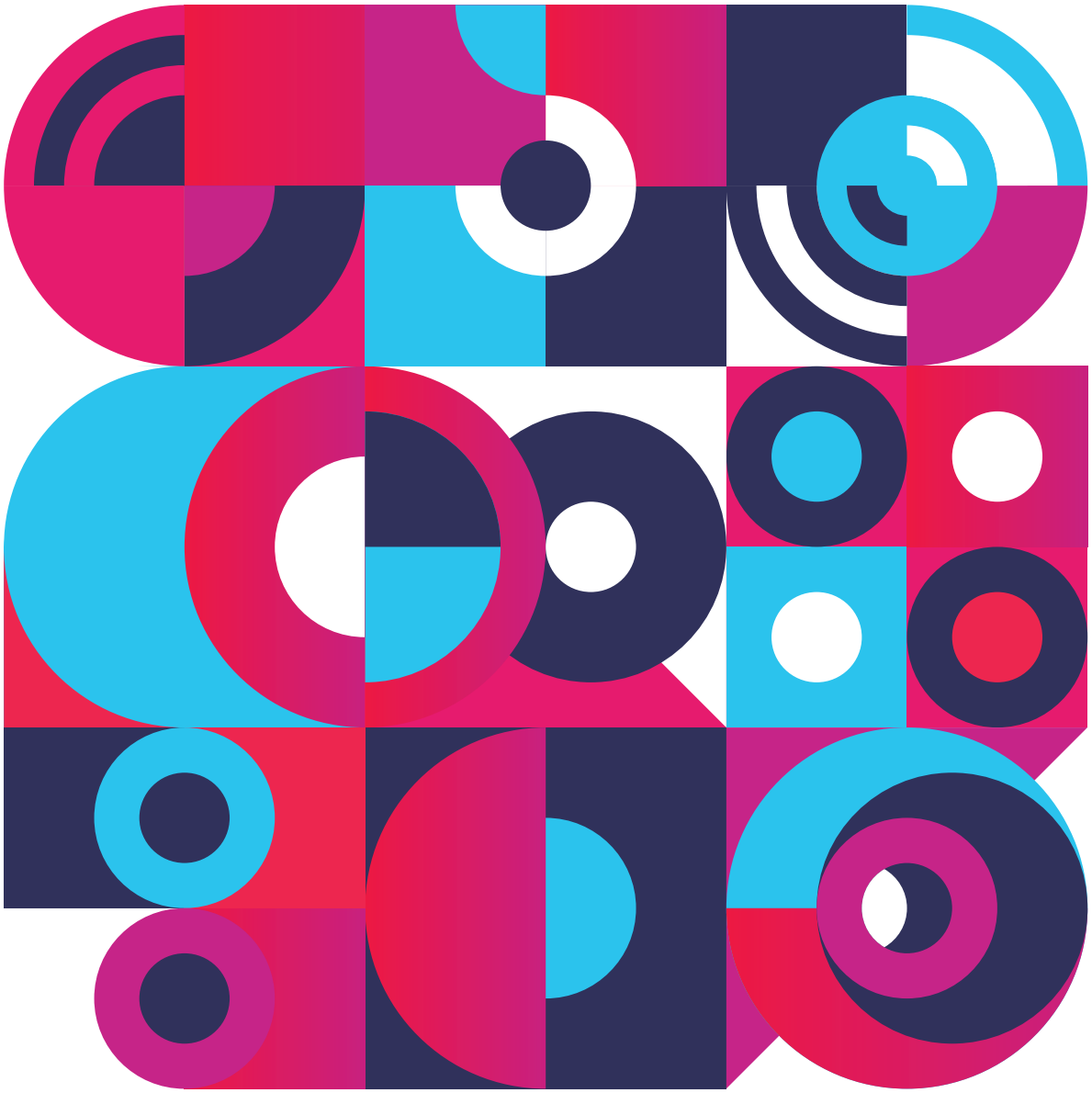
universität wien

DIGITAL TRANSFORMATIONS FOR HEALTH LAB

GOVERNING HEALTH FUTURES 2030



Data Solidarity Glossary 2024

universität wien

DIGITAL TRANSFORMATIONS FOR HEALTH LAB

GOVERNING HEALTH FUTURES 2030

Data Solidarity Glossary 2024

Barbara Prainsack
Research Platform Governance of Digital Practices and Department of Political Science, University of Vienna, Austria.

Ilona Kickbusch
Digital Transformations for Health Lab, University of Geneva, Switzerland.

This report has been made possible by financial contribution from Fondation Botnar, Switzerland, to the Project IMG-22-005 “Digital Transformations of Health Lab (DTH-Lab). Their commitment to advancing global health is deeply appreciated, and this project would not have been possible without their contribution. DTH-Lab is hosted by Université de Genève (UNIGE), Switzerland.

DTH-Lab is committed to ensuring and enabling Global Access. The knowledge and information gained from the Project will be promptly and broadly disseminated and its ‘Funded Developments’ will be made available and accessible free of costs. The Global Access Commitments will survive the term of the Project.

Suggested citation: Prainsack, B,. & Kickbusch, I. (2024). Data Solidarity Glossary. Geneva: Digital Transformations for Health Lab.

Design by Inís Communication

Contents

Contents

Acknowledgements

We are grateful to all members of the data solidarity research programme, as well as Seliem El-Sayed, Torsten Möller, Péter Ferenc Gyarmati, Bernhard Jordan and Laura Koesten for their involvement in the development of the PLUTO tool. We thank Seliem El-Sayed, Nikolaus Forgó, Lukasz Szoszkiewicz, Philipp Baumer, Theresa Henne, Katja Mayer and Gertrude Saxinger for their contributions to the White Paper on Data Solidarity, parts of which have influenced this glossary. The entry on public value draws on research by Connor Hogan. We thank Caitlin Harjes, Louise Holly and Ananya Choyal for help with formatting and editing the manuscript. We are grateful to Antonia Modelhart, Anurag Agrawal, Connor Hogan, Deborah Drgac, Deborah Mascalzoni, Elias Weiss, Gertrude Saxinger, Katharina Kieslich, Kazuto Kato, Njide Ndili and Rohinton P. Medhora for helpful comments on this manuscript and to Eric Sutherland for his – as always, perceptive and thoughtful – comments, edits and amendments.

About the glossary

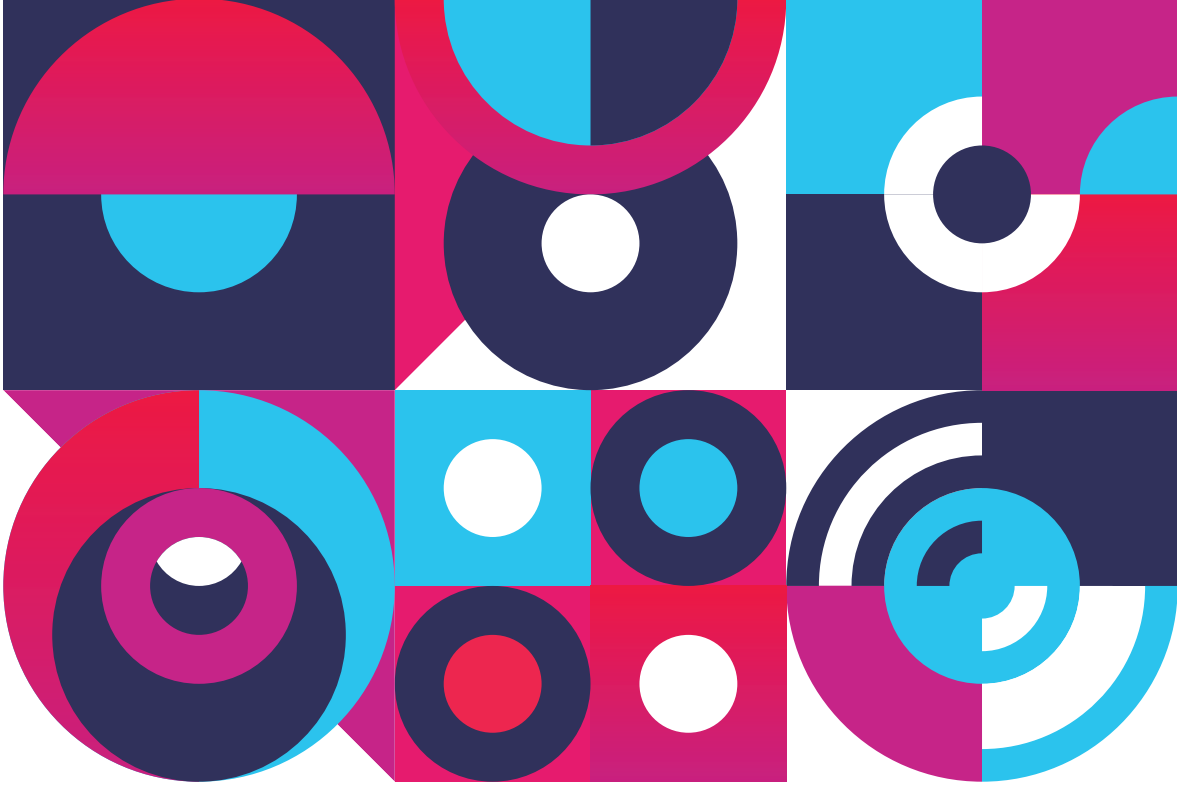
This glossary was developed within the Data Solidarity Work Programme, a multidisciplinary collaboration of researchers and policy makers led by Professor Barbara Prainsack at the University of Vienna. Since 2024, the Data Solidarity Work Programme has also been affiliated with the Digital Transformations for Health Lab (DTH-Lab) led by Professor Ilona Kickbusch. This cooperation underlines the high relevance of data solidarity for health in the context of digital transformations.

This glossary seeks to clarify key concepts relevant to data solidarity and explain data solidarity's relationship to other key concepts and instruments in the domain of data governance and data ethics. It complements previous publications on this topic and in particular, the White Paper on Data Solidarity. Throughout, the glossary aims to indicate why data solidarity must become integral to data use in the health ecosystem.

The first section of the glossary starts with a clarification of key terms that are central to the data solidarity approach. Section two then moves on to discuss key approaches to data governance. Section three introduces concepts that are related to data solidarity, either because of related practices or in that they may be confused with data solidarity. Our discussion of related concepts focuses both on a basic definition of these concepts and on clarifying their relation to data solidarity. Section four takes on ethical challenges and refers to important approaches that analyse the new dimensions of power and inequality that have emerged with digital transformations. Section five underlines key issues that can help move us forward and ends with a strong plea for a new concept of digital health citizenship.

This glossary is a starting point to be followed by additional materials focused on the application of data solidarity in the health ecosystem. The DTH-Lab is also engaged in providing information on other instruments to complement the regulatory approaches that have been taken in Europe. We decided to include some examples from Europe because they are a first globally and have begun to influence governance approaches elsewhere.

We hope the glossary will help clarify the need for a data solidarity approach in health and lead to many engaged discussions on its application.



Section 1: Solidarity

1.1 Solidarity

Solidarity is a crucial element for building fairer societies, where all people have access to the same opportunities to achieve health, well-being and other goods.

Solidarity has many meanings. To better understand solidarity, this glossary takes Barbara Prainsack and Alena Buyx's definition as a starting point. These authors define solidarity *as a practice that reflects people's commitments to supporting others with whom they recognize similarity in a relevant respect*. The similarities between the members of these "communities of interest" are not necessarily objectively measurable characteristics. They can be a shared goal, a joint fight against oppression or a part of social or political identity. In principle, none of these characteristics or commonalities are more important than others: What connects people to others is dependent on the specific situation or practice in question.

Solidarity is often described as a social value, with changing norms leading to new solidarities emerging. For example, intergenerational solidarity in relation to climate action or gender-based solidarities. But solidarity in one sphere does not necessarily carry over into another: while a person of the same gender may support another when the latter becomes the target of gender-based harassment, the same person may not act in solidarity

Table 1: The tiers of solidarity

	**Interpersonal solidarity**	Practices of solidarity practised between individuals
	**Group-based solidarity**	Practices of solidarity exercised within communities of interest
	**Institutionalized solidarity**	Legal, administrative, bureaucratic norms that define and implement mechanisms of solidarity Formal institutions

with the other in a context where their political values or actions set them apart. In other words, solidarity takes place when people act upon things that they consider themselves as having in common with others – as a community of interest – rather than acting upon their differences.

While solidarity is not a replacement for justice, it can help to counteract injustices and unite people behind shared goals. In this sense, solidarity can be a mechanism to promote the common good not only within but also between countries.

Prainsack and Buyx also distinguish three tiers of solidarity (see **Table 1**): Tier 1 is the level of interpersonal solidarity: It takes place when individual people enact solidarity with others who they consider themselves connected to in some relevant way. Tier 2 is the level of group-solidarity: It takes place when solidaristic practice becomes 'normal' behaviour in a group. Tier 3 is the level of institutionalized solidarity: It takes place when legal, bureaucratic, administrative or social norms reflect a solidaristic spirit. It also includes formal solidaristic institutions. Solidaristic institutions are those to which people contribute according to their ability and from which they receive support based on their need.

The paradigmatic case of a solidaristic institution is universal health coverage (UHC). It means that all people have access to the full range of quality health services they need, when and where they need them, without financial hardship. This includes financial solidarity, the models for which differ in different countries and health systems and the pooling of risks. In relation to health, there are also other forms of solidarity: behavioural solidarity (donating organs, foregoing non-urgent interventions if others need them more urgently), solidarity in terms of sharing data and monitoring solidarity (to manage one's health in a responsible manner). Understood in this manner, solidarity can give guidance to the development of policies and the building of institutions in various fields of policy and practice. Among other things, it has also been used to develop a new approach to data governance (see **Data solidarity**). Solidarity is also considered a key principle of international health cooperation as expressed in the Political Resolution of the High-Level Meeting on UHC at the United Nations in 2023.

References: Dawson & Verweij, 2012; Prainsack, 2022; Prainsack & Buyx, 2011; Samochowiec & Müller, 2021; Sangiovanni & Viehoff, 2023; UHC 2030, undated; van Till et al., 2023.

1.2 Data solidarity

Data solidarity is an approach that seeks to achieve a more equitable sharing of benefits and risks emerging from digital practices. Moreover, not only individual people, but also communities and other collectives need to be able to exercise meaningful control over how data is used, by whom and for whose benefit.

Current health data governance frameworks have been designed to protect primary data subjects – meaning the people who the data come from – and especially sensitive information such as their medical data. In digital societies, however, the risks and benefits of digital practices – ranging from data creation to secondary data use – can affect a much wider range of people and include many more data points from everyday life and behaviours. Data from one group can be used to benefit or discriminate against another group. This is why it is not sufficient to protect the people that the data come from. Moreover, digital practices are also embedded in stark power asymmetries, both within and across countries. Addressing these challenges and inequalities requires an approach that goes beyond merely giving people more control over their own data – just as in public health we understand that individual health rights need to be complemented by public health measures.

Data solidarity comprises three pillars (see **Table 2**):

Pillar I focuses on making data use easier when it promises to bring great benefits to people without posing significant risks to individual people or communities. This can be done by easing regulatory burdens or by providing public funding.

Pillar II seeks to prevent harm, for example by effectively prohibiting data uses that pose high risks. As not all harm can be prevented effectively, there is also the need to mitigate it. It is important that all people who have experienced harm from data use are supported. At present, this is often not the case, for example, when people have no access to legal remedies because no law was broken or because they cannot pinpoint who is responsible for the harm (the latter is becoming increasingly difficult

Table 2: The three pillars of data solidarity

Pillar I	Pillar II	Pillar III
Facilitating data use that creates significant public value	Harm prevention and harm mitigation	Sharing commercial benefits with communities
E.g. via deregulation, public support for data use	E.g. via prohibiting data uses that are known to harm individuals or communities and via the establishment of Harm Mitigation Bodies	E.g. via taxes or benefit sharing agreements

to recognize when data is shared multiple times in different settings).

Pillar III mandates that commercial profits from data use should be shared with the people and communities that have enabled the data use in the first place, for example via their actions as patients, citizens and via the public infrastructures that commercial entities use. Commercial profits can be shared via taxation or various other forms of benefit sharing (e.g. benefit sharing agreements with local communities).

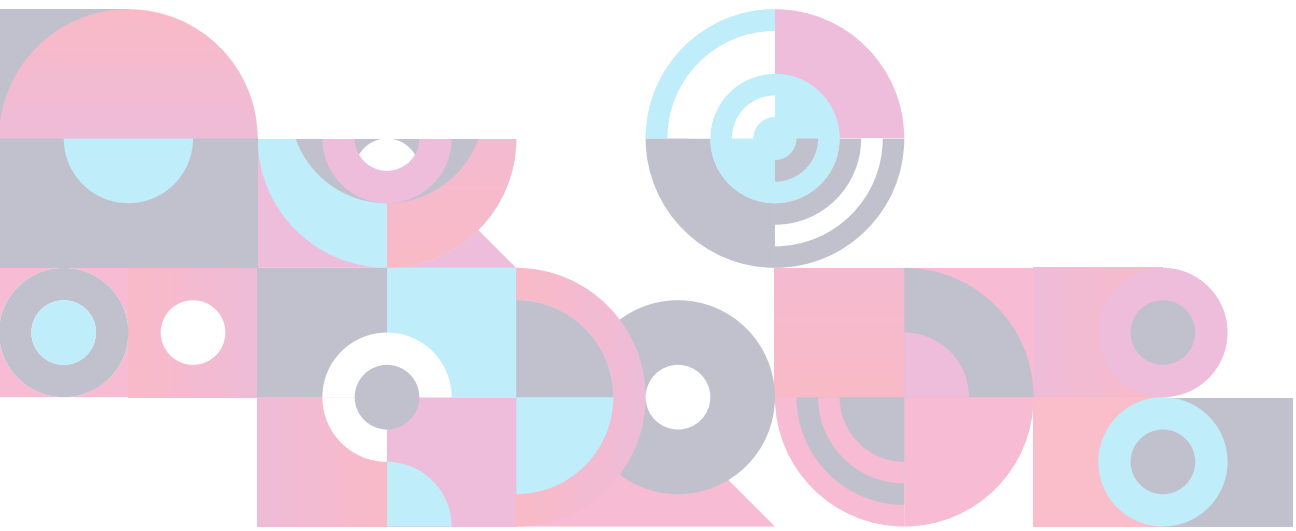
Data solidarity requires two important shifts in our thinking and acting compared to the status quo.

First, the assumption in existing data governance frameworks is often that the re-identification of individuals is the main risk emerging from data use and that some data types are 'riskier' to use than others. Data solidarity, in contrast, assumes risks lie in data *uses* rather than traditional approaches that focus on data *types*. In instances of data analytics linking different types of data, even the most innocuous data set can lead to insights that can harm people when they are linked with other datasets. Data solidarity mandates that types of data use that entail few risks to individuals and communities and are likely to yield considerable benefits should be treated differently from data uses that do the opposite (see also **Public value** and **Box: PLUTO tool**).

Second, in addition to individuals having rights and obligations with respect to their personal health, data solidarity makes use of collective instruments of control and oversight, including data commons, stronger use of binding law to support data use with high public value and outlaw harmful data use and much more.

In its report, complemented by a White Paper on Data Solidarity, *The Lancet* and *Financial Times* Commission on Governing health futures 2030: Growing up in a digital world outlined why solidarity must be one of the core principles on which any approach to health data governance is based. A solidarity-based approach to health data must be considered a defining feature of 21st century public health at national and global levels, aligned with equity as a key value of public health.

References: Braun & Hummel, 2022; El-Sayed et al., 2023; Kickbusch et al., 2021; McMahon et al., 2020; Prainsack et al., 2022a,b.



1.3 Digital solidarity

Digital solidarity refers to the use or capacity of digital technologies and online platforms to facilitate collaboration, both between countries and between communities, especially in times of crisis or need.

Digital solidarity is often used to describe a strategy that enhances the cooperation between countries to work together on joint goals in relation to the use of digital technologies, especially in times of crisis. Most recently – based, in part, on the experiences during the COVID-19 pandemic – digital solidarity has been proposed as an alternative to the concept of digital sovereignty (see **Digital sovereignty**). There is also a mounting concern in relation to efforts that contribute to erode a shared digital ecosystem, leading to an internet model that is less open, less safe and less economically beneficial for all.

Rather than shifting to closed technological ecosystems, it is suggested that policymakers move toward digital solidarity across borders, as a framework for enhancing economic progress, national security and other societal interests among open, democratic and rule-bound societies. For example, the European Union called for "EU Digital Solidarity: a pan-European approach against the pandemic". Similarly, the proposed Global Digital Compact of the United Nations aims to "outline shared principles for an open, free and secure digital future for all" and improve digital cooperation as a key feature of multilateral cooperation. There are increasing calls for regulating data use across borders globally.

Practices such as online fundraising campaigns, social media movements, collaborative problem-solving through digital platforms or the use of technology to address social issues and advocate for justice and inclusion have also been referred to as an expression of digital solidarity. This use of the concept highlights the capacity of technology to build a sense of community and to address challenges collectively in the digital age. It involves harnessing digital tools and resources to overcome economic, social and political asymmetries; and assisting those who may have limited access to technology or face various forms of digital exclusion.

The concept of digital solidarity is sometimes also used to appeal to a willingness to share data or grant access to one's data, facilitated through digital technologies, to reach certain desirable goals, such as supporting disease research as well as increasing pandemic preparedness. Digital solidarity can be considered a component of digital citizenship moving from individual agency to the collective power of loosely organized digital networks that often manifest across physical borders.

References: Afina et al., 2024; Chavez, 2022; Peng et al., 2018; Roberts & Bosch, 2023; Stalder, 2013; United Nations, undated; U.S. Department of State, 2024; Walker, undated.

1.4 Digital justice

Digital justice shares many concerns with data justice but it encompasses a broader spectrum. It includes not only data but also access to and use of digital technologies. It refers to the pursuit of equity and fairness in the digital age, addressing systemic inequalities related to access to digital technologies, digital literacy and the rights and freedoms associated with digital environments. Digital justice aims to ensure that all people, regardless of their socio-economic status, ethnicity, gender or location, have the opportunity to participate fully and equally in the digital society.

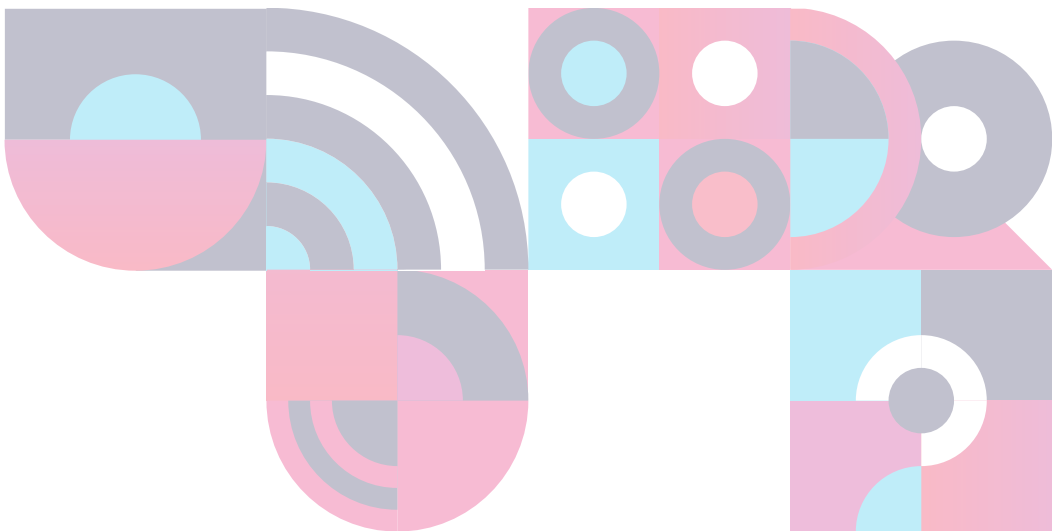
In a similar manner to climate justice, which examines equality, human rights, collective rights and historical responsibilities for climate change, digital justice is concerned with both procedural and distributive ethical dimensions. It highlights the importance of addressing individual and collective rights, ensuring that technological advancements do not exacerbate existing inequalities or create new forms of injustice.

An essential aspect of digital justice is the rectification of data-driven harms that have been inflicted upon individuals or groups. Injustices occur when the extent of harm is underappreciated or unnoticed, when there is no accountability or when there are no effective pathways for redressing harm. Digital justice seeks to address these issues by focusing on prevention, retroactive identification of harms, allocation of responsibility and identifying equitable pathways for redress. In this respect, it shares important goals with data solidarity (See **Harm mitigation**).

The concept of digital justice also involves ensuring that all voices are heard and that marginalized groups are not left behind in the digital transformation. This includes advocating for policies that promote digital literacy and accessibility, thereby enabling individuals to navigate and benefit from digital technologies.

In summary, digital justice is about creating fair and equitable digital societies. It encompasses the proactive prevention of digital harms, the identification and rectification of past injustices and the promotion of inclusive digital practices that respect and uphold individual and collective rights.

References: Adecco Group, 2023; Benjamin, 2019; Brock, 2020; Couldry & Mejias, 2019; Eubanks, 2018; Noble, 2018.



1.5 Data justice

Data justice refers to the idea that practices of data creation and data use should make our societies more just and not contribute to increased injustices. More specifically, data justice has been defined as a concept for national and supranational law-making processes that ensures fairness in the way people are made visible, represented and treated as data producers. This includes fairness in the way in which people are subject to data-based decision making. Following this rationale, a legal framework that enforces data justice must reach three central goals: First, it must provide individuals with the legal capacity to know about the collection and the use of their personal data. Second, it must make it possible for people to protect their personal data from automated commodification on global data markets and at the same time also encourage data use for the common good. Third, it must counteract technical conditions that might lead to intentional or unintentional discrimination. An example of the latter is the application of algorithms to support decision making by public authorities or private companies.

Other authors have made the case for a structural data justice perspective. Structural justice ensures that societal systems and institutions are fair, providing equal opportunities and addressing inequalities to empower all individuals, especially marginalized groups. A structural justice perspective also critically attends to the power relations that data governance is embedded in. They see data injustice as the result of structural conditions that shape wider societal relations of which data extraction and processing has become one part. This approach is especially concerned with how access to certain types of data are distributed between the Global North and South, for example.

Data solidarity and data justice are complementary. Matthias Braun and Patrik Hummel argue that data solidarity is a necessary, catalytic element for data justice. They hold that whenever injustices in the realm of data-driven practices arise and lead to individuals or groups being discriminated against or marginalized, there is a need for shared practices of solidarity to address these injustices – and for institutions that reflect and support these shared practices. In this sense, data justice depends on shared practices of hearing the voices of others (in particular, those who are marginalized) and treating their concerns as collective problems. In other words, it is necessary that people engage in shared practices of attending to and acting upon the concerns of others for sustainable real-world arrangements of data justice.

Moreover, data solidarity can play an important role identifying injustice. Often people will become aware that they have been subjected to injustice only when they consider their experience in comparison to the experiences of others. Likewise, observers might be alerted to potential injustices experienced by certain individuals or groups based on the formation of movements of solidarity. Thus, it is important that practices of solidarity within a society are recognized as also epistemically valuable in identifying and addressing injustice (and thus indirectly reinforcing the content of justice).

References: Braun & Hummel, 2022; Heeks & Renken, 2018; Hummel & Braun, 2020; Prainsack et al., 2022b; Scholz, 2008; Shults, 2024; Taylor, 2017; Young, 1990.

1.6 Public value

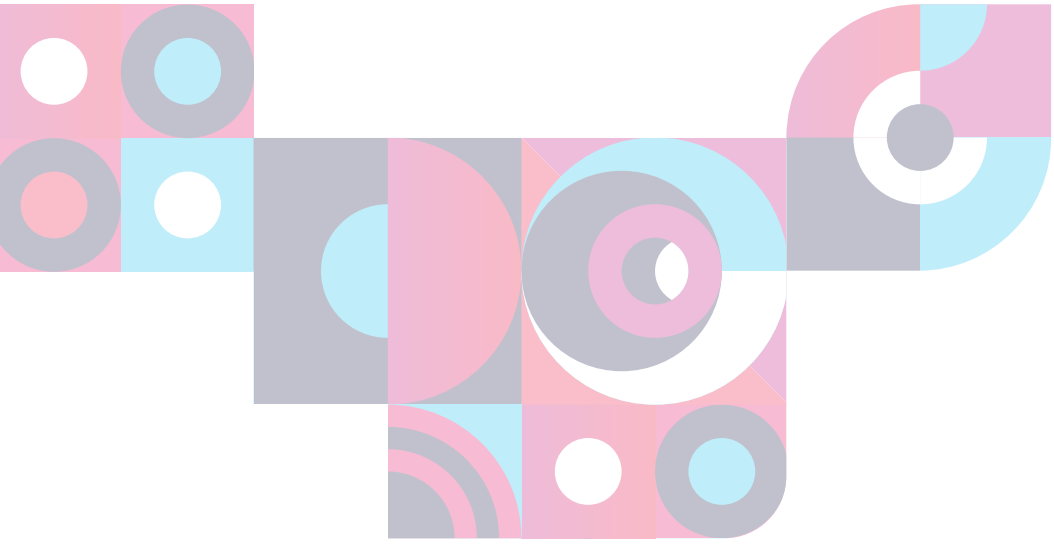
Public value is a key concept for data solidarity. It describes the value that an organization or activity contributes to society.

Originally, public value referred to the equivalent of shareholder value in public management. More broadly, public value can be understood as 'a way of measuring progress towards the achievement of broad and widely accepted societal goals', such as the transition to a sustainable global ecology, the reduction of inequality and the promotion of good health. Such a 'mission-oriented' approach to public value dovetails particularly with calls for digital health to be driven by public purpose and not by profit, based on public health principles.

Within the data solidarity approach, a data use is seen to have public value when it can be plausibly assumed that it will have clear benefits either for many people, for society as a whole or for future generations and that no person or group is likely to experience significant and undue harm. Moreover, public value will regularly be more pronounced if the benefits are likely to materialize for underserved or marginalized groups, due to the overall lower baseline and potential size of impact.

To support a structured assessment of the public value of specific instances of data use, an online tool is freely available (see **Box: PLUTO tool**). This tool could inform decision making of individuals who are asked to grant access to their data and also support decision making of organizations, public bodies and data access committees, among others.

References: Bozeman, 2007; Bryson et al., 2014; El-Sayed et al., 2023; Fukumoto & Bozeman, 2019; Kattel & Mazzucato, 2018; Kickbusch et al., 2021; Mazzucato & Ryan-Collins, 2022; Meynhardt, 2009; Moore, 1995; Nabatchi, 2012; Nabatchi, 2018; Sorbie, 2021; Turkel & Turkel, 2016.



Box: The public value assessment tool (PLUTO)

A team at the University of Vienna created an online tool to guide the structured assessment of the public value of data use. The tool can be used by anyone who wants to know about the public value that a specific instance of data use is likely to create: for example, businesses, organizations or other entities using the data, or people whose data are being used.

The online tool consists of just over 20 questions which covers four areas: Information about the data user, benefits of the data use, risks of the data use and institutional safeguards. In general, the more a specific instance of data use benefits people and communities without putting individuals or groups at risk, the higher the public value. Benefits and harms that are likely to materialize for underserved or otherwise marginalized groups are weighted more heavily than benefits and harms for privileged groups. Detailed information on the different weights assigned to answers are available online as an appendix to the online tool and openly available for anyone with internet access to see (https://pluto.univie.ac.at/).

The PLUTO tool is meant to help people and organizations think about the public value of data use in a structured manner. It does not claim to give a precise and definitive score and should not be used as the sole basis for any decision. Public value, as a concept, is not static; it evolves in response to societal changes, technological advancements and shifting values. As a result, PLUTO may need to adapt its criteria and definitions over time to remain relevant. This ongoing evolution also means that different stakeholders may interpret public value differently, leading to ongoing debates regarding the tool's effectiveness and accuracy.

References: El-Sayed & Prainsack, 2022; Prainsack & El-Sayed, 2023.

Section 2: Data governance

2.1 Data

In the most general sense, data is the plural term of measurements of values that, taken together, represent natural or social phenomena. Data can also be described as measurements or values that, when processed, yield information. The term digital data, in turn, refers to those data that are stored or processed by digital means.

We increasingly see the world through data. Ever larger parts of our bodies, behaviours and environments that used to be unmeasured and uncounted are captured in the form of (digital) data. At the same time, data are becoming a cornerstone of our societies, supporting – or even driving – innovation, efficiency and decision-making across various sectors. From healthcare and education to finance and entertainment, the collection and analysis of data enable personalized services, predictive analytics and improved outcomes. As the volume of data generated continues to grow, its importance in shaping policies, enhancing business operations and fostering technological advancements becomes ever more critical. In this context, the notion of 'big data' reflects datasets of unprecedented volume, variety, velocity (i.e. speed of collection and use) and value.

References: Castells, 2002; Kitchin, 2014; Leonelli, 2020; Prainsack, 2019b; Rieder & Simon, 2017; van Dijck, 2014.

2.2 Data governance

Data governance refers to the overall management of the availability, usability, integrity and security of the data that is collected, used and reused. It involves the establishment of policies, procedures and standards to ensure that data are managed effectively throughout their lifecycle within organizations as well as within and between countries.

Many countries and international and regional organizations are in the process of defining their approaches to data governance. One prominent example is India, which gives high priority to data sovereignty, protection of privacy, promoting digital innovation, facilitating digital inclusion and development, and ensuring greater security. Another is China which gives the state relatively easy access to personal data with the governance of digital platforms carried out in the interest of economic growth and national security. The European Union has established principles for data governance which include lawfulness, fairness and transparency, integrity and confidentiality, and accountability. The Organization for Economic Co-operation and Development (OECD) worked with their 38 member countries – which span the world, from North America and South America to Europe and Asia-Pacific – to advance the Recommendations for Data Governance in 2016. The recommendations include individual access to health information, the involvement of stakeholders in the design of health data strategies, the use of consent or appropriate alternatives, the importance of security and privacy and the optimization of data and technology in the public interest.

The World Health Organization (WHO) has recognized the need for common standards and coordinated approaches to realize the potential of digital transformations for health. In its Global Strategy on Digital Health, the WHO identifies interoperability and health data governance as two of the most pressing areas for future international agreements. Hundreds of organizations recently called on the WHO and its member states to start working on a global framework for health data governance that will allow the value of data to be harnessed for the public good whilst protecting individual rights as well as group rights, such as those of marginalized groups. Health data governance should have a prominent place in all public health policies whether global or national, regional or local. The Pandemic Treaty that is currently being negotiated is a case in point at the global level, the EU's General Data Protection Regulation (GDPR) and the Artificial Intelligence Act are examples at the European level. The latter will apply to Artificial Intelligence applications across all sectors in EU countries. The ASEAN countries with Japan are advocating for an approach of "Data Free Flow with Trust", which promotes a trusted, interoperable global system to facilitate cross-border data flows. The African Union is engaged in developing legal and regulatory interoperability on data among the legally and culturally diverse set of 55 Member States and addressing the scarcity of data infrastructure. *The Lancet* and *Financial Times* Commission proposed a value-driven governance model based on the core values of equity, data solidarity, digital stewardship, trust, accountability and public participation. While the above initiatives and policies refer to many of these core values, they do not yet include an explicit reference to data solidarity. Data solidarity is a specific approach towards data governance that places emphasis not only on individual control but also on collective forms of oversight and ownership of digital data and infrastructures.

References: D4DHub, undated; Okinawa, 2024; He, 2023; Kickbusch et al., 2021; OECD, 2016; Struett et al., undated; Transform Health, 2022; World Health Organization, 2021.

2.3 Data stewardship

In general, stewardship refers to the responsible management of resources or assets entrusted to one's care and involves making decisions that prioritize the long-term well-being and interests of stakeholders or beneficiaries. The goal of stewardship is to promote long-term conservation and sustainability of ecosystems while meeting the needs of today in an effective and efficient manner.

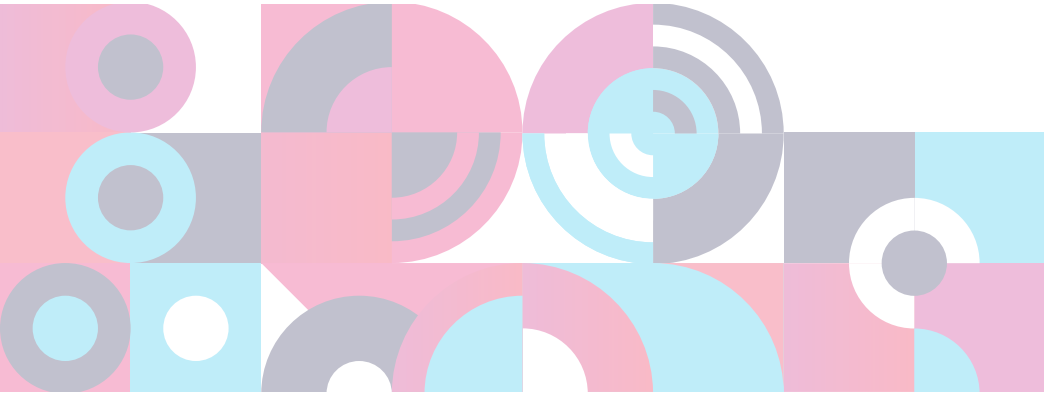
In the domain of health, data stewards should be accountable to champion sharing of and access to health data while ensuring data is fit-for-purpose and used appropriately according to data governance rules. They should also co-design policies and standards to simplify scale and spread of innovation, productivity and system effectiveness. Key responsibilities of data stewards include:

- Ensuring compliance of policies, standards and procedures for data governance and management;
- Defining and implementing measures and processes to protect data from unauthorized access, misuse or breaches;
- Ensuring data quality by implementing quality assurance processes;
- Ensuring that data is properly mapped, transformed and harmonized to support business functions;
- Overseeing the entire data value chain including measurement of the health data ecosystem and to take actions for continuous improvement; and
- Serve on the data governance bodies, where appropriate.

Data stewards oversee the practical application of policies and standards governing data originating from multiple different data generating entities across the data value chain, from data identification, collection, storage, sharing and use. Stewards ensure that fit-for-purpose data is available in a seamless way to authorized data users to derive actionable insights.

This is distinct from data custodians or trustees, who are responsible for the storage, management and protection of data assets within their own institutions and organizations, while also ensuring that data is shared according to relevant regulations and legislation. Both roles are essential for ensuring that data assets are effectively managed, protected and used for the public good.

References: Plotkin, 2020; Public Health Agency of Canada, 2022.



2.4 Data security and privacy

Data security and data privacy are closely related concepts that complement data solidarity. They focus on protecting information in the digital realm, but they address distinct aspects of handling and safeguarding data.

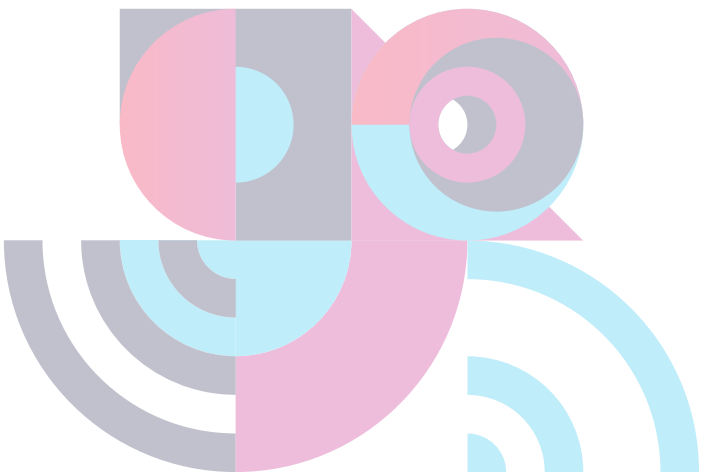
Data security involves the implementation of measures and protocols to safeguard digital information from unauthorized access, disclosure, alteration or destruction. It encompasses a wide range of practices and technologies designed to secure data throughout its lifecycle. This includes encryption, access controls, firewalls, antivirus software and other security measures aimed at preventing data breaches and ensuring the integrity and confidentiality of information. Data security is a critical aspect for businesses, organizations and individuals to protect sensitive data and maintain the trust of their stakeholders.

Data privacy specifically focuses on controls for the use of personal information – which is typically understood as data that relates to an identified or identifiable individual. It revolves around people's rights to have a say in how and by whom data about them is used and how organizations collect, process and handle personal data. Privacy measures include a range of instruments, such as obtaining informed consent before collecting data and complying with privacy regulations and policies. The goal of data privacy is to give people confidence that their personal information is handled responsibly and ethically, preventing unauthorized access or usage that could lead to privacy breaches or misuse of sensitive data. Both data security and data privacy are integral components of responsible data management.

The dominant way to understand data privacy in liberal economies is through an individualistic lens, meaning that data privacy is predominantly defined as an individual right. Increasingly, this individualistic framework is challenged by empirical and normative accounts of how privacy is a personal and a collective interest at the same time and requires protection via individual and collective rights.

Data solidarity acknowledges that data security and privacy are individual needs and rights and that data are at the same time collective goods to support community needs and rights. The frequent or even systematic infringements of individual privacy rights changes society and the same is true the other way round: People can only meaningfully exercise their individual rights within a society in which mutual respect and solidarity prevail. For example, even if individual people have an individual right of freedom of expression, this cannot be exercised if there are no sanctions for online harassment.

References: Coventry & Branley, 2018; Ebeling, 2016; Harman et al., 2012; Koontz, 2017; Mittelstadt, 2017.



2.5 Digital sovereignty

Digital sovereignty refers to the regulatory and control measures a state exercises over the technology and digital services within its jurisdiction. This includes control over where data reside, how data flows are organized and who has access to and control over it.

While data sovereignty (See **Data sovereignty**) specifically focuses on the policies and laws governing data storage and transfer, digital sovereignty extends to broader technological aspects, including the infrastructure, platforms and services that support data use and storage. Digital sovereignty thus includes control over data but also the control over hardware, software and network resources that enable digital interactions.

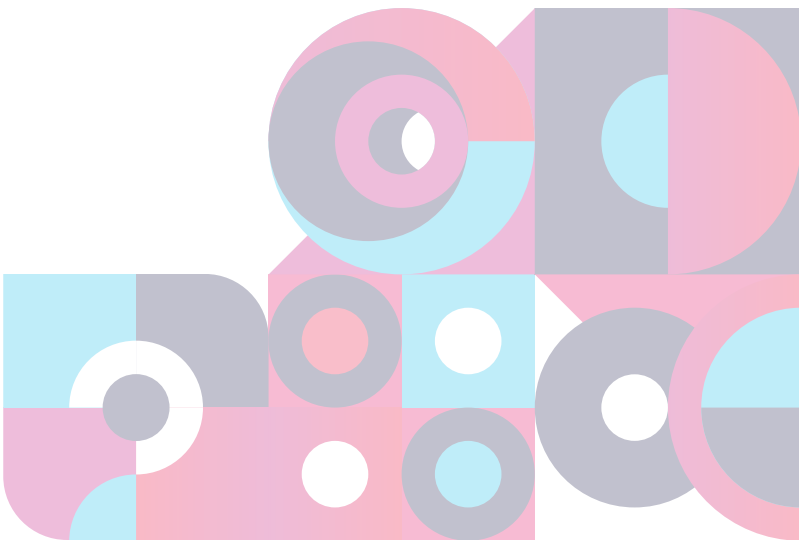
Digital sovereignty is becoming increasingly critical in today's interconnected world. States and regions are seeking to (re)claim control over their digital environments to safeguard against external dependencies and vulnerabilities. The European Union (EU), for example, has been advocating for greater digital sovereignty to reduce reliance on non-EU technologies and ensure compliance with EU data protection standards.

A broad range of issues and concerns are subsumed under the label of digital sovereignty. These include questions about the control data subjects need over the handling of their data and how such control can be implemented. This control could be at the level of individuals or collectives (e.g., families, communities). Additionally, there are concerns about how states or international organizations can manage and control both the material and immaterial aspects of digital infrastructures.

The importance of digital sovereignty is underscored by the increasing geopolitical tensions around technology. Nations are wary of foreign surveillance and data breaches, which can compromise national security and economic interests. By asserting digital sovereignty, states aim to protect their citizens' data privacy and ensure that critical digital infrastructure is resilient against external threats.

Digital sovereignty is often seen to include laws and policies that mandate local data storage and processing to keep sensitive information within national borders. For example, some countries have implemented data localization laws requiring companies to store and process data on servers physically located within the country. This not only enhances data security but also ensures that data are subject to local laws and regulations.

References: Broeders, et al., 2023; Floridi, 2020; Sciences Po, undated; Tietoevry, 2023; Gordon, 2024.



2.6 Data sovereignty

Data Sovereignty relates to the rules and reference architectures that can help safeguard some of the fundamental principles of digital sovereignty, such as, where the data are stored, who controls the data, how they can be stored and processed in a secure way and how they can be made interoperable and portable. As such, the holder of data sovereignty can be individuals, organizations, companies, governments or entire societies and countries. This can lead to conflicting claims of data sovereignty at these levels.

When it refers to individuals, data sovereignty is closely linked to the notion of digital self-determination, which denotes a person's individual right and ability to exercise autonomy over their digital presence, data and online activities. Insofar as data sovereignty pertains to collective control over data, it can refer to claims of communities (e.g. Indigenous people and communities) or nations to exercise control over what phenomena will be datafied, how the data will be used and who will benefit (see also **Indigenous data sovereignty**).

Based on their different approaches to key issues of control over data, it has been suggested that three major jurisdictions in the world – the US, China and the EU – represent three different data sovereignty regimes, namely corporate sovereignty, state sovereignty and individual sovereignty respectively. Data sovereignty is also prominently debated in the context of the design of IT architecture and/or laws governing data processing.

In virtually all accounts, digital sovereignty aims at increasing the control and power of collective actors over data. The type of power in question – unlike in some classical concepts of sovereignty – is not brute force, but it is the exercise of power that respects values such as inclusiveness, deliberation and the fundamental rights of the persons concerned.

To the extent that data sovereignty seeks to increase collective control and oversight over data, it shares a key concern with data solidarity. In contrast to sovereignty, however, data solidarity is not primarily focused on the state or the community, but it seeks to support a more equitable sharing of benefits and risks via policy instruments at all levels: local, communal, national and global.

References: Gao, 2021; Hummel et al., 2021; Sciences Po, undated; Verhulst, 2023; Woods, 2018.

2.7 Indigenous data sovereignty

Indigenous data sovereignty is a concept that emphasizes the right of Indigenous people and communities to control the data collected from and about their communities. It asserts that data related to Indigenous groups should be managed and governed according to the norms, values and interests of the communities from which the data originates. This idea challenges dominant Western data governance models that overlook Indigenous rights and fail to consider the unique cultural, contextual and historical circumstances of Indigenous people and communities, especially also in terms of the harms suffered by colonial powers and legacies (as well as the rights and interests of other marginalized groups). Of specific relevance in the context of Indigenous data sovereignty are the so-called CARE Principles, which were introduced to complement the FAIR principles (Findability, Accessibility, Interoperability and Reusability). While the FAIR principles focus on the technical aspects of data, the CARE principles put a spotlight on the people and purpose behind data collection and use:

- Collective Benefit: The design and function of data ecosystems should enable Indigenous communities to derive benefits from the data collected from them. This involves the data being used in ways that support Indigenous values and self-determination.
- Authority to Control: Indigenous communities must have authority over the data collection processes that concern them, including the right to control how this data is gathered, accessed and used.
- Responsibility: Those who handle the data have a duty to ensure that it is used in a manner that respects Indigenous rights and well-being and that adequate measures are taken to minimize harm and maximize benefit to Indigenous communities.
- Ethics: Data management practices must be guided by ethical frameworks that are informed by Indigenous worldviews, which often include values such as reciprocity, respect and care for the community.

Indigenous data sovereignty is also closely linked with efforts to rectify historical injustices and empower Indigenous people and communities by ensuring they have control over their own data. This includes data used in governmental policies, academic research, healthcare and more. Effective implementation of Indigenous data sovereignty can lead to better tailored services and policies, enhanced privacy protections and greater respect for Indigenous cultural heritage. As such, Indigenous data sovereignty is aligned with the goal of data solidarity to achieve a more equitable sharing of risks and benefits from digital practices and – besides respecting individual autonomy – also strengthening collective instruments of control and oversight over data and digital infrastructures. Data solidarity and Indigenous Data Sovereignty are aligned also in the sense that they both go beyond dichotomies that are used in Western data governance frameworks, such as the dichotomy between personal versus non-personal data. Both data solidarity and Indigenous data sovereignty recognizes that people – as individuals and as members of collectives – can have important stakes and interests in data that are not 'personal' in the technical sense (i.e. they do not refer to an identified or identifiable individual and are thus not within the remit of many data protection frameworks around the world).

References: Benjamin, 2019; Carroll et al., 2020; First Nations Centre, 2007; First Nations Information Governance Centre, 2014; Kukutai & Taylor, 2016; McDonald, 2022; Saxinger & First Nation of Na-Cho Nyak Dun, 2018; UN General Assembly, 2007; Wilkinson et al., 2016.

2.8 Data localization

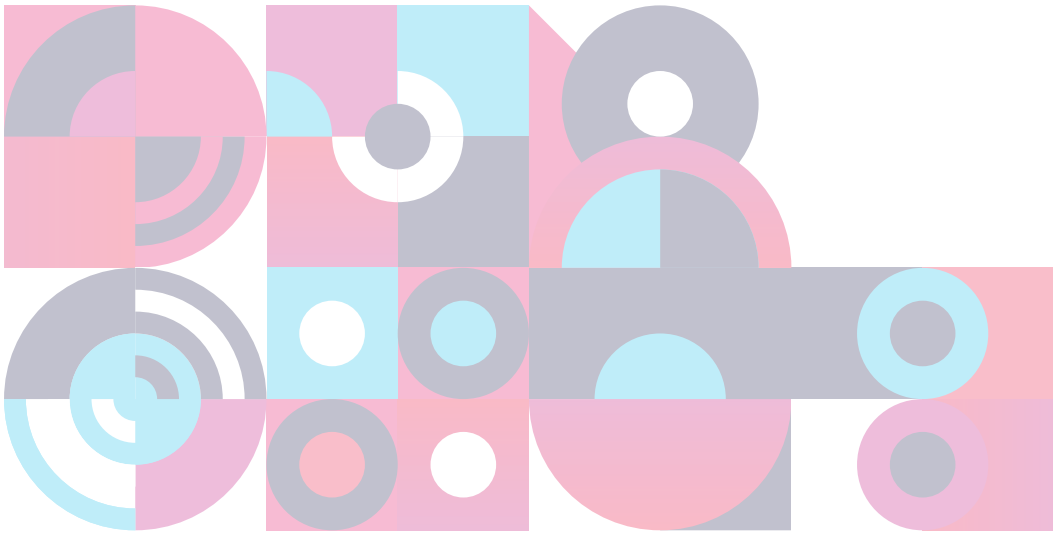
Data localization refers to the legal requirement imposed by governments for data generated within their borders to be stored and processed domestically. These regulations aim to ensure data sovereignty, where data is subject to the laws and governance of the country in which it was created. This is particularly important for data related to sensitive industries such as finance, healthcare or national security, where concerns over privacy and data security are paramount. Countries enforce data localization to safeguard against unauthorized foreign access, protect personal privacy and enable local law enforcement to access data for investigation and regulation.

Proponents of data localization argue that keeping data within national borders enhances data security and privacy by allowing countries to enforce their own regulations directly. It also stimulates local economies by creating job opportunities in data centres, cloud computing and IT infrastructure development. Moreover, it can help emerging economies foster local tech industries by ensuring that data processing resources remain within the country.

Critics of data localization point out several drawbacks. They argue that it can increase operational costs for multinational companies that need to comply with multiple regulatory frameworks. This fragmentation can also hinder the flow of data across borders, limiting global innovation and collaboration. Additionally, data localization requirements may impede access to the most advanced data processing tools, which are often located in other regions, thus potentially restricting technological advancement within the country.

Within data solidarity, data localization is a welcome development when it helps to create greater equity between countries and world regions – that is, when it is used by digitally disadvantaged nations to ensure more benefits for them. When it is used by rich nations to entrench their advantage, data solidarity considers data localization harmful.

References: Chander, 2020; Chander & Lê, 2014; Liu, 2022; Taylor, 2020.



2.9 Harm mitigation

Harm mitigation is one of the three pillars of data solidarity (see **Table 2: The three pillars of data solidarity**). Whenever data is used – even when there is great benefit for people and communities – there is a risk that individuals or groups are harmed. For example, when sensitive personal information is exposed, this could lead to identity theft and financial losses. Unauthorized data sharing can also result in discrimination, as people might be unfairly treated based on their data profiles, affecting their access to jobs, insurance and services. Lastly, extensive data collection and surveillance can erode personal freedoms, limiting free speech and other freedoms due to fear of being monitored.

While we need to try to ensure that risks are reduced as much as possible, it is also important to openly acknowledge that harms might still occur, that some harms are not yet fully known or understood, and that people who have experienced harm must receive adequate support and compensation.

Generally speaking, harms may occur from either data use or non-use. Harms from data use may result in breaches of privacy, emotional damage or breaches of cultural rights. Harms from data non-use include physical harms from not being aware of prior medical history, lack of responsiveness to serious medical conditions, failure to benefit from science or to identify inequities or increasing health system costs through unnecessary duplication. The consideration of risks related to harms ideally considers the full range of data-related harms along with their likelihoods and impacts.

Today, people and communities who are disadvantaged because of data use are often left without such support, for various reasons. Harm can occur without any laws being broken, such as when people are charged higher rates for the same services as others or they are denied services, due to predictive analytics. People can also experience harm from social media or digital platforms, without the content being illegal. In other instances, harm occurs without the harmed party being able to pinpoint who exactly caused the harm. The more data is shared and linked and the less transparent these processes are, the more difficult it becomes for people to identify what or who is responsible for the harm they have experienced. Finally, some people do not have access to legal remedies because they lack the social and economic resources to use them.

From a data solidarity perspective, it is essential that people who are harmed by data use have access to support, independent of where in the world they are. One way to do so is the establishment of Harm Mitigation Bodies. Harm Mitigation Bodies are independent organizations who review appeals from people who claim to have been harmed by data use. The law could mandate that every organization above a particular size needs to be affiliated with a Harm Mitigation Body. Large organizations, such as multinational companies, could set up their own Harm Mitigation Bodies, while smaller enterprises could submit themselves to the purview of a Harm Mitigation Body established at regional, national, supranational or even international level.

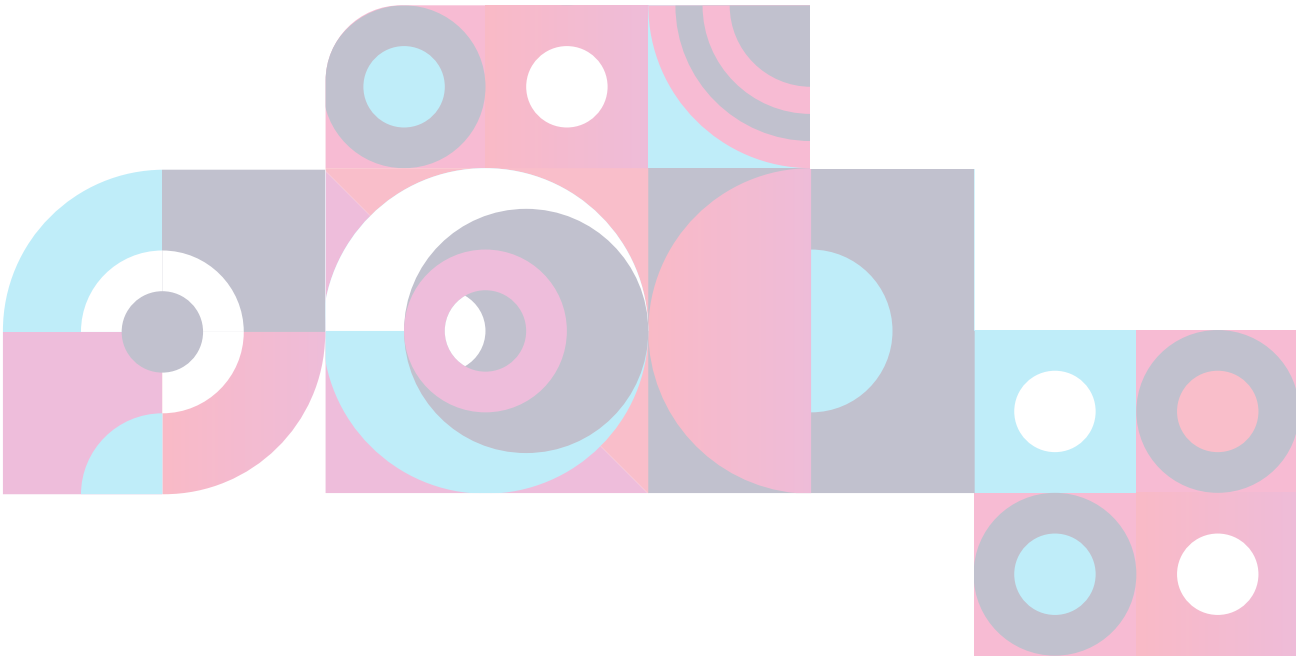
Harm Mitigation Bodies ought to fulfil three primary functions: First, they would be a *de facto* monitoring body due to the harms that people report as occurring to them. Data controllers (or custodians or stewards) and public agencies may then access that information to improve the operation of systems of data governance. Second, in specific cases, where people have suffered financial harm and been unable to receive support elsewhere, they should also be

able to provide financial support. Unlike in formal legal mechanisms, there is no requirement to prove wrongdoing or direct legal causation of the harms suffered. Third, Harm Mitigation Bodies would monitor where data access in the public interest is not being provided in a timely manner and with the required quality. In such cases, the Harm Mitigation Body would quantify the potential impact on communities from data-non use and be able to provide appropriate remediations.

Next to Harm Mitigation Bodies, there are also other measures for harm mitigation. They include data breach response plans that lay out implementation plans for containment, investigation and remediation to address data breaches. Post-incident audits and reviews can help to understand the causes of the harm in specific cases and to improve data governance as a result. Data rectification and erasure provides mechanisms for affected individuals to correct erroneous data and get their personal data deleted to prevent further misuse.

Whatever measures are chosen, harm mitigation needs to be set up as a separate, additional measure next to risk minimization and it needs to be easy to access.

References: Taylor et al., 2017; McMahon et al., 2020; Prainsack et al., 2022a;b; Affleck et al., 2024.



Section 3: Sharing data

3.1 Digital and data commons

In the context of data solidarity, commons are one way to increase collective oversight and ownership of data and digital infrastructures. Commons are social institutions for governing common-pool resources – that is, resources that are accessible to multiple people (they are 'common') and for which it is difficult to exclude anyone from using (they are 'non-excludable'). Commons are governed by the principles of values of fairness, equality, justice and sustainability.

Commons have a long tradition in law and history in fields ranging from agricultural land use to forests to educational resources. There have been debates about the extent to which commons regimes can be applied to intangible resources such as digital data. Some authors use the notion of commons in an even wider sense, including under the label of digital commons (data, information, culture and knowledge) that have been created and or maintained online and that are for public use. Such a broad understanding of commons tends to equate commons regimes, where people jointly own the resource and decide over its use, with open access regimes, where anyone can use the resource as they please and nobody can be excluded.

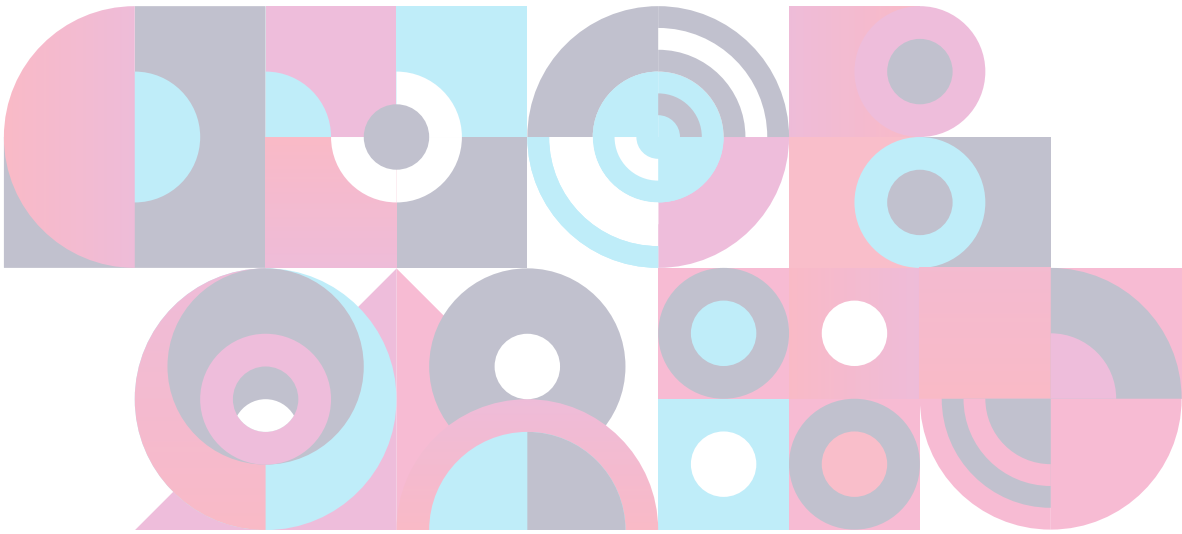
The digital commons movement was particularly strong in the aftermath of the banking crisis of 2008, but also when access to scientific literature became increasingly expensive, around the year 2010. All over the world, new volunteer organizations, novel digital formats of participation, non-commercial

infrastructures to share resources and new social spaces emerged. Their intention was to create an alternative to the hegemonic power structures and markets in a networked society. The success of these initiatives has been compromised by the commercialization of many open knowledge resources and also because actors in research-rich contexts could afford 'opening up' their data and resources more easily and also make better use of data and resources that others had opened up. These issues illustrate once more the limitations of 'commons' concepts that are, in fact, open access regimes, which tend to unfold a Matthew Effect: If everything is up to be taken, then those who already have more power and resources can take more of the open resource.

Data solidarity supports commons as a way for people – at local, regional, national or transnational levels – to jointly own and govern resources. It does not support 'commons' that are open access regimes, meaning that there is no collective ownership of the resource and anyone can take it as they will.

Digital and data commons that are compatible with the spirit of data solidarity can be implemented by establishing platforms where data are governed collectively by everyone who contributes to data, ensuring transparency and equitable use. An emerging trend in this context is the establishment of 'virtualized data commons' across trusted networks of collaborators. In such cases, the data are not copied or consolidated into a singular data holding. Rather, the data remain at source and are available across the network through an agreed collective query mechanism. Such virtualized data trusts support federated learning. These networks adhere to common requirements across the network for legal, governance and data interoperability. In addition, there is a requirement for policy controls, training and stakeholder engagement to learn and sustain trust. Such virtualized data trusts will be increasingly common with trans-national partnerships such as in the European Health Data Space, for example.

References: Bollier & Helfrich, 2019; De Angelis, 2017; Dulong & Stalder, 2020; Fuster Morell, 2011; Micheli et al., 2023; Paprica et al., 2023; Prainsack, 2019a; Terzis et al., 2023.



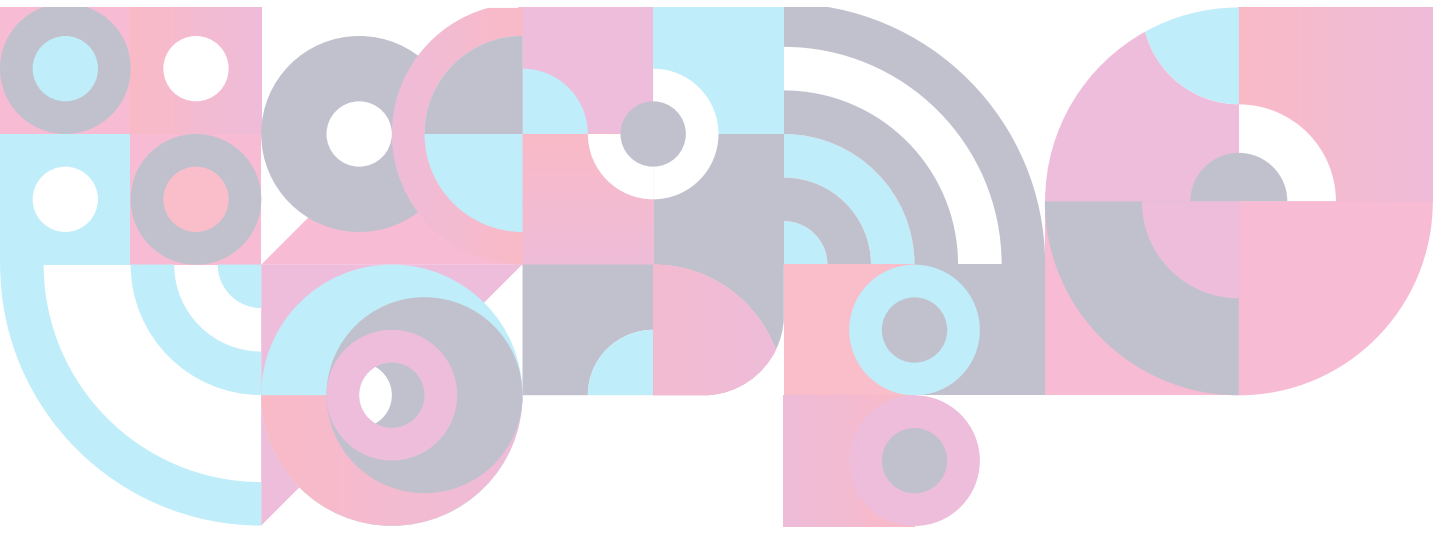
3.2 Data cooperatives

In general, data cooperatives are organizations where people pool their data for mutual benefit. This term is often used synonymously with data commons. Both represent collective forms of owning and governing data. When a difference between data commons and data cooperatives is made, then it is to emphasize the following features that characterize cooperatives: voluntary membership, democratic control, economic participation, autonomy from other commercial or public entities and a public value orientation.

By joining forces, members can negotiate better terms with data collectors and access services that leverage their collective data while maintaining greater control over its use. While some data cooperatives aim primarily at creating public value, others (also) serve the purpose of helping people to monetize their data.

Like data commons, data cooperatives can help to realize data solidarity if the public value orientation is not overruled by particularistic or for profit-interests.

References: Blasimme et al., 2018; Hardjono & Pentland, 2020; Micheli et al., 2023; Zhu & Marjanovic, 2022.



3.3 Data trusts

Data trusts are legal structures designed to manage and oversee the use of data on behalf of a group of beneficiaries, such as individuals, communities or society at large. Data trusts are governed by trustees who make decisions about its use and management based on the interests of the beneficiaries. The trustees have a fiduciary duty to act in the best interests of the beneficiaries and ensure that the data is used responsibly and ethically.

Data trusts can be established to address various concerns related to data governance, including privacy protection, data access and ensuring that data is used for societal benefit. They provide a mechanism for individuals and communities to retain some control over their data while still allowing for its use in previously agreed ways.

So-called data vaults can serve as the technical architecture that underpins data trusts, enabling organizations to store data securely while enabling trusted parties to access necessary information, maintaining transparency and accountability. They are a type of warehouse modelling methodology designed to handle large-scale data environments, especially those that need to adapt quickly to new requirements or changes. They focus on scalability, flexibility and consistent integration of data from multiple sources.

The main difference between data commons and cooperatives on the one hand and data trusts on the other, lies in their governance and ownership structures. In the case of data commons and data cooperatives, data are – at least morally or even legally – considered joint property of all members. Data trusts, in contrast, can serve as 'data vaults' for individual people to deposit their data for an entrusted entity (the trustees) to be governed on their behalf. This means that while data cooperatives and data commons can be considered a way of owning and governing data that go against data individualism and the prioritization of financial profit, some data trusts serve exactly these latter purposes. They treat data not as common property but as individual assets. As such, data trusts are not among the policy instruments promoted by data solidarity, unless they enforce the same solidaristic principles that data commons do.

An example for the latter from the domain or research are so-called trusted research environments (TREs), which serve as secure platforms within data trusts, enabling researchers to access and analyse sensitive data while ensuring privacy and compliance with ethical standards. These environments implement stringent access controls, data anonymization techniques and audit mechanisms to protect individuals' data from misuse. By fostering transparency and accountability, TREs build trust among data subjects and stakeholders, facilitating the responsible use of data for scientific and public benefit.

References: Hardinges et al., 2019; Delacroix & Lawrence, 2019; Element AI & Nesta, 2019; Hill, 2023; Linstedt & Olschimke, 2015; McDonald, 2019; Micheli et al., 2023; Paprica et al., 2023.

3.4 Data sharing

A wide range of diverse activities – from research institutions making interpreted results of genomic research available to participants, to customers allowing online companies to use information on how they use their services – all fall under data sharing. It thus includes the copying of data and access to the source data without creating a copy. Another disadvantage of this inclusive definition is that it makes it impossible to distinguish between instances of data sharing that create public value and benefit people and societies and those that serve merely the maximization of commercial profits. For data solidarity, in contrast, this distinction is crucial.

Data solidarity is sometimes conflated with data sharing, which is incorrect.

Data sharing refers to the making data available to third parties, regardless of what purpose the data is used for and to whose benefit. Data solidarity, in contrast, aims to distribute the harms and benefits emerging from digital practices more equitably. Thus, while some instances of data sharing can be an expression or a result of data solidarity, others (such as data altruism) are not. At times, data solidarity can express itself in refraining from making data available to specific entities. It can also express itself in refraining from recording some aspects of people's bodies and lives in data in the first place.

References: Jussen et al., 2023; Longo & Drazen, 2016; Prainsack et al., 2022b.

3.5 Data altruism

Data altruism is central to the European Union's Data Governance Act, which was adopted by the European Union on May 30, 2022. This Regulation aims to create a framework for data governance within the EU, focusing on the safe reuse of public-sector data and establishing a level playing field in the data economy by promoting data sharing and reducing barriers to data accessibility. In this Regulation, data altruism is defined as 'data voluntarily made available by individuals or companies for the common good' (Chapter IV). This chapter details how individual people and companies can voluntarily make data available for the common good and it establishes mechanisms for organizations engaging in such activities to register as 'Data Altruism Organisations recognized in the EU'. To do so, an organization needs to operate on a not-for-profit basis and be independent from any entity that operates on a for-profit basis. It also needs to be able to ensure that its activities related to data altruism take place through a legally independent structure, separate from other activities it has undertaken.

The European Commission's perspective on 'altruism' seems to be underpinned by specific assumptions about how people can be motivated to make their data available 'for free'. It remains to be seen whether the additional gain of 'certified trustworthiness' of registered data altruism organizations and consent form templates will create sufficient incentives for data sharing.

Apart from the specific context of EU regulation, in the wider legal, policy and ethical literature, there is no common understanding of what data altruism means. Some authors use it as a generic term to refer to a set of values and practices that is closely linked to the concepts of data donation and data sharing. From a data solidarity perspective, the notion of altruism is problematic in several respects: First, because it assumes that people should give up stakes in the data that they share, which – particularly in connection with health data – does not make sense. Few people would seriously argue that patients who share their health data should no longer have a right to control these data. The notion of solidarity, which emphasizes an ongoing relationship between data subjects and data users, seems more fitting in this respect. Another problem with the data altruism framework is that entire institutions can receive the stamp of approval, assuming that they are working in the general interest. Such a broad-brush approach misses the necessary nuances that come with different kinds of data use, irrespective of who the data user is. For this reason, data solidarity binds regulatory consequences to different types of data use, following an assessment of both risks and potential benefits, considering also for what groups these risks and benefits are most likely to materialize.

References: Kraut, 2020; Prainsack et al., 2022b; European Commission, 2020; European Parliament & Council of the European Union, 2022; Raj et al., 2020; TEHDAS, 2021.

3.6 Data donation

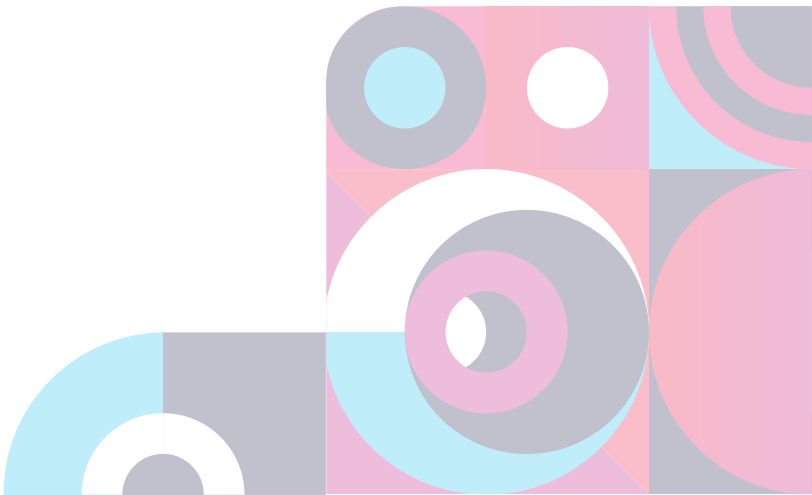
Legal definitions of the concept of donation, leading back to ancient Roman law, focus on the owner of a thing transferring it to another person or entity without expecting anything in return. The latter aspect – that something is given without demanding or even expecting anything in return – tells us two things about donations. First, that no economic profit motive is attached to a transfer. Second, donations are not reciprocal in a direct and linear manner – even if they, like other gifts, are embedded in networks of mutual moral and social obligations. Instead, donations are indirectly reciprocal. In addition, donations are rivalrous and consumable: If a person donates money to a hospital, then they cannot give the same money to disaster relief. If someone donates a kidney to one person, they cannot donate the same kidney to somebody else. Traditionally, donations have entailed that there is a consumable thing that is transferred from one entity to another.

The question is whether the same can be said for digital data, including health data. Given that digital data can be in more than one place at the same time and that they often leave traces even when they are 'deleted', the question arises where a donation begins and ends. Are all copies of a dataset being donated or can a copy be maintained by the original data subject? The concept of data donation is especially confusing when it is used in a context where people give something to others that they continue to have access to – such as when a person allows data from their mood diary to be used for research.

Because of these ambiguities, the data solidarity approach avoids the concept of donation in the context of data. Insofar as other authors or policy makers use the term data donation, whether a specific instance of data donation is also solidaristic depends on the motivation of the person making the data available and on the purposes and contexts that the data is used for. Because donating something typically means that the person donating no longer has any rights or stakes in the donated thing, the use of the term donation is particularly problematic in the context of health data. It would not be ethical and in some cases also illegal, to demand that people making their health data available for use by others no longer have access to them.

The concept of data donation can, however, be very helpful in relation to considering what will happen with a person's data after their death. In most legislations, data about and owned by deceased individuals are largely unregulated. Data donation could be a way for people to decide on the fate of their data as long as they are still alive.

References: Carrier, 1991; Krutzinna & Floridi, 2019; Prainsack, 2019a; Prainsack et al., 2022b.



3.7 Open data / Open science

Open data describes any data that can be freely accessed, (re)used and shared by anyone without restrictions. Open data has been developing as a movement for decades and has gradually influenced public policies at the national and international levels. The primary focus is facilitating the disclosure of publicly held data in open repositories in a machine-readable format. To this end, countries develop Open data portals and Application Programming Interfaces that enable businesses and researchers to access and process administrative data efficiently. Open data is considered a vehicle for developing science, technology, innovation and the economy. In this context, it has also been recognized by the United Nations as an initiative that can significantly contribute to achieving the Sustainable Development Goals.

Open data remains closely related with Open science. The latter combines various concepts, movements and practices aiming to make scientific knowledge openly available and accessible to everyone. Openness refers primarily to the absence of cost barriers, but it also extends to informal barriers related to the discoverability of data, digital skills and available resources. What is to be made openly available are mainly the means and outputs of knowledge production, particularly academic publications and scientific data. More recent policy instruments also apply to algorithms, source codes, software and workflows. The notion of Open Science is also closely connected to the open source movement. Open source refers to any programme whose source code is made available for use or modification as users or other developers see fit. Unlike proprietary software, open source software is computer software that is developed as an open public collaboration and made freely available to the public.

Especially insofar as the facilitation of data use that creates significant public value is concerned, the open data, open science and open source movements share important goals with data solidarity. At the same time, as critical scholarship has emphasized, openness is not an end itself. Especially in cases where openness is focused on formal equality in access, this often leads to more economically powerful actors being better able to make use of the openly available resources than others. This increases, rather than decreases, inequalities. If Open science is not put in the service of substantive goals such as increasing equity and justice, it could have merely cosmetic effects and even contribute to the exacerbation of the gap between researchers and publics in resource-rich and resource-poor contexts.

References: Bezuidenhout et al., 2017; Kitchin, 2014; Levin et al., 2016; Nerlich et al., 2018; Szoszkiewicz, 2021; World Health Organization, 2020.

3.8 European Health Data Space (EHDS)

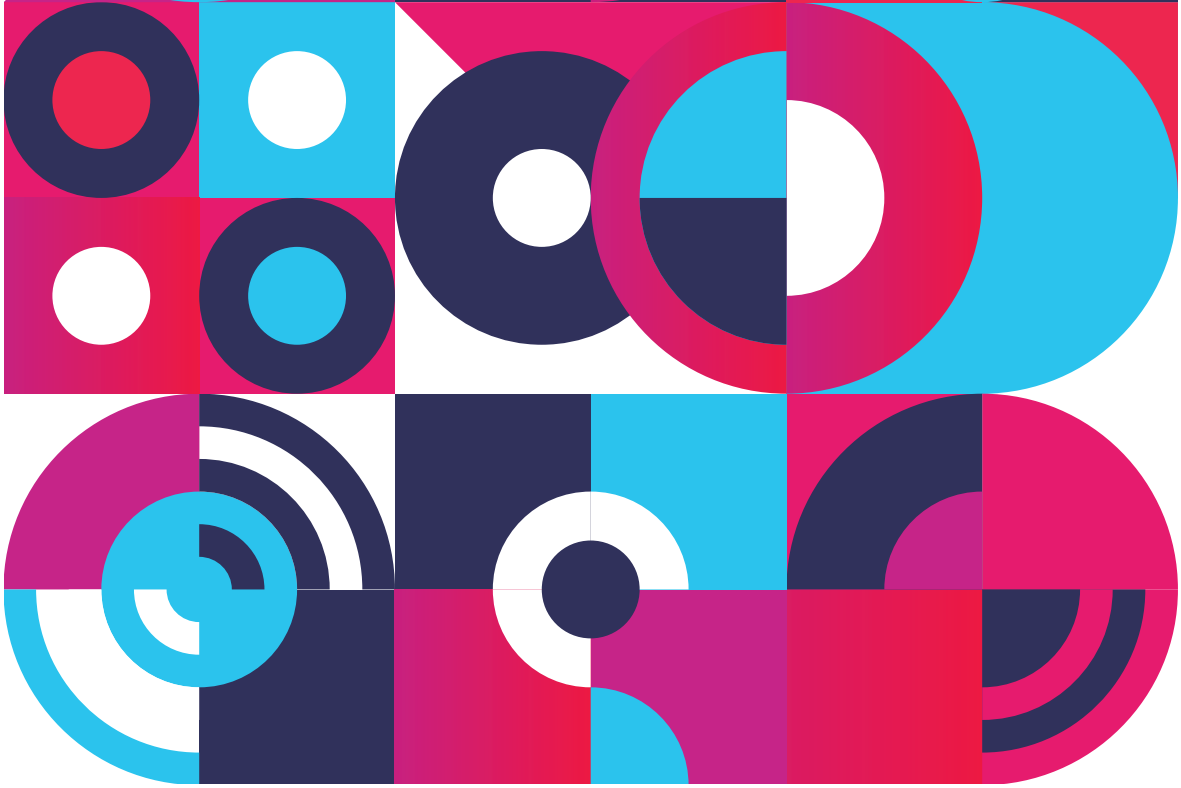
The European Health Data Space (EHDS) is an initiative by the European Union aimed at improving the accessibility, interoperability and sharing of health data across Member States. With a first draft published in May 2022, it has been discussed in various EU institutions. If adopted, it could come into effect as early as 2025.

The EHDS seeks to harness the potential of digital health technologies to enhance healthcare delivery, research and innovation while safeguarding data protection and privacy. It aims to create a common framework and infrastructure for securely exchanging health data, including electronic health records, genomic data and real-world data from healthcare systems, research institutions and other sources. By facilitating the seamless exchange of health data, the EHDS aims to support more effective healthcare planning, personalized medicine and health research initiatives, ultimately contributing to better health outcomes for European citizens. During the French Presidency of the Council of the European Union in 2022, ethical principles for the use of digital health were proposed: base digital health on humanistic values; enable individuals to manage their digital health and data; make digital health inclusive; and implement eco-responsible digital health.

Critics have raised concerns about the potential risks to individual privacy and the security of health data, particularly regarding the centralized storage and sharing of sensitive information. There are also challenges related to ensuring the interoperability of diverse health data systems across Member States, as different countries may have varying standards and protocols for data exchange. Additionally, questions have been raised about the governance structure of the EHDS and the involvement of stakeholders, including patients and healthcare providers, in decision-making processes. It has been argued that greater transparency and accountability are needed to address these concerns and ensure that the EHDS effectively balances the benefits of data sharing with the protection of individuals' rights and interests. Also the notion of data altruism within the EHDS has been critiqued as problematic (see **Data altruism**).

From a data solidarity perspective, there are various problems with the EHDS proposal, including its strong use of the term altruism. In contrast to solidarity, which is a relational concept that emphasizes the mutual needs and responsibilities between different actors, altruism could be seen to suggest that those sharing data do so for purely selfless reasons and are ready to give up their stakes in the data. Moreover, there are concerns that the provisions of the EHDS could benefit large corporations to access data even more easily and thus increase the asymmetry in power and influence between larger and smaller entities in data economies.

References: European Commission, 2022; Marelli et al., 2023; Shabani, 2022.



Section 4: Ethics and power

4.1 Digital and data ethics

Digital and data ethics (including ethical AI) are important complements to data solidarity. Digital and data ethics focuses on the moral obligations that all societal actors have (or should have) when collecting, generating, analysing and disseminating both structured and unstructured data, human-provided data as well as the leverage of existing databases, including decisions driven by automated/artificial intelligence (AI) in relation to data in general and personal data in particular. It relates to general principles on which our societies are built and is highly relevant to building trust and ensuring fairness.

The development of digital health raises legitimate and specific questions and concerns about data uses, security and sovereignty issues. In health, it is particularly important to build a trustworthy framework surrounding data uses in view of the rapid development of datafication in health. It is essential to frame the development of digital health with humanistic and citizen values, to implement them in a concrete way and to communicate the progress made to citizens in a transparent way.

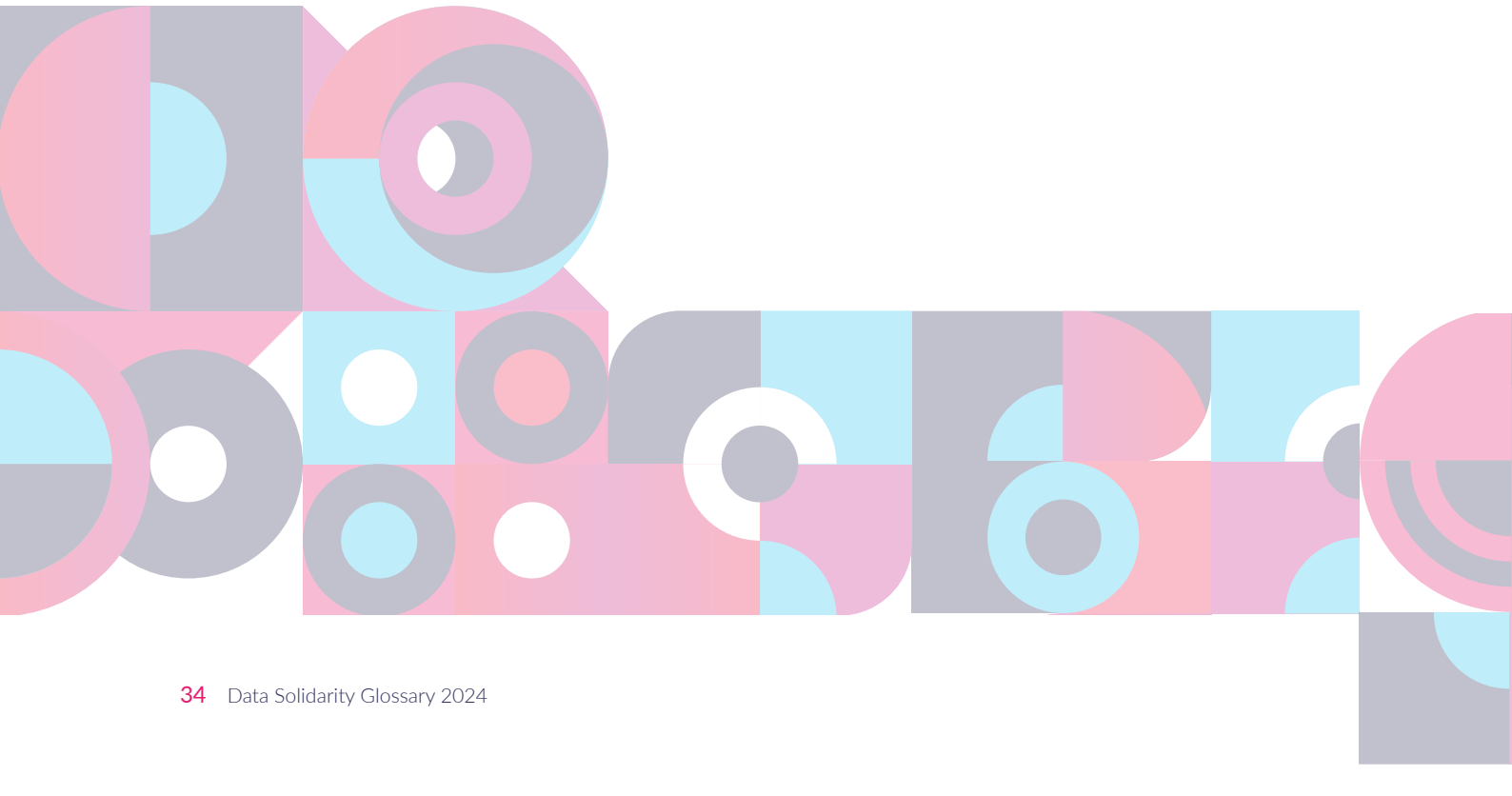
Some actors are not protecting or using data ethically. For example, many tech platforms share data generated by their users with third parties; indeed, their business model is based on the sale of these data – the data collected go far beyond personal data and include sharing of a user's friends list, etc. Many algorithms discriminate against minorities and vulnerable groups in society. But

above all many actors are negligent in procedural compliance.

Data governance proposals typically include reference to ethical principles which include, inter alia, transparency, fairness, accountability, individual agency and data privacy. Governmental risk agencies – such as NIST, the US technology standards organization and DataEthics.eu – have provided guidance on practical application considering potential harm to people, organizations and systems. An important step is to introduce Internal Review Processes and Boards to oversee ethical data management. Five critical issues for review of ethical data handling have been proposed. As they examine new projects that will involve data, companies need to focus beyond privacy on five critical issues: the provenance of the data, the purpose for which it will be used, how it is protected, how the privacy of the data providers is ensured and how the data is prepared for use. There is a need to move on from policy discussions to practical technological ethics-by-design solutions that integrate these principles into practice.

Digital and data ethics are central to data solidarity also in the sense that they underline that regulation related to digital technologies is not only about protecting data privacy or security. It is also about protecting citizens, customers and users from data practices by both the public and the private sector that adversely impact people and society.

References: Cepelak, 2023; Ministère de la Santé et de la Prévention, 2022; Segalla & Rouziès, 2023; Viberg Johansson et al., 2022.



4.2 Digital humanism

Influenced by the historical notion of humanism during the Renaissance and Enlightenment, today, humanism is often considered as a guiding principle for human interaction. In the context of digital practices, it is often used to refer to human-machine interaction that is focused on the well-being of people and that is respectful of values such as privacy, dignity or solidarity.

Scholars and practitioners in the field of digital humanism work on a range of questions such as: How can humanistic values be translated into tools for governing data practices in the public and private sector? What requirements must be set, for example, for the application of algorithmic decision making to avoid the quest for technological efficiency and economic growth that hurts fundamental human rights? These questions make the protection of human rights a crucial subject of data governance.

An example is the Vienna Manifesto on Digital Humanism (2019). This document, to which scholars and practitioners from a wide range of fields contributed, defines digital humanism as the linking of humanistic ideals with critical thoughts about technological progress. It defines it as an interdisciplinary approach to understanding and shaping the interplay of technology and humankind for a better society.

A digital humanism perspective also challenges some common assumptions, such as the idea that automated systems outperform human mathematical and analytical skills. Digital humanism opposes such an understanding of supposedly 'autarchic technological development'. Digital humanism emphasizes the exclusive human ability to determine the purposes of computational problem-solving mechanisms by shaping the premises and values being applied in them. Policymakers should focus on the opportunities that digital technologies provide to improve human living conditions. In other words, digital humanism does not reject data-driven practices, but it wants to see digital practices being used in the service of giving 'people the possibility to concentrate on what is essential and contribute to a more humane and just future for humanity'.

While data solidarity shares a lot with digital humanism, it is not limited to humanism in terms of the substantive values that it draws upon. It is oriented around a wider range of values such as equity, justice and, of course, solidarity.

References: Autili et al., 2019; Coeckelbergh, 2024; Mittelstadt et al., 2016; Neidhardt et al., 2022; Nida-Rümelin, 2022; Nowotny, 2022; Prainsack et al., 2022b; Werther et al., 2019; Werthner et al., 2022.

4.3 Data discrimination

Data discrimination is one of the harms in digital societies that data solidarity sets out to prevent. With enormous volumes of data generated every day, more and more decisions – also in health and health care – are influenced by data analysis and algorithms. This situation is exacerbated with the use of generative AI in ever wider fields of life and work. Despite the often-presumed neutrality of technology, AI systems can have discriminatory effects when used for decision-making. In Europe, the General Data Protection Regulation (GDPR) emphasizes the need to prevent discrimination as a result of automated decision making and gives people a right to 'meaningful information' about the logic underlying automated decisions.

Data discrimination occurs when individuals or groups are treated unfairly because of characteristics or traits identified through the collection and analysis of their data. The introduction and application of big data takes place within the context of historical inequities in health and health care – the discrimination can derive from the data sources used to train AI systems, the way the systems are used and the way they have been designed. This can lead to perpetuating social inequalities and creating new patterns of discrimination in the health care system related to, for example, age, gender, ethnicity, religion, sexual preference or genetic characteristics. Concerns in relation to ethics, fairness, equity and transparency in the development of big data tools must be addressed. This is best done through the involvement and open communication with stakeholders. In the case of health care, the stakes are particularly high, as the life and health of marginalized and underserved groups could be endangered.

Structural inequalities, biases and racism in society are easily encoded in datasets and in the application of data science. When it is these data that are used to train software, this replicates the bias. It is therefore important to address the low diversity in health data science and increase the competencies of data stewards (the people responsible for managing and overseeing an organization's data) so that data systems do not unfairly discriminate against groups, whether intentional or not. The European Union's AI Act includes a provision that would enable organizations to use special categories of data for auditing their AI systems to ensure they do not discriminate.

Data solidarity endorses the goal to fight data discrimination. More broadly, it seeks to ensure that all harms – not only discrimination – and all benefits are distributed more equitably across and within societies.

References: Ibrahim et al., 2020; Knight, 2021; Pot et al., 2021; Wójcik, 2022.

4.4 Data extraction

Data extraction refers to the process of collecting or retrieving disparate types of data from a variety of sources, many of which may be poorly organized or completely unstructured and then applying it to analytical processing for specific purposes, for example marketing. This is referred to as web scraping with data sources including social media use, behaviour tracking, web pages, emails and a wide variety of documents. Data extraction in research involves collecting and retrieving relevant data from various sources for the purpose of analysis, interpretation and deriving conclusions.

Extracting patterns from large quantities of unstructured data is referred to as data mining or data analytics. Increasingly this is now done through methods such as artificial intelligence and machine learning, both profit and as algorithmic governance for public policy objectives. In healthcare, data extraction plays an increasingly important role in patient care and predictive medicine as well as in medical research. For example, the demand for reliable health information increased significantly during the COVID-19 pandemic. Many health systems could not, however, ensure the flow of necessary data and information between providers and public health agencies, making it difficult to detect patterns and interpret them to obtain actionable insights. As such, data extraction creates commercial and other benefits, while also posing risks. A central aim of data solidarity is to ensure that these benefits and risks are shared more fairly than is the case today.

As with all forms of data use, data extraction raises issues of privacy, ethics, politics, and issues of serious legal concern. This has been the case in several programmes that have applied algorithmic governance to the welfare system. The aggregation and combining of data may facilitate analysis but might also make identification of individual level data possible, even if the data were originally anonymous, possibly leading to data breaches. It can also imply new forms of exploitation when data are analysed and monetized without consent or even the knowledge of the people who the data come from – in favour of actors who derive profit. This increases power asymmetries between data subjects (the people that share their data) and data using organizations, with the latter having much greater opportunities to benefit from the data economically and the former carrying almost all of the risk.

Data solidarity seeks to bring down the risks of data extraction. It also seeks to ensure that the remaining risks, as well as the benefits stemming from the extraction, use and re-use of data are distributed equitably within and across societies.

References: Constantaras et al., 2023; Talend, undated; Taylor et al., 2021.

4.5 Data colonialism

Data colonialism aims to capture a development that is no longer defined by the extraction of natural resources or labour but is based in the appropriation of human life through data.

The concept of data colonialism encompasses all digital practices through which individuals and communities (such as Indigenous people and communities) are marginalized or dispossessed through the extraction, control and use of their data by more powerful actors, both private and public, either for profit or for political control. This process shares many defining characteristics with the colonial extraction of resources linked to territorial conquests.

Data colonialism works at many levels. It impacts users through the terms of use to which they consent for their on-line interactions and the ways in which data on their everyday life activities is bundled and monetized. The related concept of surveillance capitalism analyses the ways in which human behaviours, bodies and environments are turned into a resource that is converted into data and consequently into profits. Generative AI can perpetuate data colonialism by extracting data from content creators without fair compensation, concentrating control and benefits in the hands of a few and widening global inequalities.

Another extractive process is global data capture – data from everyone, everywhere – that has not yet been subject to a serious global governance response.

We have not yet considered sufficiently the impact of new data methods and systems based in the Global North and being introduced and reinforced through global institutions – for example the UN Statistical Commission – without sufficient consideration to national and local contexts. Data provide the basis for international reporting on developmental progress, such as the Sustainable Development Goals and define the allocation of resources. The increasing reliance on data from these processes for decision making exacerbate the problem: phenomena and factors that cannot be measured and represented in the form of data are invisible to policy makers.

Credible and reliable data are particularly relevant for global health – especially during outbreaks and pandemics. Countries must be able to have full trust in the mechanisms of data sharing and especially the value it brings for low- and middle-income countries in the face of major inequities. The WHO has proposed that global health data be treated as a public good but data solidarity has not yet been accepted as an approach to apply. Concerns have also been raised, in relation to global reporting requirements such as the Global Burden of Disease Report, in that it transfers power from institutions in low-income countries to ones based in high-income countries, hampers the development of national health information systems and privileges certain forms of knowledge over others.

References: Birch, 2023; IHME, undated; Kim et al., 2017; Mitchell, 2021; Shiffman & Shawar, 2020; Universität Bern, 2021; Zuboff, 2019.

Section 5: Moving forward

5.1 Digital transformations for health

Digital technologies and artificial intelligence (AI) are now at the very core of health – not least because of their ubiquity in everyday life. In 2021, *The Lancet* and *Financial Times* Commission issued an urgent call to action for health and digital policy makers to ensure that digital transformations are motivated by public value rather than private profit and support the missions of public health, universal health coverage and health for all. It proposed to apply the term digital health only to clearly defined applications in health and medicine and to develop an understanding of the broader impact of digital technologies. Ethical perspectives on digital transformations for health need an expansion from bioethics to socio-technical ethics that assess the broader impact of technologies on health and health care.

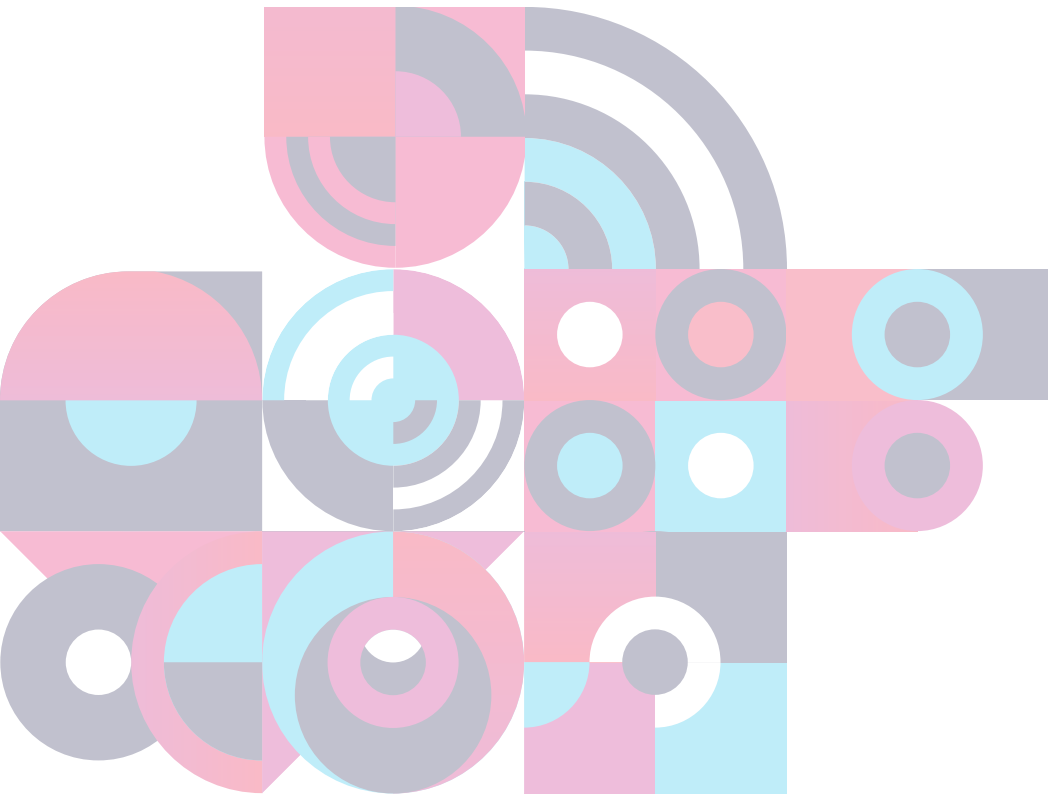
Digital transformations are *determinants* of health that interact with larger political, societal and economic dynamics and policies must address them accordingly. They will increasingly become the dominant prism through which we think about health and well-being, driven forward by the datafication of health, including AI as well as data-driven analyses within genomics. Medicine has always been driven by scientific breakthroughs and technological innovation. But the very nature of the technology linked to the level of convergence that we are seeing now and the speed of change, are unprecedented. There is also an increasing convergence between digital transformations and public health, reinforced through the COVID-19 pandemic. The pandemic showed how health, data and the power of digital

connectivity transcend borders but at the same time reinforce established inequalities and discriminations. The pandemic also highlighted the influence of the large, global digital providers and platforms, many of whom were already rapidly entering the health space and were now gaining increasing relevance.

The boundaries of digital transformations of health are being pushed forward at an accelerating pace, often without concern for their effects on health equity and human rights. The rapid access to real time information and the intensity of the digital debate require constant vigilance and updating.

Without a commitment to solidarity, justice and new forms of digital health citizenship, health could become a favoured entry point in support of new forms of surveillance capitalism, data colonialism or digital welfare dystopias. (See **Data colonialism**) Following a massive surveillance surge during the pandemic, we are already witnessing such developments in several countries around the world. The most challenging dimension of the extreme imbalance of who benefits from the digital transformation is what Shoshana Zuboff has termed 'surveillance capitalism'.
Data solidarity works toward the goal of maximizing the value that health data and other digital data create for the public, yet not at the cost of people and communities.

References: Kickbusch et al, 2021; Zuboff, 2019.



5.2 Trust in data and platforms

The Lancet and *Financial Times* Commission has argued that building trust among all stakeholders of the digital health ecosystem is one of the most urgent areas for action as low-trust environments are risk environments for health. Data solidarity, as an approach to data governance that seeks to achieve a more equitable sharing of the benefits and risks of digital practice, can help to build trust in data practices.

Data can be a matter of life or death in a health crisis – they also pose a set of ethical and human rights challenges. We saw saw during COVID-19 how missing data on the ethnic background of those who become critically ill with COVID, led to unaddressed disparities in health outcomes. The lack of harmonized data collection standards made cross-country comparison of epidemiological information unnecessarily challenging. Health misinformation is another well-known consequence of poor data governance. As people felt they were not gaining access to services or reliable information, their confidence in existing systems and sources of information was lost.

Concerns about privacy, safety and rights violations are contributing to a lack of trust among communities, health workers and other groups. This limits the adoption of potentially beneficial innovations as well as the sharing of data and solutions between people, countries and digital health actors – and leads to lack of evidence-based decision making for health.

But without trust – between people, institutions and nations – to share data at local, national, regional and global levels, society will not be able to benefit from the huge volumes of health data that exist to improve health, health care and decision-making. Innovations with the potential to advance public health goals will remain limited.

As noted, data solidarity is a way to increase trust – not by demanding it from people or emphasizing its importance, but by increasing the genuine trustworthiness of data use. By ensuring that particularly risky data uses are prohibited and these prohibitions effectively enforced and by introducing measures to mitigate harm, they seek to protect people more effectively than was previously the case. Moreover, data solidarity also tries to address inequities at a global level.

References: Bollyky et al., 2023; Borges do Nascimento et al., 2022; Kickbusch et al., 2021.

5.3 Datafication of health

Datafication transforms various aspects of our lives and health into (often) large volumes of data that can be collected, stored, analysed, shared and used to gain insights and train AI. In the domain of health, datafication has transformed clinical research and drug development processes. It supports health professionals in making informed decisions and personalizing care, allows the analysis of aggregated and de-identified health data for population health research and public health surveillance. Datafication can play a role in improving patient care as well as increasing efficiencies in health care systems. The increasing datafication of our lives and environments is a key reason why data solidarity is needed.

A breakthrough in datafication has come with the introduction of wearable devices which can help users monitor progress, identify patterns, detect anomalies and make data-based decisions about their health and wellness, based on real-time feedback. This is also regarded by some with concern, as it means that qualitative aspects of health and well-being are turned into quantified data. People – taking images and logging calories and other data from their meals – are datafying an important aspect of their health that used to be unrecorded before. Whereas patients used to report about these aspects of their lives in their own voice, their data now tell the story. Moreover, many types of health data are highly sensitive, meaning that their unauthorized use by third parties could cause a lot of harm, ranging from losing access to (private) health and other insurance to, in extreme cases, job losses and severe social stigmatization. Moreover, even innocuous sets of data, when linked with other datasets, can lead to inferences being made regarding individuals that can lead to discriminatory or other harmful action. Sometimes this is because the algorithms that are employed for data analysis reflect problematic biases; at other times this is because existing laws and policies do not sufficiently protect people from the harms of predictive analytics and other data analyses. This is not only a problem in the business sector, but also the public sector in some countries which has used predictive analytics to the detriment of people. The Robodebt scandal in Australia and the Dutch child benefit scandal illustrate significant issues with data usage by public bodies, resulting in severe consequences for affected individuals.

Against this backdrop, next to data security and privacy, data solidarity seeks to ensure that people have adequate control over data that they have a stake in. This includes giving people a say – individually or as part of communities that they belong to – in what types of knowledge and information should be datafied in the first place. Data solidarity also seeks to ensure that commercial profits that are achieved with people's data are fairly shared with communities.

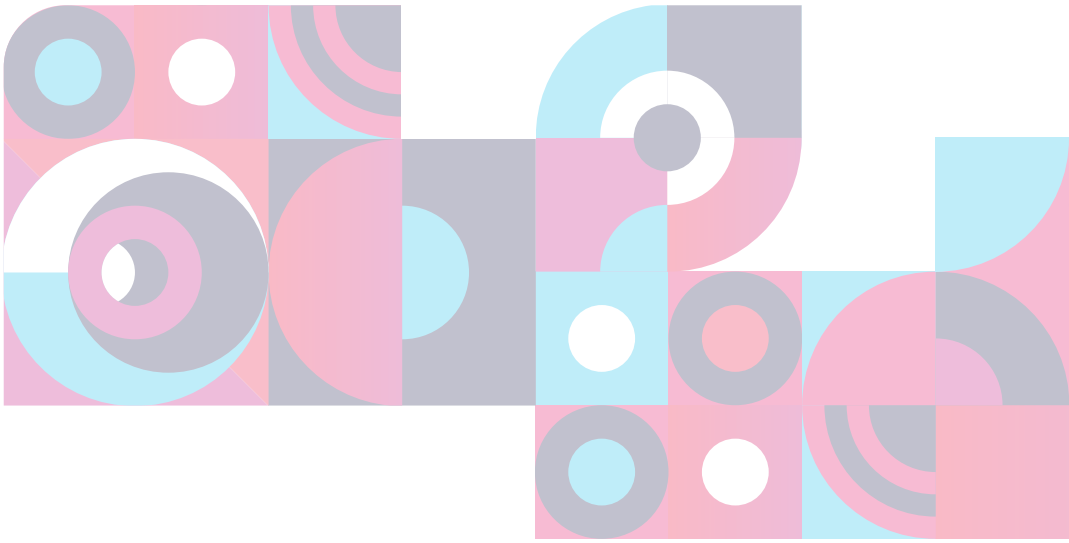
References: Carney, 2019; Eubanks, 2018; Fenger & Simonse, 2024; Quantified Self Through Numbers, undated; Ruckenstein et al., 2018; ten Seldam & Brenninkmeijer, 2021; University of Sydney, 2023.

5.4 Digital health literacy

General health literacy has long been identified as a key determinant of health – low health literacy is a major risk to health. As the digital transformation progresses, digital literacy and digital health literacy have also gained in relevance, especially when addressing the digital divide in health. As disparities in digital access and digital literacy affect people's access to health information and health services, they affect health outcomes. We know that the demand for basic and advanced digital skills will grow significantly for patients and health care professionals as healthcare organizations expand the use of digital technologies, including artificial intelligence. But a digital health report from the WHO European Region shows very few countries are actively investing in digital health literacy. This will create increasing problems and inequalities – for example due to significant demographic shifts.

A useful approach to the many dimensions of digital health literacy is the transactional model of e-health literacy which outlines four competence levels for digital health literacy: functional, communicative, critical and translational. In the context of data solidarity, critical digital health literacy gains particular importance as it refers to the 'ability to evaluate the relevance, trustworthiness and risk of sharing and receiving health related information through the digital ecosystem'. But there is also a very important component to communicative health literacy which is captured in the notion of civic literacy – it addresses the knowledge and ability to participate and refers to how people communicate in digital contexts and how aware they are with regard to their rights and responsibilities in the digital ecosystem. Digital health literacy is therefore of high relevance to practising digital health citizenship. (See **Digital health citizenship**)

References: Kickbusch & Holly, 2023; Paige et al., 2018; Seidel et al., 2023; van Kessel et al., 2022; World Health Organization Regional Office for Europe, 2023.



5.5 Digital health citizenship

Digital health citizenship not only defines a set of rights and responsibilities that emerge through the use of digital technology (e.g. health apps and platforms) to meet health-related purposes but also the process and forms of interaction and participation that are created in the digital health space.

There is a strong need for data governance to become more democratic and help ensure equitable access to resources. Individuals and groups must be able to actively participate in and cocreate the design and implementation of digital health policy and technologies and to feed back to decision makers, development agencies and private companies and developers. This includes equity frameworks for technology development and digital spaces and building community resilience to negative impacts of digital transformations. A value-based and people-centred approach to governing digital transformations for health builds on digital health citizenship to counteract what has been termed surveillance capitalism. The digital ecosystem is dependent on the participation of its users – it only works if patients and others are willing to contribute their data. Indeed it would protect users from the extraction of their data and the constant algorithm nudges that drive online behaviour.

The digital ecosystem offers new spaces for political participation and civic debate, including on health matters. But equitable health benefits can only be realized when citizens are able to critically engage, feel protected from misinformation and discrimination and can make informed choices in respect to their data. Participatory data governance must be a defining feature of 21st century digital health citizenship. This could entail that, where data about people's bodies or very personal aspects of their lives are concerned, people have a direct say in how the data are used. The data solidarity approach also proposes that stronger use be made of collective forms of oversight and the strengthening of institutionalized solidarity. But so far very few governments have worked to strengthen the democratic and solidarity incentives and benefits of the digital health ecosystem.

Research on the new 'digital health citizenship' shows the willingness of people to share information, experiences and data – but frequently they are not aware if they are doing this on a publicly owned or non-profit or on a commercial platform or what role algorithms play in prompting their choices and what happens with the data they share. Digital health citizenship requires competencies in health literacy, digital literacy and broader democratic and civic literacy. Civic technology models, which broadly refer to the co-creation (between users, tech developers, etc) and use of digital technologies to improve public participation in democratic and decision-making processes, are increasingly seen as enablers of improved public policy and service delivery, including in health.

Active digital heath citizenship is often constrained by the digital divide. Inequality is reinforcing; it is often the same people and communities who are not connected to the internet, who have low levels of literacy and who have least access to quality healthcare. Collaborative governance models that bring together different sectors – public and private – must also include such communities to address the ensuing equity challenges.

References: Kickbusch, 2023; Petrakaki et al., 2021; Prainsack & Buyx, 2017; Zuboff, 2019.

Bibliography

Adecco Group. (2023). *Understanding Digital Justice: How Can We Fight for Fair Technological Practices.* [Online] https://www.adeccogroup.com/future-of-work/latest-insights/understanding-digital-justice-how-can-we-fight-for-fair-technological-practices

Affleck, E., Sutherland, E., Lindeman, C., Golonka, R., Price, T., Murphy, T., Williamson, T., Chapman, A., Layton, A., & Fraser, C. (2024). Human Factor Health Data Interoperability. *HealthcarePapers*, *21*(4), 47–55. https://doi.org/10.12927/hcpap.2024.27272

Afina, Y. et al. (2024). Towards a global approach to digital platform regulation: Preserving openness amid the push for internet sovereignty. *Royal Institute of International Affairs.* https://doi.org/10.55317/9781784135935.

Autili, M., Di Ruscio, D., Inverardi, P., et al. (2019). A Software Exoskeleton to Protect and Support Citizen's Ethics and Privacy in the Digital World. *IEEE Access*, *7*, *62011-62021*. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8712524

Benjamin, R. (2019). *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge: Polity Press.

Bezuidenhout, L. M., Leonelli, S., Kelly, A. H., et al. (2017). Beyond the digital divide: towards a situated approach to open data. *Sci Public Policy*, *44*(4),464-475. https://doi.org/10.1093/scipol/scw036

Birch, K. (2023). *Data.* In: Data Enclaves. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-46402-7_2

Blasimme, A., Vayena, E. & Hafen, E. (2018). Democratizing Health Research Through Data Cooperatives. *Philos. Technol.*, *31*, 473-479. https://doi.org/10.1007/s13347-018-0320-8

Bollier, D,. & Helfrich, S. (2019). *Free, fair and alive: The insurgent power of the commons.* New Society Publishers.

Bollyky. T.J., Kickbusch, I., Petersen, M.B. (2023). *The Trust Gap: How to Fight Pandemics in a Divided Country* [Online]. Foreign Affairs. www.foreignaffairs.com/united-states/trust-gap-fight-pandemic-divided-country

Borges do Nascimento, I. J., Pizarro, A. B., Almeida, J. M., Azzopardi-Muscat, N., Gonçalves, M. A., Björklund, M., & Novillo-Ortiz, D. (2022). Infodemics and health misinformation: a systematic review of reviews. *Bulletin of the World Health Organization*, *100*(9), 544–561. https://doi.org/10.2471/BLT.21.287654

Bozeman, B. (2007) *Public values and public interest: Counterbalancing economic individualism*. Georgetown University Press. https://www.jstor.org/stable/j.ctt2tt37c

Braun, M., & Hummel, P. (2022). Data justice and data solidarity. *Patterns. (New York, N.Y.)*, *3*(3), 100427. https://doi.org/10.1016/j.patter.2021.100427

Brock, A. (2020). *Distributed Blackness: African American Cybercultures*. NYU Press.

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. *JCMS: Journal of Common Market Studies*, (61), 1261–1280. https://doi.org/10.1111/jcms.13462.

Bryson, J.M., Crosby, B.C. and Bloomberg, L. (2014). Public Value Governance: Moving Beyond Traditional Public Administration and the New Public Management. *Public Admin Rev*, 74, 445-456. https://doi.org/10.1111/puar.12238

Carney, T. (2019). Robo-debt illegality: The seven veils of failed guarantees of the rule of law? *Alternative Law Journal*, *44*(1), 4-10. https://doi.org/10.1177/1037969X18815913

Carrier, J.G. (1991). Gifts, commodities and social relations: A Maussian view of exchange. *Sociological Forum*, *6*, 119-136. https://doi.org/10.1007/BF01112730

Carroll, S.R., Garba, I., Figueroa-Rodríguez, O.L., et al. (2020). The CARE principles for indigenous data governance. *Data Science Journal*, *19*, 43-43. https://doi.org/10.5334/dsj-2020-043

Castells, M. (2002). I*nformational capitalism*. In: Theories of The Information Society, *Routledge*, 97-123. https://doi.org/10.4324/9780203426265

Cepelak, C. (2023). *An Introduction to Data Ethics: What is the Ethical Use of Data?* [Online]. Datacamp. https://www.datacamp.com/blog/introduction-to-data-ethics

Chander, A. (2020). Is Data Localization a Solution for Schrems II? *Journal of International Economic Law*, *23*, (3), 771–784. https://doi.org/10.1093/jiel/jgaa024

Chander, A. & Lê, U.P. (2014). Data nationalism. *Emory LJ*, 64, 677. https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2

Chavez, P. (2022). *Toward digital solidarity*. Lawfare Media. [Online]. https://www.lawfaremedia.org/article/toward-digital-solidarity

Coeckelbergh, M. (2024). What is digital humanism? A conceptual analysis and an argument for a more critical and political digital (post) humanism. *Journal of Responsible Technology*, 17:100073. https://doi.org/10.1016/j.jrt.2023.100073

Cohen, B., Hall, B. & Wood, C. (2017). *Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy*. Antitrust, 32, 107. https://www.americanbar.org/digital-asset-abstract.html/content/dam/aba/publications/antitrust/magazine/archived/2017/fall/data-localization-laws-impact-on-privacy.pdf

Constantaras, E., Geiger, G., Braun, J. C., et al. (2023). *Inside the Suspicion Machine* [Online]. Wired. https://www.wired.com/story/welfare-state-algorithms/

Couldry, N., & Mejias, U. A. (2019). *The Costs of Connection: How Data is Colonizing Human Life and Appropriating it for Capitalism*. Stanford University Press.

Coventry, L., & Branley, D. (2018) Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48-52. https://doi.org/10.1016/j.maturitas.2018.04.008

Dawson, A., & Verweij, M. (2012). Solidarity: a Moral Concept in Need of Clarification. *Public Health Ethics*, *5*(1), 1–5. http://www.jstor.org/stable/26644892

De Angelis, M. (2017). *Omnia Sunt Communia: On the Commons and the Transformation to Postcapitalism*. London: Zed Books. https://www.bloomsbury.com/uk/omnia-sunt-communia-9781783600625/

Delacroix, S., & Lawrence, N.D. (2019) Bottom-up data trusts: Disturbing the 'one size fits all' approach to data governance. *Int Data Privacy Law*, *9*(4),236-252. https://doi.org/10.1093/idpl/ipz014

Dulong de Rosnay, M. & Stalder, F. (2020). Digital commons. *Internet Policy Review, 9*(4). https://doi.org/10.14763/2020.4.1530

D4DHub. (Undated). *Data governance in Africa*. [Online] https://d4dhub.eu/initiatives/data-governance-in-africa

Ebeling, M. F. (2016). *Healthcare and big data*. London, New York: Palgrave Macmillan. https://link.springer.com/book/10.1057/978-1-137-50221-6

Element AI, Nesta. (2019). *Data Trusts: A new tool for data governance*. White Paper. https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf

El-Sayed, S., & Prainsack, B. (2022). Success of the European Health Data Space hinges on operationalizing public value, in addition to bridging digital divides. *BMJ Rapid Response*. https://www.bmj.com/content/378/bmj-2022-071913/rr-0

El-Sayed, S., Prainsack, B., Hogan, C., et al. (2023). *PLUTO – Public Value Assessment Tool*. University of Vienna. https://pluto.univie.ac.at/

Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor:* St. Martin's Press, New-York, 2018, 272 p. https://doi.org/10.4000/sdt.42117

European Commission. (2020). *Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*. COM(2020) 767 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

European Commission. (2022). Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. COM(2022) 197 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197

European Parliament & Council of the European Union. (2022). *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)*, OJ L 152. http://data.europa.eu/eli/reg/2022/868/oj

Fenger, M., & Simonse, R. (2024). The implosion of the Dutch surveillance welfare state. *Social Policy & Administration*, *58*(2), 264–276. https://doi.org/10.1111/spol.12998

First Nations Centre. (2007). *OCAP: Ownership, Control, Access and Possession. Sanctioned by the First Nations Information Governance Committee. Assembly of First Nations*. Ottawa: National Aboriginal Health Organization. https://icwrn.uvic.ca/wp-content/uploads/2013/08/FNC-OCAP.pdf

First Nations Information Governance Centre. (2014). *Ownership, Control, Access and Possession (OCAP): The Path to First Nations Information Governance*. Ottawa: The First Nations Information Governance Centre. https://achh.ca/wp-content/uploads/2018/07/OCAP_FNIGC.pdf

Floridi, L. (2020). The fight for digital sovereignty: What it is and why it matters, especially for the EU. *Philosophy & Technology, 33*, 369–378. https://doi.org/10.1007/s13347-020-00423-6

Fukumoto, E., & Bozeman, B. (2019). Public Values Theory: What Is Missing? *American Review of Public Administration, 49*(6), 635-648. https://doi.org/10.1177/0275074018814244

Fuster Morell, M. (2011). *An Introductory Historical Contextualization of Online Creation Communities for the Building of Digital Commons: The Emergence of a Free Culture Movement*. In Hellmann, S., Frischmuth, P., Auer, S. & Dietrich, D. (ed.). OKCon 2011. Open Knowledge Conference Proceedings of the 6th Open Knowledge Conference Berlin, Germany, June 30 & July 1, 2011. Universität Leipzig, Germany and Technical University Berlin, Germany. http://ceur-ws.org/Vol-739/

Gao, H.S. (2021). *Data Sovereignty and Trade Agreements: Three Digital Kingdoms*. In: Chander A, Haochen, S, eds. Data sovereignty: From the digital Silk Road to the return of the state. Oxford: Oxford University Press. 213-239. https://doi.org/10.1093/oso/9780197582794.003.0010

Gordon, G. (2024). Digital sovereignty, digital infrastructures, and quantum horizons. *AI & Soc 39*, 125–137. https://doi.org/10.1007/s00146-023-01729-7

Hardinges, J., Wells, P., Blindfold, A., Tennison, J., & Scott, A. (2019). *Data trusts: lessons from three pilots*. Open Data Institute. https://theodi.org/article/odi-data-trusts-report/

Hardjono, T., & Pentland, A. (2020). 4. *Empowering Innovation through Data Cooperatives*. In Building the New Economy. https://doi.org/10.21428/ba67f642.0499afe0

Harman, L. B., Flite, C. A., & Bond, K. (2012). Electronic health records: privacy, confidentiality and security. *The virtual mentor : VM*, *14*(9), 712–719. https://doi.org/10.1001/virtualmentor.2012.14.9.stas1-1209

He, A. (2023). *State-centric data governance in China*. CIGI Papers No. 282. Centre for International Governance Innovation. https://www.cigionline.org/static/documents/no.282.pdf

Heeks, R., & Renken, J. (2018). Data justice for development: what would it mean? *Information Development*, *34*(1), 90-102. https://doi.org/10.1177%2F0266666916678282

Hill, E.R. (2023). *Are data trusts trustworthy? Data is vital to health innovation but there remains a common feeling of mistrust in those who hold that data. Why?* [Online]. PHG Foundation. Accessed at: https://www.phgfoundation.org/blog/are-data-trusts-trustworthy/

Hummel P., Braun M. (2020). Just data? Solidarity and justice in data-driven medicine. *Life Sciences, Society and Policy. 16*(8), 1-18. https://doi.org/10.1186/s40504-020-00101-7

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society, 8*(1). https://doi.org/10.1177/2053951720982012

Ibrahim, S. A., Charlson, M. E., & Neill, D. B. (2020). Big Data Analytics and the Struggle for Equity in Health Care: The Promise and Perils. *Health equity*, *4*(1), 99–101. https://doi.org/10.1089/heq.2019.0112

IHME. (Undated). *Global Burden of Disease* [Online]. https://www.healthdata.org/research-analysis/gbd

Jussen, I., Schweihoff, J., Dahms, V., et al. (2023). *Data Sharing Fundamentals: Characteristics and Definition*. In: Proceedings of the 56th Hawaii International Conference on System Sciences (HICSS), Maui, Hawaii, USA. http://dx.doi.org/10.24251/HICSS.2023.452

Kattel, R., & Mazzucato, M. (2018). Mission-oriented innovation policy and dynamic capabilities in the public sector. *Industrial and corporate change. 27*(5), 787-801. https://doi.org/10.1093/icc/dty032

Kickbusch, I. (2023). *Digital transformations – why we must build digital health citizenship* [Online]. Governing Health Futures: The Lancet and Financial Times Commission. https://www.governinghealthfutures2030.org/digital-transformations-why-we-must-build-digital-health-citizenship/

Kickbusch I, Holly L. (2023). Addressing the digital determinants of health: health promotion must lead the charge. *Health Promotion International*, *38*(3). https://academic.oup.com/heapro/article/38/3/daad059/7188360

Kickbusch, I., Piselli, D., Agrawal, A., et al. (2021). The Lancet and Financial Times Commission on governing health futures 2030: Growing up in a digital world. *The Lancet*, *398* (10312), 1727-1776. https://doi.org/10.1016/s0140-6736(21)01824-9

Kim, J. U., Oleribe, O., Njie, R., & Taylor-Robinson, S. D. (2017). A time for new north-south relationships in global health. *International journal of general medicine*, *10*, 401–408. https://doi.org/10.2147/IJGM.S146475

Kitchin, R. (2014). The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences. *Journal of Regional Science*, *56* (4). http://dx.doi.org/10.1111/jors.12293

Kraut, R. 2020. *Altruism*. In E. N. Zalta (Ed.), The Stanford Encyclopedia of Philosophy (Fall 2020 Edition). https://plato.stanford.edu/archives/fall2020/entries/altruism/.

Knight, H. E., Deeny, S. R., Dreyer, K., Engmann, J., Mackintosh, M., Raza, S., Stafford, M., Tesfaye, R., & Steventon, A. (2021). Challenging racism in the use of health data. *The Lancet. Digital health*, *3*(3), e144–e146. https://doi.org/10.1016/S2589-7500(21)00019-4

Koontz, L. (2017). *Information Privacy in the Evolving Healthcare Environment (2nd ed.).* CRC Press. https://doi.org/10.1201/b21867

Krutzinna, J., Floridi, L. (2019). Ethical Medical Data Donation: A Pressing Issue. In: Krutzinna, J., Floridi, L. (eds) The Ethics of Medical Data Donation. *Philosophical Studies Series, 137*. Springer, Cham. https://doi.org/10.1007/978-3-030-04363-6_1

Kukutai, T., & Taylor, J. (2016). eds. *Indigenous Data Sovereignty: Toward an Agenda*. Canberra: Australian National University Press.

Leonelli, S. (2020). *Scientific Research and Big Data*. In E. N. Zalta (Ed.), The Stanford Encyclopedia of Philosophy (Summer 2020 Edition). https://plato.stanford.edu/archives/sum2020/entries/science-big-data

Levin, N., Leonelli, S., Weckowska, D., et al. (2016). How Do Scientists Define Openness? Exploring the Relationship Between Open Science Policies and Research Practice. *Bulletin of science, technology & society, 36*(2), 128–141. https://doi.org/10.1177/0270467616668760

Linstedt, D. & Olschimke, M. (2015). *Building a scalable data warehouse with data vault 2.0*. Morgan Kaufmann. https://www.sciencedirect.com/book/9780128025109/building-a-scalable-data-warehouse-with-data-vault-2-0

Liu, J. (2022). *China's data localization*. In China's Globalizing Internet, 83-102. Routledge. https://doi.org/10.4324/9781003319184

Longo, D. L., & Drazen, J. M. (2016). Data Sharing. *The New England journal of medicine*, *374*(3), 276–277. https://doi.org/10.1056/NEJMe1516564

Mazzucato, M., & Ryan-Collins, J. (2022). Putting value creation back into "public value": from market-fixing to market-shaping. *Journal of Economic Policy Reform*, *25*(4), 345–360. https://doi.org/10.1080/17487870.2022.2053537

Marelli, L., Stevens, M., Sharon, T., et al. (2023). The European health data space: Too big to succeed?. *Health policy, 135*104861. https://doi.org/10.1016/j.healthpol.2023.104861

McDonald, S. (2019). *Reclaiming data trusts*. Centre for International Governance Innovation [Online]. https://www.cigionline.org/articles/reclaiming-data-trusts/

McDonald, S. (2022). *A Digital Sovereign, by any other name* [online]. Available at SSRN: https://ssrn.com/abstract=4035822 or http://dx.doi.org/10.2139/ssrn.4035822

McMahon, A., Buyx, A., & Prainsack, B. (2020). Big data governance needs more collective responsibility: The role of harm mitigation in the governance of data use in medicine and beyond. *Med Law Rev.*, *28(1)*155. https://doi.org/10.1093/medlaw/fwz016

Meynhardt, T. (2009). Public Value Inside: What is Public Value Creation? *International Journal of Public Administration*, *32*(3–4), 192–219. https://doi.org/10.1080/01900690902732632

Micheli, M., Farrell, E., Carballa Smichowski, B., et al. (2023). *Mapping the landscape of data intermediaries.* Publications Office of the European Union, Luxembourg. https://publications.jrc.ec.europa.eu/repository/handle/JRC133988

Ministère de la Santé et de la Prévention. (2022). *Digital health actions and initiatives under the French Presidency of the Council of the European Union during the first semester of 2022*. Press Kit. https://ue.esante.gouv.fr/sites/default/files/2022-08/DP%20PFUE%202022_EN.pdf

Mitchell, J., Ker, D., Lesher, M. (2021) *Measuring the economic value of Data*. Going Digital Toolkit Note, No. 20. https://goingdigital.oecd.org/data/notes/No20_ToolkitNote_MeasuringtheValueofData.pdf

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2). https://doi.org/10.1177/2053951716679679

Mittelstadt, B. (2017). From Individual to Group Privacy in Big Data Analytics. *Philos Technol. 30*, 475–494. https://doi.org/10.1007/s13347-017-0253-7

Moore, M. H. (1995). *Creating public value: Strategic management in government*. Harvard University Press. https://www.hup.harvard.edu/books/9780674175587

Nabatchi, T. (2012). Putting the "public" back in public values research: Designing participation to identify and respond to values. *Public Adm Rev. 72*(5), 699-708.

Nabatchi, T. (2018). Public values frames in administration and governance. P*erspect Public Manag Governance*, *1*(1), 59-72. https://doi.org/10.1093/ppmgov/gvx009

Neidhardt, J., Werthner, H., Woltran, S. (2022). It Is Simple, It Is Complicated. In: Werthner, H., Prem, E., Lee, E.A., Ghezzi, C. (eds) *Perspectives on Digital Humanism*. Springer, Cham. https://doi.org/10.1007/978-3-030-86144-5_46

Nerlich, B., Hartley, S., Raman, S., Smith, A., eds. (2018). *Science and the Politics of Openness*. Manchester: Manchester University Press. https://manchesteruniversitypress.co.uk/9781526106469/

Nida-Rümelin, J. (2022). Digital Humanism and the Limits of Artificial Intelligence. In: Werthner, H., Prem, E., Lee, E.A., Ghezzi, C. (eds) *Perspectives on Digital Humanism*. Springer, Cham. 71–75. https://doi.org/10.1007/978-3-030-86144-5_10

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.

Nowotny, H. (2022). Digital Humanism: Navigating the Tensions Ahead. In: Werthner, H., Prem, E., Lee, E.A., Ghezzi, C. (eds) *Perspectives on Digital Humanism*. Springer, Cham. 317–322. https://doi.org/10.1007/978-3-030-86144-5_43

OECD. (2016). *Recommendation of the Council on Health Data Governance.* OECD/LEGAL/0433. Paris: OECD Publishing. https://legalinstruments.oecd.org/public/doc/348/348.en.pdf

Okinawa, K. (2024) *Policy brief: Future of Data Governance in Asia and Operationalisation of 'Data Free Flow with Trust'*. ERIA. https://www.eria.org/uploads/Data-Free-Flow-with-Trust.pdf

Paige, S. R., Stellefson, M., Krieger, J. L., et al. (2018). Proposing a Transactional Model of eHealth Literacy: Concept Analysis. *Journal of medical Internet research*, *20*(10), e10175. https://doi.org/10.2196/10175

Paprica, P.A., Crichlow, M., Maillet, D.C., Kesselring, S., Pow, C., Scarnecchia, T.P., Schull, M.J., Cartagena, R.G., Cumyn, A., Dostmohammad, S. and Elliston, K.O. (2023). Essential requirements for the governance and management of data trusts, data repositories and other data collaborations. *International Journal of Population Data Science*, *8*(4). https://doi.org/10.23889/ijpds.v8i4.2142

Peng, S., Silverstein, M., Suitor, J., et al. (2018). *Use of communication technology to maintain intergenerational contact: Toward an understanding of 'digital solidarity'.* In Neves, B.B., Casimiro, C., eds. Connecting Families? Policy Press. 159-180. http://dx.doi.org/10.1332/policypress/9781447339946.003.0009

Petrakaki, D., Hilberg, E., & Waring, J. (2021). The Cultivation of Digital Health Citizenship. *Social science & medicine*, *270*, 113675. https://doi.org/10.1016/j.socscimed.2021.113675

Plotkin, D. (2020). *Data stewardship: An actionable guide to effective data management and data governance*. Academic press.

Pot, M., Kieusseyan, N. & Prainsack, B. (2021). Not all biases are bad: equitable and inequitable biases in machine learning and radiology. *Insights Imaging 12*, 13. https://doi.org/10.1186/s13244-020-00955-7

Prainsack, B. (2019a). Logged out: Ownership, exclusion and public value in the digital data and information commons. *Big Data & Society*, *6*(1). https://doi.org/10.1177/2053951719829773

Prainsack, B. (2019b). Data Donation: How to Resist the Leviathan. In: Krutzinna, J., Floridi, L., eds. The Ethics of Medical Data Donation. *Philosophical Studies Series*, *137*. Cham: Springer. https://doi.org/10.1007/978-3-030-04363-6_2

Prainsack, B. (2022). Beyond Vaccination Mandates: Solidarity and Freedom During COVID-19. *Am J Public Health*, *112*(2), 232-233. https://doi.org/10.2105%2FAJPH.2021.306619

Prainsack, B., & Buyx, A. (2011). *Solidarity: Reflections on an emerging concept in bioethics*. London: Nuffield Council on Bioethics. https://www.nuffieldbioethics.org/publications/solidarity

Prainsack, B., & Buyx, A. (2016). Thinking ethical and regulatory frameworks in medicine from the perspective of solidarity on both sides of the Atlantic. *Theoretical medicine and bioethics*, *37*(6), 489–501. https://doi.org/10.1007/s11017-016-9390-8

Prainsack B, Buyx A. (2017). *Solidarity in Biomedicine and Beyond*. Cambridge, UK: Cambridge University Press; 2017. https://doi.org/10.1017/9781139696593

Prainsack, B., El-Sayed, S., Forgó, N., et al. (2022a). Data Solidarity: a blueprint for governing health futures. *The Lancet Digital Health*, *4*(11), e773-e774. https://doi.org/10.1016/S2589-7500(22)00189-3.

Prainsack, B., El-Sayed, S., Forgó, N., et al. (2022b). *White Paper: Data Solidarity*. Geneva: The Lancet & Financial Times Commission on Governing Health Futures. https://www.governinghealthfutures2030.org/wp-content/uploads/2022/12/DataSolidarity.pdf

Prainsack, B., & El-Sayed, S. (2023). Beyond Individual Rights: How Data Solidarity Gives People Meaningful Control over Data. *The American Journal of Bioethics*, *23*(11), 36–39. https://doi.org/10.1080/15265161.2023.2256267

Public Health Agency of Canada. (2022). *Pan-Canadian Health Data Strategy: Toward a world-class health data system.* Expert Advisory Group – Final Report. https://www.canada.ca/en/public-health/corporate/mandate/about-agency/external-advisory-bodies/list/pan-canadian-health-data-strategy-reports-summaries/expert-advisory-group-report-03-toward-world-class-health-data-system.html

What is Quantified Self?. (undated). Quantified Self. [Online]. https://quantifiedself.com/about/what-is-quantified-self/

Raj, M., De Vries, R., Nong, P., et al. (2020). Do people have an ethical obligation to share their health information? Comparing narratives of altruism and health information sharing in a nationally representative sample. *PloS one*, *15*(12), e0244767. https://doi.org/10.1371/journal.pone.0244767

Rieder, G., & Simon, J. (2017). *Big Data: A New Empiricism and its Epistemic and Socio-Political Consequences*. In Pietsch W, Wernecke J, Ott M, eds. Berechenbarkeit der Welt?: Philosophie und Wissenschaft im Zeitalter von Big Data. Wiesbaden: Springer, 85-105. https://doi.org/10.1007/978-3-658-12153-2_4

Roberts, T., & Bosch, T., (2023.) eds. *Digital citizenship in Africa: Technologies of agency and repression*. Bloomsbury Publishing. New York: Zed Books 2023. http://dx.doi.org/10.25969/mediarep/20034.

Ruckenstein, M., & Schüll, N.D. (2018). The Datafication of Health. *Ann Rev Anth.*, *46*, 261-278. https://doi.org/10.1146/annurev-anthro-102116-041244

Samochowiec, J., & Müller, A. (2021). *Are smartwatches eroding solidarity? Scenarios for a data-driven healthcare system*. Gottlieb Duttweiler Institute, Zurich. http://doi.org/10.59986/JTWO8035

Sangiovanni, A., & Viehoff, J. (2023). *Solidarity in Social and Political Philosophy*. In: Zalta EN, Nodelman U, eds. The Stanford Encyclopedia of Philosophy (Summer 2023 Edition). https://plato.stanford.edu/archives/sum2023/entries/solidarity/

Saxinger, G., & First Nation of Na-Cho Nyak Dun. (2018). Community Based Participatory Research as a Long-Term Process: Reflections on Becoming Partners in Understanding Social Dimensions of Mining in the Yukon. *North Rev.*, *47*,187–207. https://doi.org/10.22584/nr47.2018.009

Scholz, S.J. (2008). *Political solidarity*. Penn State University Press.

Sciences Po. (Undated). *Digital and Data Sovereignty*. [Online] https://www.sciencespo.fr/public/chaire-numerique/en/thematic-research/digital-and-data-sovereignty/

Seidel, E., Cortes, T., Chong, C. (2023). *Digital Health Literacy*. Patient safety Network. [Online] https://psnet.ahrq.gov/primer/digital-health-literacy

Segalla, M., & Rouziès, D. (2023). *The Ethics of Managing People's Data*. Harvard Business Review. https://hbr.org/2023/07/the-ethics-of-managing-peoples-data

Shabani, M. (2022). Will the European Health Data Space change data sharing rules?. *Science*, *375*(6587), 1357–1359. https://doi.org/10.1126/science.abn4874

Shiffman, J., & Shawar, Y. R. (2020). Strengthening accountability of the global health metrics enterprise. *Lancet*, *395*(10234), 1452–1456. https://doi.org/10.1016/S0140-6736(20)30416-5

Shults, L.M. (2024). Avoiding parasitical uses of global solidarity. *Frontiers in Human Dynamics*, *6*, 1305952. https://doi.org/10.3389/fhumd.2024.1305952

Sorbie, A. (2021). *The public interest*. In Laurie G, Dove E, Ganguli-Mitra A, et al. eds. The Cambridge Handbook of Health Research Regulation. Cambridge: Cambridge University Press. 65-72. https://doi.org/10.1017/9781108620024.009

Stalder, F. (2013). *Digital solidarity*. Vol. 6. Mute Publishing. PML Books. https://www.metamute.org/sites/www.metamute.org/files/u1/Digital-Solidarity-Felix-Stalder-9781906496920-web-fullbook.pdf

Struett, T., Aaronson, S. A., & Zable, A. (Undated). *Global data governance mapping project, Year 4*. Digital Trade & Data Governance Hub. https://globaldatagovernancemapping.org/images/DataGovHub-Year-4/short-4th-report.pdf

Szoszkiewicz, L. (2021). *Open Data: Toward Achieving and Measuring the Sustainable Development Goals*. In: Leal Filho, W., Azul, A.M., Brandli, L., Lange Salvia, A., Wall, T. (eds) Industry, Innovation and Infrastructure. Encyclopedia of the UN Sustainable Development Goals. Springer, Cham. https://doi.org/10.1007/978-3-319-71059-4_129-1

Talend. (Undated). *What is Data Extraction? Definition and Examples* [Online]. https://www.talend.com/resources/data-extraction-defined/

Taylor, K. S., Mahtani, K. R., & Aronson, J. K. (2021). Summarising good practice guidelines for data extraction for systematic reviews and meta-analysis. *BMJ evidence-based medicine*, *26*(3), 88–90. https://doi.org/10.1136/bmjebm-2020-111651

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, *4*(2). https://doi.org/10.1177/2053951717736335

Taylor, L., Floridi, L. and Van der Sloot, B. (2017). eds. *Group Privacy: New Challenges of Data Technologies*. Cham: Springer.

Taylor, R.D. (2020). Data localization: The Internet in the balance. *Telecommunications Policy*, *44*(8), p.102003. https://doi.org/10.1016/j.telpol.2020.102003

TEHDAS. (2021). *Presentation of a First Set of Data Altruism Definitions, Use Cases and Findings*. [Online]. https://tehdas.eu/app/uploads/2021/09/tehdas-presentation-of-a-first-set-of-data-altruism-definitions-use-cases-and-findings.pdf

ten Seldam, B. & Brenninkmeijer, A. (2021) *The Dutch Childcare Benefits Scandal: A Cautionary Tale of Algorithmic Governance and Discrimination*. EU Law Enforcement. [Online] https://eulawenforcement.com/?p=7941

Terzis, P. and Santamaria Echeverria, O.E. (2023). Interoperability and governance in the European Health Data Space regulation. *Medical Law International*, *23*(4), 368-376. https://doi.org/10.1177/09685332231165692

Tietoevry. (2023). *Digital Sovereignty. Adapting to a challenging digital landscape.* https://www.tietoevry.com/siteassets/files/tech-services/tech-services-digital-sovereignty-whitepaper-v1-2023.pdf

Transform Health. (2022). *Statement ahead of the 75th World Health Assembly.* [Online]. https://transformhealthcoalition.org/transform-health-world-health-assembly-statement/

Turkel, E., & Turkel, G. (2016). Public value theory: Reconciling public interests, administrative autonomy and efficiency. *Rev Public Adm Manag*, *4*(2). http://dx.doi.org/10.4172/2315-7844.1000189

UHC 2030. (Undated). *Taking action for universal health coverage*. The UN High-Level Meeting on UHC 2023 [Online]. https://www.uhc2030.org/un-hlm-2023/

UN General Assembly. (2007). *United Nations Declaration on the Rights of Indigenous Peoples : resolution / adopted by the General Assembly*, A/RES/61/295. https://www.refworld.org/legal/resolution/unga/2007/en/49353

United Nations. (Undated). *Office of the Secretary-General's Envoy on Technology*. Global Digital Compact [Online]. https://www.un.org/techenvoy/global-digital-compact

Universität Bern. (2021). *Security implications of digitalization*. Report for the Federal Department of Foreign Affairs. https://boris.unibe.ch/157323/1/Security_implications_of_digitalization.pdf

University of Sydney. (2023). *Unraveling Robodebt: Legal Failures, Impact on Vulnerable Communities and Future Reforms.* [Online] https://www.sydney.edu.au/law/news-and-events/news/2023/12/13/unraveling-robodebt-legal-failures-impacts.html

U.S. Department of State. (2024). *Building Digital Solidarity: The United States International Cyberspace & Digital Policy Strategy.* [Online] https://www.state.gov/building-digital-solidarity-the-united-states-international-cyberspace-and-digital-policy-strategy/

van Dijck, J. (2014). Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology. *Surveillance & Society 12*(2), 197– 208. https://doi.org/10.24908/ss.v12i2.4776

van Kessel, R., Wong, B. L. H., Clemens, T., & Brand, H. (2022). Digital health literacy as a super determinant of health: More than simply the sum of its parts. *Internet interventions*, *27*, 100500. https://doi.org/10.1016/j.invent.2022.100500

van Till, S. A. L., Smids, J., & Bunnik, E. M. (2023). Access to effective but expensive treatments: An analysis of the solidarity argument in discussions on funding of medical treatments. *Bioethics*, *37*, 111–119. https://doi.org/10.1111/bioe.13108

Verhulst, S. G. (2023). Operationalizing digital self-determination. *Data & Policy*, *5*, e14. https://doi.org/10.1017/dap.2023.11

Viberg Johansson, J., Bentzen, H.B. & Mascalzoni, D. (2022). What ethical approaches are used by scientists when sharing health data? An interview study. *BMC Med Ethics*, *23*, 41. https://doi.org/10.1186/s12910-022-00779-8

Walker, K. (Undated). *From a Splintering Net to Digital Solidarity*. Foreign Policy [Online] https://sponsored.foreignpolicy.com/google/from-a-splintering-net-to-digital-solidarity/

Werther, H., Lee, E. A., Akkermans, H., et al. (2019). *Vienna Manifesto on Digital Humanism*. [Online] https://dighum.ec.tuwien.ac.at/dighum-manifesto/

Werthner, H., Prem, E., Lee, E. A., Ghezzi, C., eds. (2022). *Perspectives on Digital Humanism*. Cham: Springer International Publishing. https://library.oapen.org/handle/20.500.12657/51945

Wilkinson, M.D., Dumontier, M., Aalbersberg, I.J., et al. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific data*, *3*(1), 1-9. https://doi.org/10.1038/sdata.2016.18

Wójcik M. A. (2022). Algorithmic Discrimination in Health Care: An EU Law Perspective. *Health and human rights*, *24*(1), 93–103. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9212826/

Woods, A. K. (2018). Litigating Data Sovereignty. *Yale Law Journal*, *128*. https://ssrn.com/abstract=3256422

World Health Organization. (2021). *Global strategy on digital health 2020-2025*. Geneva: World Health Organization. https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf

World Health Organization. (2020). *Data Principles.* [Online] https://data.who.int/about/data/who-data-principles.

World Health Organization Regional Office for Europe. (2023). *Digital Health in the WHO European Region: the ongoing journey to commitment and transformation.* https://www.who.int/andorra/publications/m/item/digital-health-in-the-who-european-region-the-ongoing-journey-to-commitment-and-transformation

Young, I.M. (1990). *Justice and the Politics of Difference*. Princeton, NJ: Princeton University Press.

Zhu, J., & Marjanovic, O. (2022). *A Taxonomy of Data Cooperatives*. In: PACIS 2022 Proceedings. 257. https://aisel.aisnet.org/pacis2022/257

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* Profile Books. https://profilebooks.com/work/the-age-of-surveillance-capitalism/

Digital Transformations for Health Lab (DTH-Lab)
Hosted by: The University of Geneva
Campus Biotech, Chemin des Mines 9
1202 Geneva, Switzerland
Email: team@dthlab.org

www.DTHLab.org