

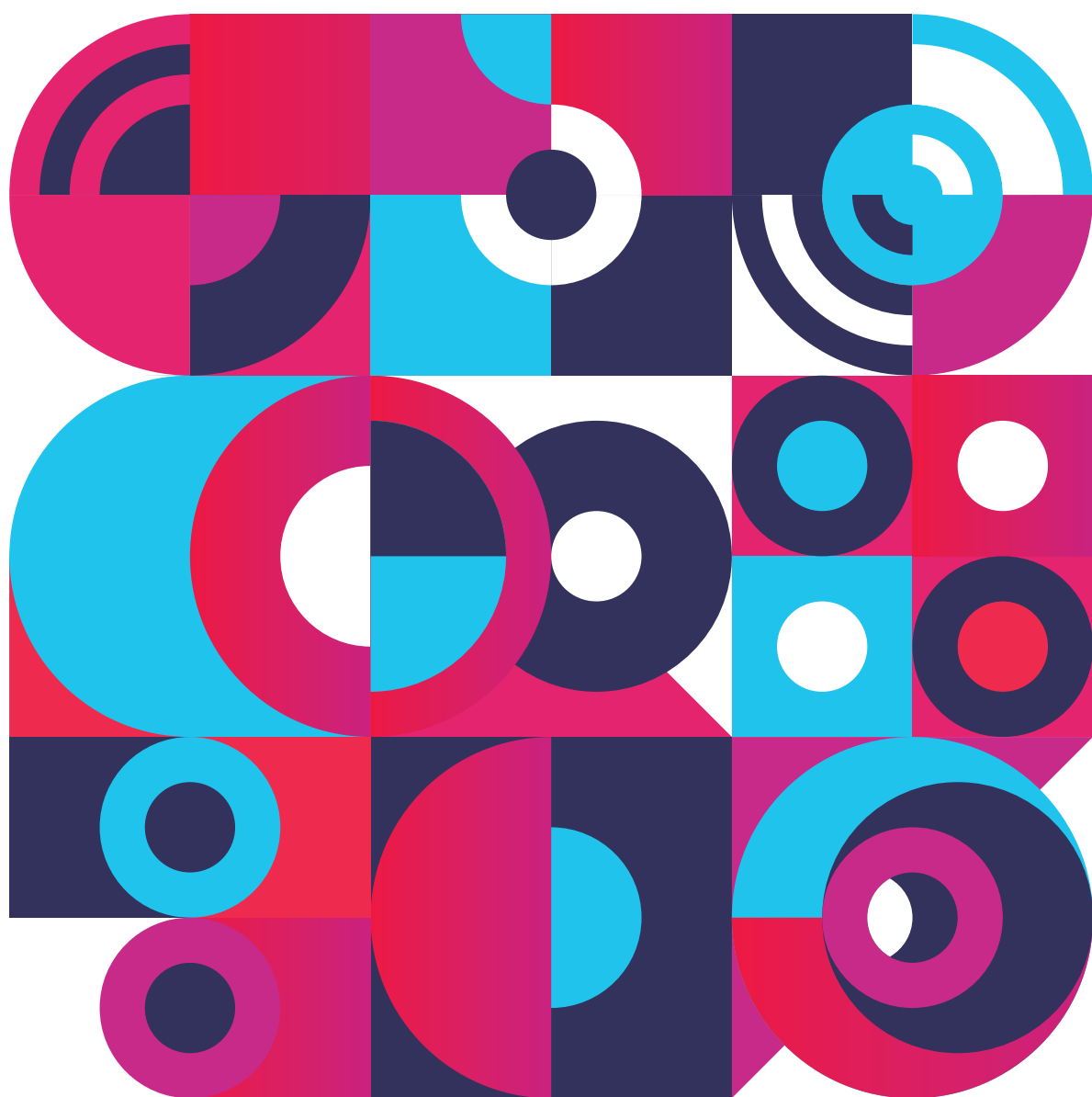


universität
wien



DIGITAL
TRANSFORMATIONS
FOR HEALTH LAB

GOVERNING HEALTH FUTURES 2030



Lexicon Datasolidariteit 2024

Dutch translation



universität
wien



DIGITAL
TRANSFORMATIONS
FOR HEALTH LAB

GOVERNING HEALTH FUTURES 2030

Lexicon Datasolidariteit 2024 Dutch translation

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.

Dutch translation: **Daniel Kapitan & Egge van der Poel** on behalf of Zorginstituut Nederland

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



Inhoud

Over dit lexicon	3
Deel 1: Solidariteit	4
1.1 Solidariteit	4
1.2 Datasolidariteit	7
1.3 Digitale solidariteit	9
1.4 Digitale rechtvaardigheid	10
1.5 Data rechtvaardigheid	11
1.6 Publieke waarde	13
Deel 2: Data governance	15
2.1 Data	15
2.2 Data governance	16
2.3 Data rentmeesterschap	18
2.4 Databeveiliging en data privacy	19
2.5 Digitale soevereiniteit	20
2.6 Data soevereiniteit	21
2.7 Inheemse data soevereiniteit	22
2.8 Data lokalisatie	24
2.9 Schadebeperking	25
Deel 3: Delen van data	27
3.1 Digitale commons en data commons	27
3.2 Data coöperaties	29
3.3 Data trusts	30
3.4 Data delen	31
3.5 Data altruïsme	32

3.6 Data donatie.....	33
3.7 Open data / Open science.....	34
3.8 European Health Data Space (EHDS).....	35
Section 4: Ethiek en macht.....	36
4.1 Digital and data ethics.....	36
4.2 Digitaal humanisme.....	38
4.3 Data discriminatie.....	39
4.4 Data extractie.....	40
4.5 Data kolonialisme.....	41
Section 5: Vooruit kijken.....	42
5.1 Digitale transformatie van de zorg.....	42
5.2 Vertrouwen in data en platformen.....	44
5.3 Dataficering van zorg.....	45
5.4 Digitale gezondheidsvaardigheden.....	46
5.5 Digitale gezondheidsburgerschap.....	47
Bibliografie.....	49



Over dit lexicon

Dit lexicon is een vertaling van het Engelstalige Data Solidarity Glossary 2024 dat is opgesteld door Barbara Prainsack en Ilona Kickbusch. Het originele document is op 23 september 2024 verschenen en online beschikbaar op <https://dthlab.org/data-solidarity-glossary/>.

Deze vertaling is gemaakt in opdracht van het Zorginstituut Nederland, in het kader van het project Datalogica. Een eerste ruwe vertaling, gemaakt met behulp van deepl.com, is bewerkt door Egge van der Poel en Daniel Kapitan. De vertalers hebben bij het redigeren

zich vooral gericht op het toegankelijk maken van het originele document voor een zo groot mogelijk publiek. Er is zo veel mogelijk gezocht naar Nederlandse woorden, ter vervanging van het Engelse vakjargon. In het geval dat er geen passend Nederlands woord gevonden kon worden, is de Engelse term gehandhaafd (bijvoorbeeld 'governance' en 'data trust').

De Nederlandstalige vertaling is door Barbara Prainsack nagelezen, waarvoor de vertalers haar zeer erkentelijk zijn.



Deel 1: Solidariteit

1.1 Solidariteit

Solidariteit is een cruciaal element voor het opbouwen van eerlijkere samenlevingen, waarin alle mensen toegang hebben tot dezelfde mogelijkheden om gezondheid, welzijn en andere goederen te bereiken.

Solidariteit heeft vele betekenissen. Om solidariteit beter te begrijpen, nemen wij in dit lexicon de definitie van Barbara Prainsack en Alena Buyx als uitgangspunt. Zij definiëren solidariteit als een handelwijze die de toewijding weerspiegelt

van mensen om anderen te ondersteunen met wie zij in een relevant opzicht overeenkomsten herkennen. De overeenkomsten tussen de leden van deze “gedeelde belangen gemeenschappen” zijn niet noodzakelijk objectief meetbare kenmerken. Ze kunnen een gemeenschappelijk doel, een gezamenlijke strijd tegen onderdrukking of een deel van de sociale of politieke identiteit zijn. In principe is geen van deze kenmerken of overeenkomsten belangrijker dan andere: Wat mensen met anderen verbindt is afhankelijk van de specifieke situatie of praktijk

Tabel 1: Niveaus van solidariteit

	Interpersoonlijke solidariteit	Solidariteit tussen individuele personen
	Groepssolidariteit	Solidariteit binnen belangengroepen
	Geïstitutionaliseerde solidariteit	Wettelijke, administratieve en/of bureaucratische normen die principes van solidariteit definiëren en implementeren. Formele instituties

in kwestie. Solidariteit wordt vaak beschreven als een sociale waarde, waarbij veranderende normen leiden tot het ontstaan van nieuwe solidariteiten. Bijvoorbeeld, solidariteit tussen generaties in relatie tot klimaatactie of solidariteit op basis van geslacht. Maar solidariteit op het ene gebied hoeft niet noodzakelijkerwijs door te werken op het andere: een persoon van hetzelfde geslacht kan een andere persoon steunen wanneer deze het doelwit wordt van intimidatie op grond van geslacht, maar dezelfde persoon kan niet solidair handelen met de ander in een context waarin hun politieke waarden of handelingen hen van elkaar onderscheiden. Met andere woorden, solidariteit vindt plaats wanneer mensen handelen naar dingen die ze als gemeenschappelijk beschouwen met anderen - als een gemeenschap van belangen - in plaats van te handelen op basis van hun verschillen.

Hoewel solidariteit geen vervanging is voor rechtvaardigheid, kan het helpen om onrechtvaardigheden tegen te gaan en mensen te verenigen achter gedeelde doelen. In die zin kan solidariteit een mechanisme

zijn om het algemeen welzijn te bevorderen, niet alleen binnen maar ook tussen landen.

Prainsack en Buyx onderscheiden ook drie niveaus van solidariteit (zie [Tabel 1: Niveaus van solidariteit](#)). Niveau 1 is het niveau van interpersoonlijke solidariteit: deze vindt plaats wanneer individuele mensen solidariteit betonen met anderen met wie ze zich op een relevante manier verbonden achten. Niveau 2 is het niveau van groepssolidariteit: het vindt plaats wanneer solidariteit 'normaal' gedrag wordt in een groep. Niveau 3 is het niveau van geïstitutionaliseerde solidariteit: Dit vindt plaats wanneer wettelijke, bureaucratische, administratieve of sociale normen een solidaristische geest weerspiegelen. Het omvat ook formele solidaristische instellingen. Solidaristische instellingen zijn instellingen waaraan mensen bijdragen naar vermogen en waarvan ze steun ontvangen op basis van hun behoefte.

Het schoolvoorbeeld van geïstitutionaliseerde solidariteit is universele gezondheidszorg (Engels: Universal Health Coverage of UHC). Dit betekent dat alle mensen toegang

hebben tot het volledige aanbod van kwaliteitsvolle gezondheidsdiensten die ze nodig hebben, waar en wanneer ze die nodig hebben, zonder nadelige financiële consequenties. Dergelijke solidariteit berust op financiële solidariteit via het poolen van risico's. Met betrekking tot gezondheid zijn er ook andere vormen van solidariteit: solidair gedrag (doneren van organen, afzien van niet-urgente ingrepen als anderen ze dringender nodig hebben), solidariteit in termen van het delen van data en solidariteit in zorgen voor jezelf (om op een verantwoorde manier met je gezondheid om te gaan).

Zo opgevat kan solidariteit een leidraad zijn voor de ontwikkeling van beleid en de

opbouw van instellingen op verschillende terreinen van beleid en praktijk. Het is onder andere ook gebruikt om een nieuwe benadering van data governance te ontwikkelen (zie [1.2 Datasolidariteit](#)). Solidariteit wordt ook beschouwd als een sleutelprincipe van internationale samenwerking op het gebied van gezondheid, zoals tot uitdrukking komt in de politieke resolutie van de bijeenkomst op hoog niveau over UHC bij de Verenigde Naties in 2023.

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



1.2 Datasolidariteit

Datasolidariteit is een benadering die streeft naar een eerlijker verdeling van de voordelen en risico's die voortkomen uit digitale gebruiken. Bovendien moeten niet alleen individuele mensen, maar ook gemeenschappen en andere collectieven in staat zijn om zinvolle controle uit te oefenen over hoe data worden gebruikt, door wie en ten voordele van wie.

De huidige kaders voor het beheer van gezondheidsdata zijn ontworpen om de primaire betrokkenen te beschermen - dat wil zeggen de mensen van wie de data afkomstig zijn - en in het bijzonder gevoelige informatie zoals hun persoonlijke medische data. In digitale samenlevingen kunnen de risico's en voordelen van digitale toepassingen - variërend van het creëren van data tot secundair gebruik - van invloed zijn op een veel breder scala aan mensen en veel meer datapunten uit het dagelijks leven en gedrag omvatten. Data van de ene groep kunnen worden gebruikt om een andere groep te bevoordelen of te discrimineren. Daarom is het niet voldoende om de mensen te beschermen van wie de data afkomstig zijn. Bovendien gaat digitalisering gepaard met grote machtsongelijkheid, zowel binnen als tussen landen. Om deze uitdagingen en ongelijkheden aan te pakken is een aanpak nodig die verder gaat dan alleen mensen meer controle geven over hun eigen data - net zoals we in de volksgezondheid begrijpen dat individuele gezondheidsrechten moeten worden aangevuld met maatregelen op het gebied van de volksgezondheid.

Datasolidariteit bestaat uit drie pijlers (zie [Tabel 2: De drie pijlers van datasolidariteit](#)). Pijler I richt zich op het vergemakkelijken van het gebruik van data wanneer dit grote voordelen belooft op te leveren voor mensen zonder dat dit significante risico's met zich meebrengt voor individuele mensen of gemeenschappen. Dit kan worden gedaan door de regelgeving te versoepelen of door overheidsfinanciering te verstrekken. Pijler II is gericht op het voorkomen van schade, bijvoorbeeld door het effectief verbieden van datagebruik dat grote risico's met zich meebrengt. Omdat niet alle schade effectief kan worden voorkomen, is het ook nodig om de schade te beperken. Het is belangrijk dat alle mensen die schade hebben ondervonden als gevolg van datagebruik worden ondersteund. Op dit moment is dit vaak niet het geval, bijvoorbeeld wanneer mensen geen toegang hebben tot rechtsmiddelen omdat geen wet werd overtreden of omdat ze niet kunnen vaststellen wie verantwoordelijk is voor de schade (dit laatste wordt steeds moeilijker om te herkennen wanneer data meerdere keren worden gedeeld in verschillende instellingen).

Pijler III schrijft voor dat commerciële winsten uit het gebruik van data gedeeld moeten worden met de mensen en gemeenschappen die het gebruik van data in eerste instantie mogelijk hebben gemaakt, bijvoorbeeld via hun acties als patiënten, burgers en via de openbare infrastructuur die commerciële entiteiten gebruiken. Commerciële winsten kunnen worden gedeeld via belastingen of verschillende andere vormen van winstdeling (bijvoorbeeld benefit sharing overeenkomsten met lokale gemeenschappen).

Datasolidariteit vereist twee belangrijke verschuivingen in ons denken en handelen ten opzichte van de status quo.

Ten eerste is de aanname in bestaande kaders voor data governance vaak dat de heridentificatie van individuen het belangrijkste risico is dat voortvloeit uit het gebruik van data en dat sommige soorten data ‘risicovoller’ zijn om te gebruiken dan andere. Datasolidariteit daarentegen gaat ervan uit dat de risico’s liggen in het gebruik van data in plaats van in de traditionele aanpak die zich richt op het soort data. In gevallen van data-analyse waarbij verschillende soorten data worden gekoppeld, kan zelfs de meest onschuldige dataset leiden tot inzichten die mensen kunnen schaden wanneer ze worden gekoppeld aan andere datasets. Datasolidariteit vereist dat soorten datagebruik die weinig risico’s voor individuen en gemeenschappen met zich meebrengen en waarschijnlijk aanzienlijke voordelen opleveren, anders worden behandeld dan datagebruik dat het tegenovergestelde doet (zie ook [1.6 Publieke waarde](#) en [Kader: Het instrument voor de beoordeling van de publieke waarde \(PLUTO\)](#)).

Ten tweede, naast het feit dat individuen rechten en plichten hebben met betrekking tot hun persoonlijke gezondheid, maakt datasolidariteit gebruik van collectieve controle- en toezicht instrumenten, waaronder data commons, sterker gebruik van bindend recht om datagebruik met een hoge publieke waarde te ondersteunen en schadelijk datagebruik te verbieden en nog veel meer. In haar rapport, aangevuld met een whitepaper over datasolidariteit, schetsen The Lancet and Financial Times in ‘Governing health futures 2030: Growing up in a digital world’ waarom solidariteit een van de kernprincipes moet zijn waarop elke benadering van het beheer van gezondheidsdata is gebaseerd. Een op solidariteit gebaseerde benadering van gezondheidsdata moet worden beschouwd als een bepalend kenmerk van de 21e-eeuwse volksgezondheid op nationaal en mondiaal niveau, afgestemd op rechtvaardigheid als kernwaarde van de volksgezondheid.

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

Tabel 2: De drie pijlers van datasolidariteit

Pijler I	Pijler II	Pijler III
Het vergemakkelijken van datagebruik dat aanzienlijke publieke waarde creëert	Voorkomen en beperken van schade	Delen van commerciële voordelen met gemeenschappen
Bijv. via deregulering, overheidssteun voor hergebruik van data	Bijv. door het verbieden van datagebruik waarvan bekend is dat het schadelijk is voor individuen of gemeenschappen en door het opzetten van instanties die schade beperken	Bijv. via belastingen of overeenkomsten voor het delen van opbrengsten

1.3 Digitale solidariteit

Digitale solidariteit verwijst naar het gebruik of de capaciteit van digitale technologieën en online platforms om samenwerking te vergemakkelijken, zowel tussen landen als tussen gemeenschappen, vooral in tijden van crisis of nood.

Digitale solidariteit beschrijft strategie die de samenwerking tussen landen verbetert om samen te werken aan gezamenlijke doelen met betrekking tot het gebruik van digitale technologieën, vooral in tijden van crisis. Recentelijk - deels gebaseerd op de ervaringen tijdens de COVID-19 pandemie - is digitale solidariteit voorgesteld als alternatief voor het concept van digitale soevereiniteit (zie [2.5 Digitale soevereiniteit](#)). Er is ook een toenemende bezorgdheid over inspanningen die bijdragen tot de uitholling van een gedeeld digitaal ecosysteem, wat leidt tot een internet model dat minder open, minder veilig en minder economisch voordelig is voor iedereen.

In plaats van over te stappen op gesloten technologische ecosystemen, wordt voorgesteld dat beleidsmakers zich bewegen in de richting van digitale solidariteit over de grenzen heen, als een kader voor het verbeteren van economische vooruitgang, nationale veiligheid en andere maatschappelijke belangen in open, democratische en aan regels gebonden samenlevingen. De Europese Unie heeft bijvoorbeeld opgeroepen tot “EU digitale solidariteit: een pan-Europese aanpak tegen de pandemie”. Ook het voorgestelde Global Digital Compact van de Verenigde Naties beoogt “gedeelde beginselen voor een open, vrije en veilige digitale toekomst voor iedereen” en het verbeteren van digitale

samenwerking als een belangrijk kenmerk van multilaterale samenwerking. Er gaan steeds meer stemmen op om het gebruik van data over de grenzen heen wereldwijd te reguleren.

Gebruiken zoals online fondsenwerving campagnes, bewegingen in de sociale media, gezamenlijke probleemoplossing via digitale platforms of het gebruik van technologie om sociale problemen aan te pakken en te pleiten voor rechtvaardigheid en inclusie worden ook wel een uitdrukking van digitale solidariteit genoemd. Dit gebruik van het concept benadrukt het vermogen van technologie om een gemeenschapsgevoel op te bouwen en uitdagingen in het digitale tijdperk collectief aan te pakken. Het gaat om het gebruik van digitale hulpmiddelen en middelen om economische, sociale en politieke asymmetrieën te overwinnen; en om het bijstaan van mensen die beperkte toegang hebben tot technologie of geconfronteerd worden met verschillende vormen van digitale uitsluiting. Het concept van digitale solidariteit wordt soms ook gebruikt om een beroep te doen op de bereidheid om data te delen of toegang te verlenen tot iemands data, vergemakkelijkt door digitale technologieën, om bepaalde wenselijke doelen te bereiken, zoals het ondersteunen van zorgonderzoek en het verbeteren van de paraatheid voor pandemieën. Digitale solidariteit kan worden beschouwd als een component van digitaal burgerschap dat verschuift van individuele agency naar de collectieve kracht van losjes georganiseerde digitale netwerken die zich vaak manifesteren over fysieke grenzen heen.

Referenties: 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 Digitale rechtvaardigheid

Digitale rechtvaardigheid heeft veel gemeen met data rechtvaardigheid, maar omvat een breder spectrum. Het omvat niet alleen data, maar ook de toegang tot en het gebruik van digitale technologieën. Het verwijst naar het streven naar gelijkheid en rechtvaardigheid in het digitale tijdperk, waarbij systemische ongelijkheden met betrekking tot de toegang tot digitale technologieën, digitale geletterdheid en de rechten en vrijheden in verband met digitale omgevingen worden aangepakt. Digitale rechtvaardigheid moet ervoor zorgen dat alle mensen, ongeacht hun sociaaleconomische status, etniciteit, geslacht of locatie, de kans krijgen om volledig en gelijkwaardig deel te nemen aan de digitale samenleving.

Net als klimaatrechtvaardigheid, waarbij gekeken wordt naar gelijkheid, mensenrechten, collectieve rechten en historische verantwoordelijkheden voor klimaatverandering, houdt digitale rechtvaardigheid zich bezig met zowel procedurele als distributieve ethische dimensies. Het benadrukt het belang van de aanpak van individuele en collectieve rechten, waarbij ervoor wordt gezorgd dat technologische vooruitgang bestaande ongelijkheden niet verergert of nieuwe vormen van onrecht creëert.

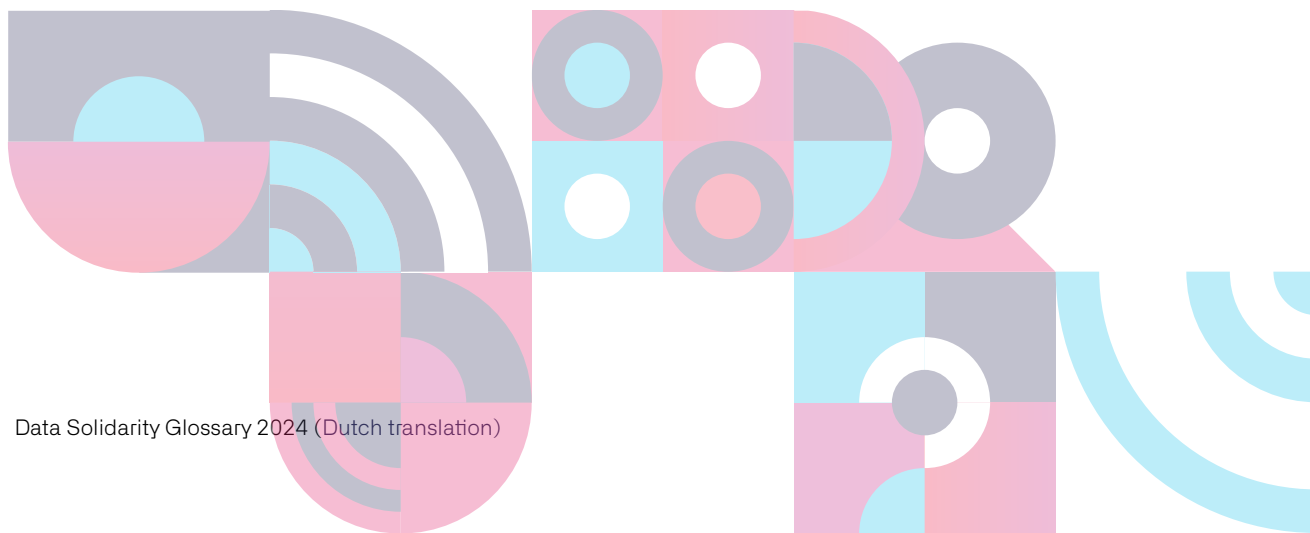
Een essentieel aspect van digitale rechtvaardigheid is het rechtzetten van datagestuurde schade die is toegebracht aan individuen of groepen. Er is sprake van onrecht wanneer de omvang van

de schade wordt ondergewaardeerd of onopgemerkt, wanneer er geen verantwoording wordt afgelegd of wanneer er geen effectieve manieren zijn om schade te herstellen. Digitale gerechtigheid probeert deze problemen aan te pakken door zich te richten op preventie, het met terugwerkende kracht identificeren van schade, het toewijzen van verantwoordelijkheid en het identificeren van rechtvaardige routes voor schadeloosstelling. In dit opzicht deelt het belangrijke doelstellingen met datasolidariteit (Zie [2.9 Schadebeperking](#)).

Het concept van digitale rechtvaardigheid houdt ook in dat alle stemmen worden gehoord en dat gemarginaliseerde groepen niet achterblijven bij de digitale transformatie. Dit omvat het pleiten voor beleid dat digitale geletterdheid en toegankelijkheid bevordert, zodat mensen beter kunnen navigeren door digitale technologieën en er optimaal van kunnen profiteren.

Samengevat gaat digitale rechtvaardigheid over het creëren van eerlijke en rechtvaardige digitale samenlevingen. Het omvat de preventie van digitale schade, het identificeren en herstellen van onrechtvaardigheden uit het verleden en het bevorderen van inclusieve digitale gebruiken die individuele en collectieve rechten respecteren en hoog houden..

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



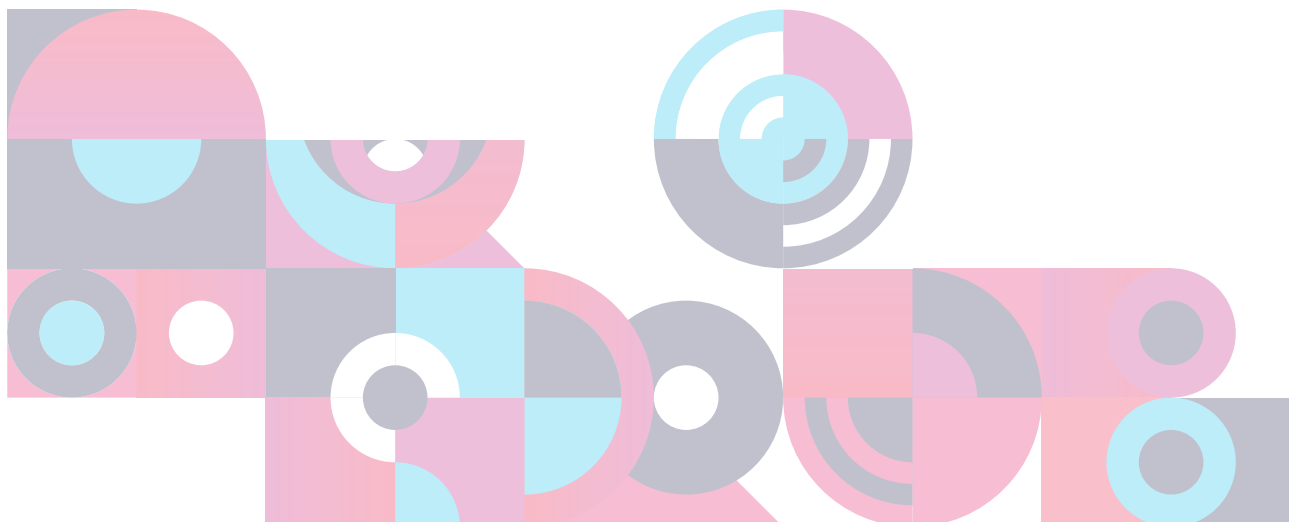
1.5 Data rechtvaardigheid

Data rechtvaardigheid verwijst naar het idee dat vormen van data creatie en datagebruik onze samenlevingen rechtvaardiger moeten maken en niet mogen bijdragen aan meer onrechtvaardigheid. Meer specifiek is data rechtvaardigheid gedefinieerd als een concept voor nationale en supranationale wetgevende processen die rechtvaardigheid garanderen in de manier waarop mensen zichtbaar worden gemaakt, worden vertegenwoordigd en worden behandeld als producenten van data. Dit omvat eerlijkheid in de manier waarop mensen worden onderworpen aan op data gebaseerde besluitvorming. Volgens deze grondgedachte moet een rechtskader dat data rechtvaardigheid afdwingt, drie centrale doelen bereiken: Ten eerste moet het het individu de rechtsbevoegdheid geven om op de hoogte te zijn van het verzamelen en gebruiken van hun persoonlijke data. Ten tweede moet het mensen in staat stellen hun persoonlijke data te beschermen tegen geautomatiseerde commodificering op de wereldwijde datamarkten en tegelijkertijd ook het gebruik van data voor het algemeen belang aanmoedigen. Ten derde moet het technische situaties tegengaan die kunnen leiden tot opzettelijke of onbedoelde discriminatie. Een voorbeeld van deze laatste is de toepassing van algoritmen ter

ondersteuning van de besluitvorming door overheidsinstanties of privébedrijven.

Andere auteurs hebben gepleit voor een structureel data rechtvaardigheidsperspectief. Structurele rechtvaardigheid zorgt ervoor dat maatschappelijke systemen en instellingen eerlijk zijn, gelijke kansen bieden en ongelijkheden aanpakken om alle individuen, vooral gemarginaliseerde groepen, mondiger te maken. Een perspectief van structurele rechtvaardigheid besteedt ook kritisch aandacht aan de machtsverhoudingen waarin data governance is ingebed. Zij zien data rechtvaardigheid als het resultaat van structurele omstandigheden die vorm geven aan bredere maatschappelijke relaties waarvan het extraheren en verwerken van data een onderdeel is geworden. Deze benadering houdt zich vooral bezig met de manier waarop de toegang tot bepaalde soorten data verdeeld is tussen het Globale Noorden en Zuiden.

Datasolidariteit en data rechtvaardigheid vullen elkaar aan. Matthias Braun en Patrik Hummel stellen dat datasolidariteit een noodzakelijk, katalyserend element is voor data rechtvaardigheid. Zij stellen dat wanneer onrechtvaardigheden op het gebied van datagestuurde gebruiken zich voordoen en ertoe leiden dat individuen

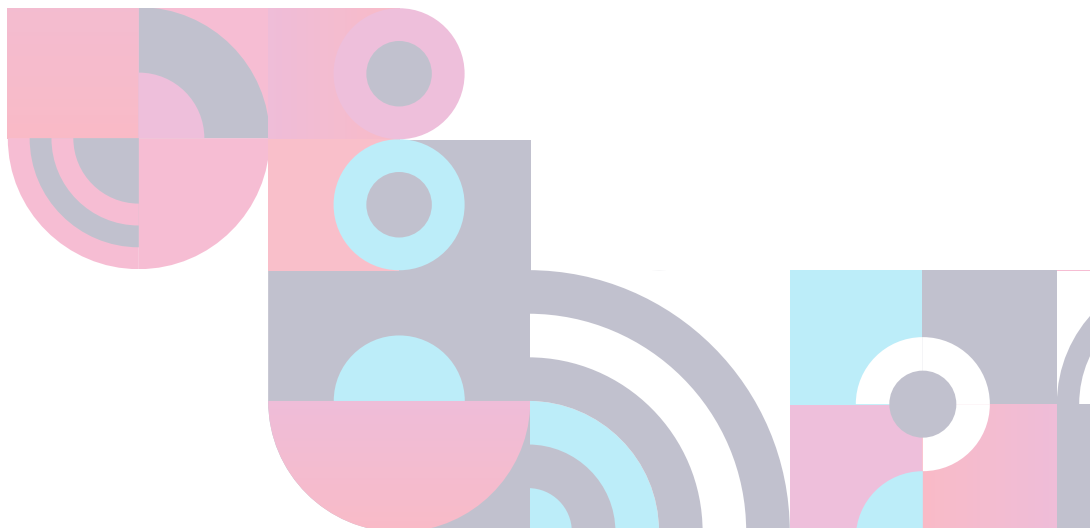


of groepen gediscrimineerd of gemarginaliseerd zijn, er behoefte is aan gedeelde praktijken van solidariteit om deze onrechtvaardigheden aan te pakken - en aan instellingen die deze gedeelde praktijken weerspiegelen en ondersteunen. In die zin hangt data rechtvaardigheid af van een gedeelde praktijk de stemmen van anderen te horen (in het bijzonder van degenen die gemarginaliseerd zijn) en hun zorgen te behandelen als collectieve problemen. Met andere woorden, het is noodzakelijk dat mensen zich bezighouden met gezamenlijke praktijken van aandacht en actie op basis van de zorgen van anderen, om zo duurzame, praktische regelingen voor data rechtvaardigheid te realiseren.

Bovendien kan datasolidariteit een belangrijke rol spelen bij het identificeren van onrechtvaardigheid.

Vaak worden mensen zich er pas van bewust dat hen onrecht is aangedaan, wanneer ze hun ervaring vergelijken met die van anderen. Op dezelfde manier kunnen waarnemers worden geattendeerd op mogelijke onrechtvaardigheden die worden ervaren door bepaalde individuen of groepen op basis van de vorming van solidariteitsbewegingen. Het is dus belangrijk dat solidariteitspraktijken binnen een samenleving erkend worden als ook epistemisch waardevol in het identificeren en aanpakken van onrechtvaardigheid (en dus indirect het versterken van de inhoud van rechtvaardigheid)..

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



1.6 Publieke waarde

Publieke waarde is een sleutelbegrip voor datasolidariteit. Het beschrijft de waarde die een organisatie of activiteit bijdraagt aan de samenleving.

Oorspronkelijk verwees het concept van publieke waarde naar het equivalent van aandeelhouderswaarde in publiek management. Meer in het algemeen kan publieke waarde worden opgevat als “een manier om vooruitgang te meten in de richting van het bereiken van brede en algemeen aanvaarde maatschappelijke doelen”, zoals de overgang naar een duurzame mondiale ecologie, de vermindering van ongelijkheid en de bevordering van een goede gezondheid. Een dergelijke ‘missiegerichte’ benadering van publieke waarde sluit in het bijzonder aan bij de roep om digitale gezondheid te laten aansturen door een publiek doel en niet door winst, op basis van volksgezondheid principes.

Binnen de datasolidariteit benadering wordt een datagebruik gezien als een gebruik met publieke waarde wanneer aannemelijk kan worden gemaakt dat het duidelijke voordelen zal hebben voor veel mensen, voor de samenleving als geheel of voor toekomstige generaties en het

onwaarschijnlijk is dat een enkele persoon of groep aanzienlijke en onevenredige schade zal ondervinden. Bovendien zal de publieke waarde regelmatig meer uitgesproken zijn als het waarschijnlijk is dat de voordelen zich zullen voordoen voor minder bedeelde of gemarginaliseerde groepen, als gevolg van de algehele lagere uitgangssituatie en potentiële omvang van de impact.

Om een gestructureerde beoordeling van de publieke waarde van specifieke gevallen van datagebruik te ondersteunen, is een online tool gratis beschikbaar (zie [Kader: Het instrument voor de beoordeling van de publieke waarde \(PLUTO\)-tool](#)). Deze tool kan de besluitvorming ondersteunen van individuen die worden gevraagd om toegang te verlenen tot hun data en kan ook de besluitvorming ondersteunen van andere organisaties, overheidsinstanties en commissies voor datatoegang.

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.



Kader: Het instrument voor de beoordeling van de publieke waarde (PLUTO)

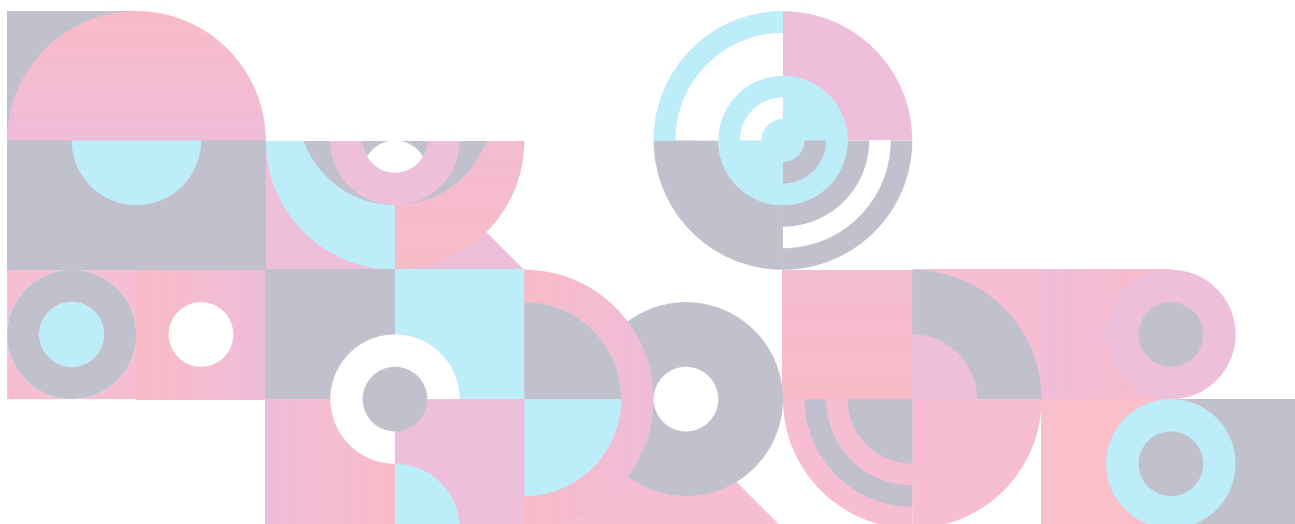
Een team van de Universiteit van Wenen heeft een online tool ontwikkeld om een gestructureerde beoordeling te maken van de publieke waarde van het gebruik van data. De tool kan worden gebruikt door iedereen die wil weten welke publieke waarde een specifiek geval van datagebruik waarschijnlijk zal creëren: bijvoorbeeld bedrijven, organisaties of andere entiteiten die de data gebruiken, of mensen van wie de data worden gebruikt.

De online tool bestaat uit iets meer dan 20 vragen die betrekking hebben op vier gebieden: Informatie over de datagebruiker, voordelen van het datagebruik, risico's van het datagebruik en institutionele waarborgen. In het algemeen geldt: hoe meer een specifiek geval van datagebruik mensen en gemeenschappen ten goede komt zonder individuen of groepen in gevaar te brengen, hoe hoger de publieke waarde. Voordelen en nadelen die zich waarschijnlijk zullen voordoen voor onderbedeelde of anderszins gemarginaliseerde groepen worden zwaarder gewogen dan voordelen en nadelen voor bevoorrechte groepen. Gedetailleerde informatie over de verschillende gewichten

die aan de antwoorden zijn toegekend, zijn online beschikbaar als bijlage bij de online tool en kunnen door iedereen met internettoegang worden ingezien (<https://pluto.univie.ac.at/>).

De PLUTO-tool is bedoeld om mensen en organisaties te helpen op een gestructureerde manier na te denken over de publieke waarde van het gebruik van data. Het pretendeert niet een precieze en definitieve score te geven en mag niet worden gebruikt als enige basis voor een beslissing. Publieke waarde, als concept, is niet statisch; het evolueert in reactie op maatschappelijke veranderingen, technologische vooruitgang en verschuivende waarden. Daarom kan het nodig zijn dat PLUTO haar criteria en definities in de loop van de tijd aanpast om relevant te blijven. Deze voortdurende evolutie betekent ook dat verschillende belanghebbenden publieke waarde verschillend kunnen interpreteren, wat leidt tot voortdurende discussies over de effectiviteit en nauwkeurigheid van het instrument.

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





Deel 2: Data governance

2.1 Data

In de meest algemene zin zijn data het meervoud van metingen van waarden die samen natuurlijke of sociale fenomenen vertegenwoordigen. Data kunnen ook worden beschreven als metingen of waarden die, wanneer ze worden verwerkt, informatie opleveren. De term digitale data verwijst op zijn beurt naar de data die worden opgeslagen of verwerkt met digitale middelen.

We zien de wereld steeds meer door data. Steeds grotere delen van ons lichaam, gedrag en onze omgeving die vroeger niet gemeten en niet geteld werden, worden vastgelegd in de vorm van (digitale) data. Tegelijkertijd worden data een hoeksteen van onze samenlevingen. Ze ondersteunen – of stimuleren zelfs – innovatie, efficiëntie en besluitvorming in verschillende sectoren.

Van gezondheidszorg en onderwijs tot financiën en entertainment, het verzamelen en analyseren van data maakt gepersonaliseerde diensten, voorspellende analyses en verbeterde resultaten mogelijk. Naarmate de hoeveelheid gegenereerde data blijft groeien, wordt het belang ervan voor het vormgeven van beleid, het verbeteren van bedrijfsactiviteiten en het bevorderen van technologische vooruitgang steeds belangrijker. In deze context weerspiegelt het begrip 'big data' datasets van ongekend volume, variëteit, snelheid (d.w.z. snelheid van verzamelen en gebruik) en waarde.

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

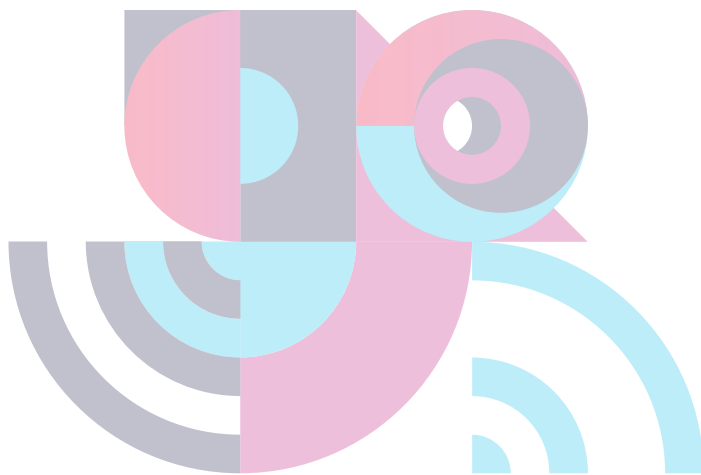
2.2 Data governance

Data governance verwijst naar het algemene beheer van de beschikbaarheid, bruikbaarheid, integriteit en veiligheid van de data die worden verzameld, gebruikt en hergebruikt. Het gaat om het opstellen van beleid, procedures en standaarden om ervoor te zorgen dat data effectief worden beheerd gedurende hun levenscyclus binnen organisaties en binnen en tussen landen.

Veel landen en internationale en regionale organisaties zijn bezig met het definiëren van hun aanpak van data governance. Een prominent voorbeeld is India, dat hoge prioriteit geeft aan data soevereiniteit, bescherming van de privacy, bevordering van digitale innovatie, facilitering van digitale inclusie en ontwikkeling en waarborging van meer veiligheid. Een ander voorbeeld is China, dat de staat relatief gemakkelijk toegang geeft tot persoonlijke data met de governance van digitale platforms in het belang van economische groei en nationale veiligheid. De Europese Unie heeft principes opgesteld voor data governance, waaronder rechtmatigheid,

eerlijkheid en transparantie, integriteit en vertrouwelijkheid, en verantwoordingsplicht. De Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) werkte samen met haar 38 lidstaten – verspreid over de hele wereld, van Noord-Amerika en Zuid-Amerika tot Europa en Azië-Pacific – om de aanbevelingen voor data governance in 2016 te bevorderen. De aanbevelingen hebben betrekking op individuele toegang tot gezondheidsinformatie, het betrekken van belanghebbenden bij het ontwerpen van strategieën voor gezondheidsdata, het gebruik van toestemming of passende alternatieven, het belang van veiligheid en privacy en de optimalisatie van data en technologie in het algemeen belang.

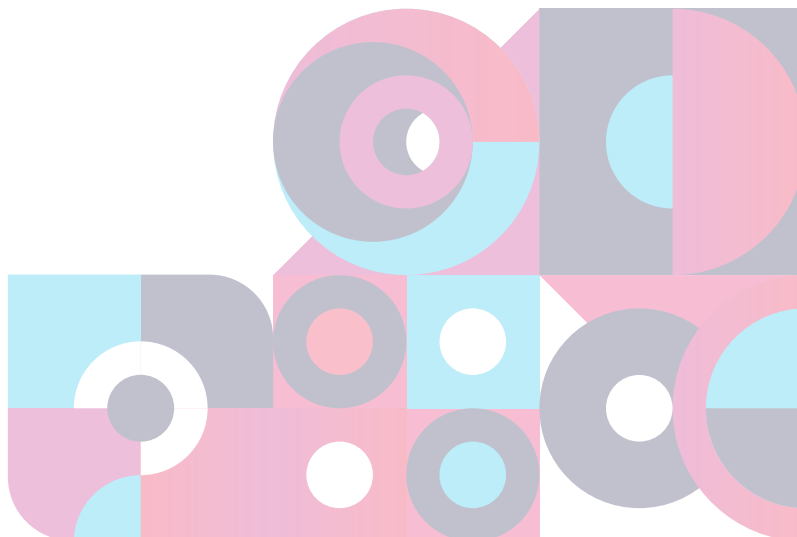
De Wereldgezondheidsorganisatie (WHO) heeft de noodzaak erkend van gemeenschappelijke normen en gecoördineerde benaderingen om te komen tot het potentieel van digitale transformaties voor de gezondheid. In haar wereldwijde strategie voor digitale gezondheid, identificeert de WHO



interoperabiliteit en het beheer van gezondheidsdata als twee van de meest urgente gebieden voor toekomstige internationale overeenkomsten. Honderden organisaties riepen onlangs de WHO en haar lidstaten op om aan de slag te gaan met een wereldwijd kader voor het beheer van gezondheidsdata waarmee de waarde van data kan worden benut voor het algemeen belang waarbij zowel individuele rechten als groepsrechten, zoals die van gemarginaliseerde groepen, worden beschermd. Het beheer van gezondheidsdata moet een prominente plaats krijgen in alle openbare gezondheidsbeleid, of dat nu mondiaal of nationaal, regionaal of lokaal is. Het Pandemieverdrag waarover momenteel wordt onderhandeld is een voorbeeld op mondiaal niveau, de General Data Protection Regulation (GDPR) van de EU en de Artificial Intelligence Act zijn voorbeelden op Europees niveau. Deze laatste zal van toepassing zijn op toepassingen van kunstmatige intelligentie in alle sectoren in EU-landen. De ASEAN-landen pleiten samen met Japan voor een aanpak van “Data Free Flow with Trust”, die een vertrouwd, interoperabel

wereldwijd systeem bevordert om grensoverschrijdende datastromen te vergemakkelijken. De Afrikaanse Unie werkt aan de ontwikkeling van wet- en regelgevings voor data interoperabiliteit tussen de 55 lidstaten, die in juridisch en cultureel opzicht van elkaar verschillen, en pakt de schaarste aan data infrastructuur aan. De commissie van *The Lancet* en *Financial Times* stelde een op waarden gebaseerd bestuursmodel voor, gebaseerd op de kernwaarden gelijkheid, datasolidariteit, digitaal rentmeesterschap, vertrouwen, verantwoording en publieke participatie. Hoewel bovenstaande initiatieven en beleidslijnen naar veel van deze kernwaarden verwijzen, bevatten ze nog geen expliciete verwijzing naar datasolidariteit. Datasolidariteit is een specifieke benadering van data governance die niet alleen de nadruk legt op individuele controle, maar ook op collectieve vormen van toezicht op en eigendom van digitale data en infrastructuren.

Referenties: 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 rentmeesterschap

In het algemeen verwijst rentmeesterschap naar het verantwoordelijke beheer van middelen of activa die aan iemands zorg zijn toevertrouwd en houdt het in dat beslissingen worden genomen die prioriteit geven aan het welzijn op lange termijn en de belangen van belanghebbenden of begunstigten. Het doel van rentmeesterschap is om het behoud en de duurzaamheid van ecosystemen op lange termijn te bevorderen en tegelijkertijd tegemoet te komen aan de behoeften van vandaag op een effectieve en efficiënte manier. Op het gebied van gezondheid moeten data rentmeesters (Engels: data stewards) verantwoordelijk zijn voor het bevorderen van het delen van en de toegang tot gezondheidsdata en er tegelijkertijd voor zorgen dat de data geschikt zijn voor het beoogde doel en op de juiste manier worden gebruikt volgens de regels voor data governance. Ze moeten ook meedenken over beleid en standaarden om de schaal en verspreiding van innovatie, productiviteit en systeem effectiviteit te vereenvoudigen. De belangrijkste verantwoordelijkheden van data rentmeesters zijn onder andere:

- ❓ Zorgen voor naleving van beleid, normen en procedures voor data governance en -beheer;
- ❓ Het definiëren en implementeren van maatregelen en processen om data te beschermen tegen ongeautoriseerde toegang, misbruik of inbreuken;
- ❓ De kwaliteit van de data waarborgen door kwaliteitsborging processen te implementeren;

- ❓ Ervoor zorgen dat data goed in kaart worden gebracht, getransformeerd en geharmoniseerd om bedrijfsfuncties te ondersteunen;
- ❓ Toezicht houden op de volledige data waardeketen, inclusief meting van het ecosysteem van gezondheidsdata en acties ondernemen voor voortdurende verbetering; en
- ❓ Waar nodig zitting nemen in de organen voor data governance.

Data rentmeesters houden toezicht op de praktische toepassing van beleid en standaarden voor data afkomstig van meerdere verschillende entiteiten die data genereren binnen de waardeketen van data, vanaf de identificatie, verzameling, opslag, uitwisseling en het gebruik van data. Rentmeesters zorgen ervoor dat geschikte data op een naadloze manier beschikbaar zijn voor geautoriseerde data-gebruikers om er bruikbare inzichten uit te halen. Dit is te onderscheiden van data bewaarders of trustees, die verantwoordelijk zijn voor de opslag, het beheer en de bescherming van data binnen hun eigen instellingen en organisaties, terwijl ze er ook voor zorgen dat data worden gedeeld in overeenstemming met relevante wet- en regelgeving. Beide rollen zijn essentieel om ervoor te zorgen dat data effectief worden beheerd, beschermd en gebruikt voor het algemeen belang.

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

2.4 Databeveiliging en data privacy

Databeveiliging en data privacy zijn nauw verwante concepten die datasolidariteit aanvullen. Ze richten zich op het beschermen van informatie in de digitale wereld, maar ze behandelen verschillende aspecten van het omgaan met en beveiligen van data.

Databeveiliging omvat de implementatie van maatregelen en protocollen om digitale informatie te beschermen tegen ongeautoriseerde toegang, openbaarmaking, wijziging of vernietiging. Het omvat een breed scala aan praktijken en technologieën die ontworpen zijn om data gedurende de hele levenscyclus te beveiligen. Dit omvat versleuteling, toegangscontroles, firewalls, antivirussoftware en andere beveiligingsmaatregelen gericht op het voorkomen van datalekken en het waarborgen van de integriteit en vertrouwelijkheid van informatie. Databeveiliging is een cruciaal aspect voor bedrijven, organisaties en individuen om gevoelige data te beschermen en het vertrouwen van hun stakeholders te behouden.

Data privacy richt zich specifiek op de controle op het gebruik van persoonlijke informatie - wat meestal wordt opgevat als data die betrekking hebben op een geïdentificeerde of identificeerbare persoon. Het draait om de rechten van mensen om inspraak te hebben in hoe en door wie data over hen worden gebruikt en hoe organisaties persoonlijke data verzamelen, verwerken en gebruiken. Privacy maatregelen omvatten een reeks instrumenten, zoals het verkrijgen van geïnformeerde toestemming voordat data worden verzameld en het naleven van privacyregels en -beleid. Het doel van data

privacy is om mensen het vertrouwen te geven dat op een verantwoorde en ethische manier met hun persoonlijke data wordt omgegaan, waarbij ongeautoriseerde toegang of ongeautoriseerd gebruik die kunnen leiden tot privacyschendingen of misbruik van gevoelige informatie wordt voorkomen. Zowel databeveiliging als data privacy zijn integrale onderdelen van verantwoorde data governance.

De dominante manier om data privacy in liberale economieën te begrijpen is door een individualistische bril, wat betekent dat data privacy voornamelijk wordt gedefinieerd als een individueel recht. Dit individualistische kader wordt in toenemende mate aangevochten door empirische en normatieve gevallen waarin privacy tegelijkertijd een persoonlijk en collectief belang is en bescherming vereist via individuele en collectieve rechten.

Datasolidariteit erkent dat databeveiliging en privacy individuele behoeften en rechten zijn en dat data tegelijkertijd collectieve goederen zijn om de behoeften en rechten van de gemeenschap te ondersteunen. Veelvuldige of zelfs systematische schendingen van individuele privacyrechten veranderen de samenleving en omgekeerd geldt hetzelfde: Mensen kunnen hun individuele rechten alleen zinvol uitoefenen in een samenleving waarin wederzijds respect en solidariteit de boventoon voeren. Bijvoorbeeld, zelfs als individuele mensen een individueel recht op vrijheid van meningsuiting hebben, kan dit niet worden uitgeoefend als er geen sancties zijn voor online intimidatie.

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



2.5 Digitale soevereiniteit

Digitale soevereiniteit verwijst naar de regelgeving en controlemaatregelen die een staat uitoefent over de technologie en digitale diensten binnen zijn jurisdictie. Dit omvat controle over waar data zich bevinden, hoe datastromen worden georganiseerd en wie er toegang tot en controle over heeft.

Terwijl data soevereiniteit (Zie [2.6 Data soevereiniteit](#)) zich specifiek richt op het beleid en de wetten voor de opslag en overdracht van data, strekt digitale soevereiniteit zich uit tot bredere technologische aspecten, waaronder de infrastructuur, platforms en diensten die het gebruik en de opslag van data ondersteunen. Digitale soevereiniteit omvat dus de controle over data, maar ook de controle over hardware, software en netwerkbronnen die digitale interacties mogelijk maken.

Digitale soevereiniteit wordt steeds belangrijker in de onderling verbonden wereld van vandaag. Staten en regio's proberen de controle over hun digitale omgeving (opnieuw) op te eisen om zich te beschermen tegen externe afhankelijkheden en kwetsbaarheden. De Europese Unie (EU) heeft bijvoorbeeld gepleit voor meer digitale soevereiniteit om de afhankelijkheid van niet-EU-technologieën te verminderen en naleving van de EU-normen voor databescherming te waarborgen.

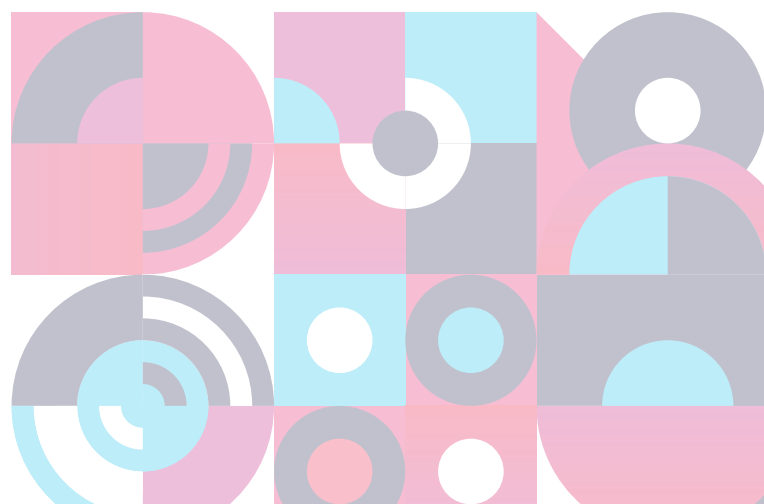
Een breed scala aan problemen en zorgen vallen onder het concept van digitale soevereiniteit, waaronder vraagstukken hoe data subjecten (de personen waar de data over gaan) controle kunnen uitoefenen op de verwerking van hun data en hoe een dergelijke controle kan worden geïmplementeerd. Deze controle kan op het niveau van individuen of collectieven (bijv. families, gemeenschappen). Daarnaast bestaat er bezorgdheid over hoe staten

of internationale organisaties zowel de materiële als immateriële aspecten van digitale infrastructuren kunnen beheren en controleren.

Het belang van digitale soevereiniteit wordt onderstreept door de toenemende geopolitieke spanningen rond technologie. Naties zijn op hun hoede voor buitenlandse surveillance en datalekken, die de nationale veiligheid en economische belangen in gevaar kunnen brengen. Door digitale soevereiniteit te laten gelden, willen staten de privacy van hun burgers beschermen en ervoor zorgen dat kritieke digitale infrastructuur bestand is tegen bedreigingen van buitenaf.

Digitale soevereiniteit omvat vaak wetten en beleidsregels die lokale dataopslag en -verwerking verplichten om gevoelige informatie binnen de landsgrenzen te houden. Sommige landen hebben bijvoorbeeld wetten voor data lokalisatie geïmplementeerd die bedrijven verplichten om data op te slaan en te verwerken op servers die zich fysiek in het land bevinden. Dit verbetert niet alleen de beveiliging van data, maar zorgt er ook voor dat data onderhevig zijn aan lokale wetten en regels..

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



2.6 Data soevereiniteit

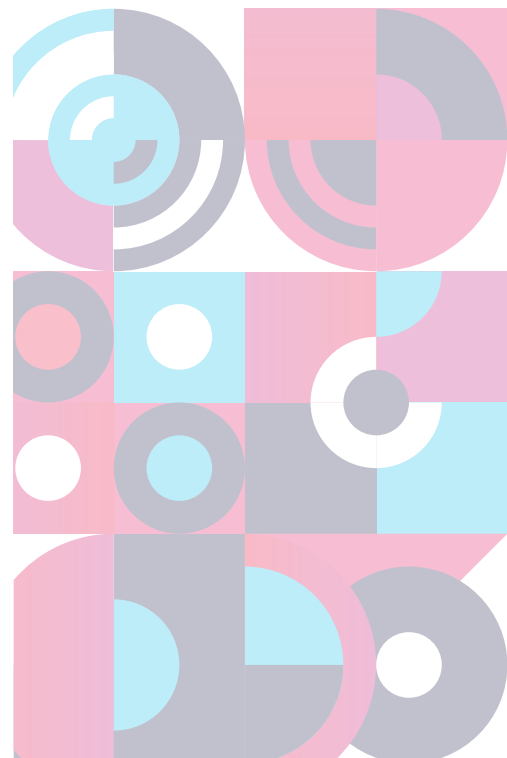
Data soevereiniteit heeft betrekking op de regels en referentiearchitecturen die kunnen helpen bij het waarborgen van een aantal fundamentele principes van digitale soevereiniteit, zoals waar de data worden opgeslagen, wie de data beheert, hoe ze op een veilige manier kunnen worden opgeslagen en verwerkt en hoe ze interoperabel en overdraagbaar kunnen worden gemaakt. Als zodanig kunnen individuen, organisaties, bedrijven, overheden of hele samenlevingen en landen de rol van houder van data soevereiniteit op zich nemen. Dit kan leiden tot tegenstrijdige claims van data soevereiniteit op deze niveaus. Wanneer het over individuen gaat, is data soevereiniteit nauw verbonden met het begrip digitale zelfbeschikking, wat duidt op het individuele recht en vermogen van een persoon om autonomie uit te oefenen over zijn digitale aanwezigheid, data en online activiteiten. Voor zover dat soevereiniteit betrekking heeft op collectieve controle over data, kan het verwijzen naar aanspraken van gemeenschappen (bijv. inheemse volkeren en gemeenschappen) of naties om controle uit te oefenen over welke verschijnselen van data worden voorzien, hoe de data worden gebruikt en wie ervan profiteert (zie ook [2.7 Inheemse data soevereiniteit](#)).

Op basis van hun verschillende benaderingen van kwesties met betrekking tot de controle over data, is gesuggereerd dat er drie belangrijke rechtsgebieden in de wereld - de VS, China en de EU - drie verschillende data soevereiniteit regimes vertegenwoordigen, namelijk respectievelijk bedrijfs soevereiniteit, staatssoevereiniteit en individuele soevereiniteit. Data soevereiniteit wordt ook prominent besproken in de context van het ontwerp van IT architectuur en/of wetten die de dataverwerking regelen.

In vrijwel alle gevallen is digitale soevereiniteit gericht op het vergroten van de controle en macht van collectieve actoren over data. Het type macht in kwestie is - anders dan in sommige klassieke concepten van soevereiniteit - geen brute kracht, maar het is de uitoefening van macht die waarden zoals inclusiviteit, deliberatie en de fundamentele rechten van de betrokken personen respecteren.

Data soevereiniteit streeft naar meer collectieve controle en toezicht over data en deelt daarmee een belangrijk punt van zorg met datasolidariteit. In tegenstelling tot data soevereiniteit is datasolidariteit echter niet primair gericht op de staat of de gemeenschap, maar streeft naar een eerlijker verdeling van voordelen en risico's via beleidsinstrumenten op alle niveaus: lokaal, gemeentelijk, nationaal en wereldwijd.

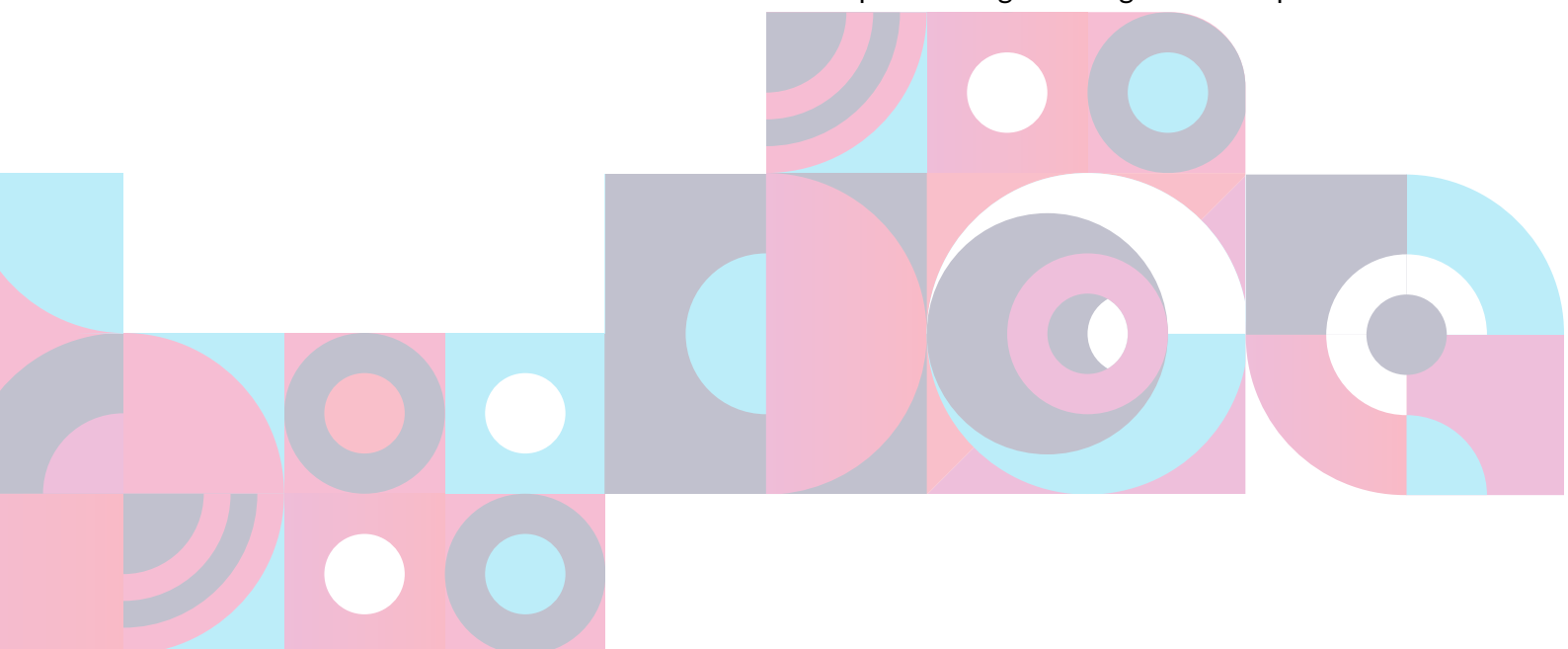
Referenties: Gao, 2021; Hummel et al., 2021; Science Po, undated; Verhulst, 2023; Woods, 2018.



2.7 Inheemse data soevereiniteit

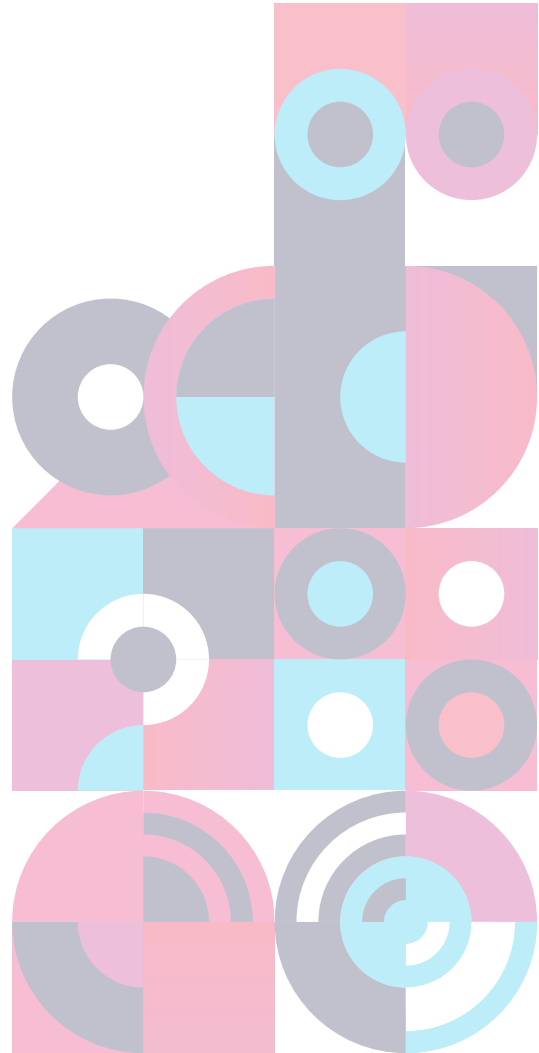
Inheemse data soevereiniteit is een concept dat de nadruk legt op het recht van inheemse volkeren en gemeenschappen om de data te controleren die van en over hun gemeenschappen worden verzameld. Het stelt dat data met betrekking tot inheemse groepen beheerd en bestuurd moeten worden volgens de normen, waarden en belangen van de gemeenschappen waaruit de data afkomstig zijn. Dit idee daagt dominante westerse modellen voor data governance uit die voorbijgaan aan Inheemse rechten en geen rekening houden met de unieke culturele, contextuele en historische omstandigheden van Inheemse volken en gemeenschappen, met name ook in termen van de schade die geleden is door koloniale machten en erfenissen (evenals de rechten en belangen van andere gemarginaliseerde groepen). Van specifiek belang in de context van inheemse data soevereiniteit zijn de zogenaamde CARE-principes, die werden geïntroduceerd als een aanvulling op de FAIR-principes (Vindbaar, Toegankelijk, Interoperabel en Herbruikbaar). Terwijl de FAIR-principes zich richten op de technische aspecten van data, leggen de CARE-principes de nadruk op de mensen en het doel achter het verzamelen en gebruiken van data:

- ? Collectief voordeel: Het ontwerp en de functie van data-ecosystemen moeten inheemse gemeenschappen in staat stellen voordeel te halen uit de data die van hen worden verzameld. Dit houdt in dat de data worden gebruikt op manieren die inheemse waarden en zelfbeschikking ondersteunen.
- ? Autoriteit om te controleren: Inheemse gemeenschappen moeten autoriteit hebben over de dataverzameling processen die hen aangaan, inclusief het recht om te bepalen hoe deze data worden verzameld, geopend en gebruikt.
- ? Verantwoordelijkheid: Degenen die omgaan met de data hebben de plicht om ervoor te zorgen dat de data worden gebruikt op een manier die de rechten en het welzijn van de inheemse bevolking respecteert en dat er adequate maatregelen worden genomen om de schade voor inheemse gemeenschappen tot een minimum te beperken en de voordelen te maximaliseren.
- ? Ethiek: Praktijken voor data governance moeten worden geleid door ethische kaders die geïnformeerd zijn door inheemse wereldbeelden, die vaak waarden omvatten zoals wederkerigheid, respect en zorg voor de gemeenschap.



Inheemse data soevereiniteit is ook nauw verbonden met inspanningen om historisch onrecht te herstellen en inheemse mensen en gemeenschappen mondig(er) te maken door ervoor te zorgen dat ze controle hebben over hun eigen data. Dit omvat data die gebruikt worden in overheidsbeleid, academisch onderzoek, gezondheidszorg en meer. Effectieve implementatie van inheemse data soevereiniteit kan leiden tot beter afgestemde diensten en beleid, betere privacybescherming en meer respect voor inheems cultureel erfgoed. Als zodanig is inheemse data soevereiniteit afgestemd op het doel van datasolidariteit om een eerlijker delen van risico's en voordelen van digitale praktijken te bereiken en - naast het respecteren van individuele autonomie - ook het versterken van collectieve instrumenten van controle en toezicht op data en digitale infrastructuren. Datasolidariteit en inheemse data soevereiniteit liggen ook op één lijn in de zin dat ze allebei verder gaan dan de dichotomieën die in het Westen worden gebruikt, zoals de dichotomie tussen persoonlijke en niet persoonlijke data. Zowel datasolidariteit als inheemse data soevereiniteit erkent dat mensen - als individuen en als leden van collectieven - belangrijke belangen kunnen hebben in data die niet 'persoonlijk' zijn in de technische zin van het woord (d.w.z. ze verwijzen niet naar een geïdentificeerd of identificeerbaar individu en vallen dus niet onder het toepassingsgebied van veel kaders voor databescherming over de hele wereld).

Referenties: 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 lokalisatie

Data lokalisatie¹ verwijst naar de wettelijke verplichting die overheden opleggen om data die binnen hun landsgrenzen worden gegenereerd, in eigen land op te slaan en te verwerken. Deze regels zijn bedoeld om data soevereiniteit te garanderen, waarbij data onderworpen zijn aan de wetten en het bestuur van het land waarin ze zijn gecreëerd. Dit is vooral belangrijk voor data die betrekking hebben op gevoelige sectoren zoals financiën, gezondheidszorg of nationale veiligheid, waar zorgen over privacy en databeveiliging van het grootste belang zijn. Landen dwingen data lokalisatie af om ongeautoriseerde buitenlandse toegang tot data te voorkomen, de persoonlijke privacy te beschermen en lokale wetshandhavers toegang te verlenen tot data voor onderzoek en regelgeving.

Voorstanders van data lokalisatie beweren dat het binnen de landsgrenzen houden van data de dataveiligheid en privacy verbetert, omdat landen dan hun eigen wet- en regelgeving kunnen handhaven. Het stimuleert ook lokale economieën door werkgelegenheid te creëren in datacenters, cloud computing en de ontwikkeling van IT-infrastructuur. Bovendien kan het opkomende economieën helpen lokale technologie-industrieën te stimuleren door ervoor te zorgen dat

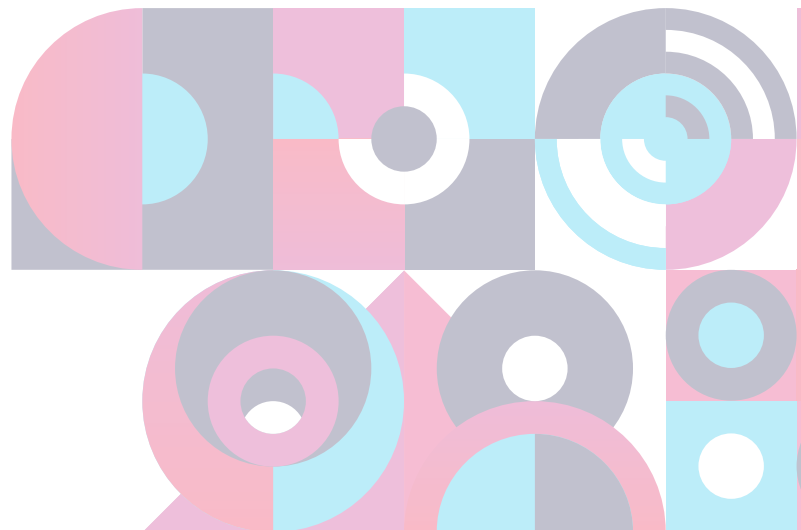
dataverwerkingsbronnen binnen het land blijven.

Critici van data lokalisatie wijzen op verschillende nadelen. Ze stellen dat het de operationele kosten kan verhogen voor multinationale bedrijven die aan meerdere regelgevingskaders moeten voldoen. Deze fragmentatie kan ook de datastroom over de grenzen heen belemmeren, waardoor wereldwijde innovatie en samenwerking worden beperkt. Bovendien kunnen vereisten voor data lokalisatie de toegang tot de meest geavanceerde dataverwerkingstools belemmeren, die zich vaak in andere regio's bevinden, waardoor de technologische vooruitgang binnen het land mogelijk wordt beperkt.

Binnen datasolidariteit is data lokalisatie een welkome ontwikkeling als het helpt om meer gelijkheid te creëren tussen landen en wereldregio's - dat wil zeggen, als het wordt gebruikt door digitaal achtergestelde naties om meer voordelen voor hen te garanderen. Als het wordt gebruikt door rijke landen om hun voordeel te versterken, beschouwt datasolidariteit data lokalisatie juist als schadelijk.

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

¹ Let op: data lokalisatie zoals hier bedoeld wordt, heeft betrekking op de opslag van data binnen politiek-geografische grenzen, zoals een land of de Europese Economische Ruimte. In de Nederlandse context wordt de term 'data lokalisatie' ook gebruikt in de context van generieke functies van de WEGIZ. In die context heeft het een andere betekenis, zie <https://www.datavoorgezondheid.nl/generieke-functies>.



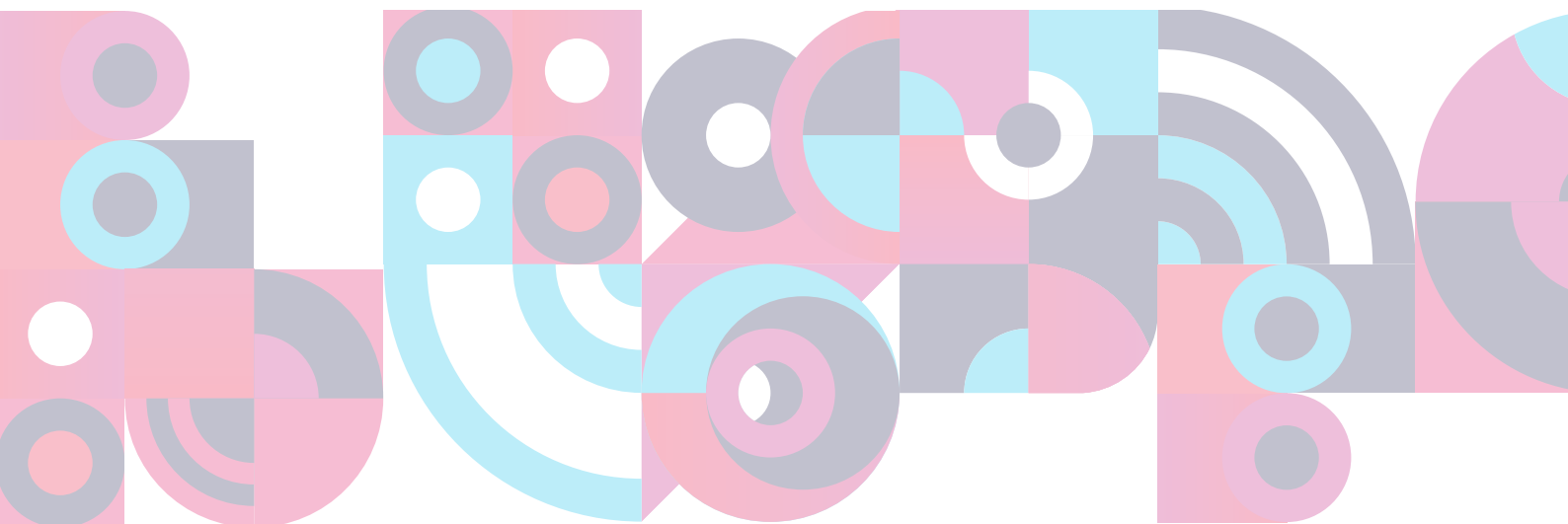
2.9 Schadebeperking

Schadebeperking is een van de drie pijlers van datasolidariteit (zie [Tabel 2: De drie pijlers van datasolidariteit](#)). Telkens wanneer data worden gebruikt - zelfs als dit grote voordelen oplevert voor mensen en gemeenschappen - bestaat het risico dat individuen of groepen worden geschaad. Wanneer bijvoorbeeld gevoelige persoonlijke informatie wordt blootgelegd, kan dit leiden tot identiteitsdiefstal en financiële verliezen. Het ongeoorloofd delen van data kan ook leiden tot discriminatie, omdat mensen oneerlijk behandeld kunnen worden op basis van hun dataprofielen, wat hun toegang tot banen, verzekeringen en diensten kan beïnvloeden. Tot slot kan het op grote schaal verzamelen en controleren van data de persoonlijke vrijheden aantasten en de vrijheid van meningsuiting en andere vrijheden beperken uit angst om gecontroleerd te worden.

Hoewel we moeten proberen om risico's zoveel mogelijk te beperken, is het ook belangrijk om openlijk te erkennen dat er nog steeds schade kan optreden, dat sommige schade nog niet volledig bekend of begrepen is en dat mensen die schade hebben ondervonden, adequate ondersteuning en compensatie moeten krijgen.

Over het algemeen kan schade ontstaan door het gebruik of niet-gebruik van data. Schade door datagebruik kan leiden tot inbreuken op de privacy, emotionele schade of inbreuken op culturele rechten. Schade door het niet-gebruik van data omvat fysieke schade door het niet op de hoogte zijn van eerdere medische voorgeschiedenis, gebrek aan responsiviteit voor ernstige medische aandoeningen, het niet profiteren van wetenschap of het niet identificeren van ongelijkheden of het verhogen van de kosten van het zorgstelsel door onnodige duplicatie. Bij het overwegen van risico's met betrekking tot schade wordt idealiter rekening gehouden met het volledige scala aan data gerelateerde schade, samen met de waarschijnlijkheid en impact ervan.

Vandaag de dag worden mensen en gemeenschappen die benadeeld worden door het gebruik van data om verschillende redenen vaak niet ondersteund. Er kan schade ontstaan zonder dat er wetten worden overtreden, bijvoorbeeld wanneer mensen hogere tarieven in rekening worden gebracht voor dezelfde diensten als anderen of dat aan hen diensten worden geweigerd op basis van voorspellende analyses. Mensen kunnen ook schade ondervinden van sociale media of digitale



platforms, zonder dat de inhoud illegaal is. In andere gevallen ontstaat er schade zonder dat de benadeelde partij precies kan vaststellen wie de schade heeft veroorzaakt. Hoe meer data worden gedeeld en gekoppeld en hoe minder transparant deze processen zijn, hoe moeilijker het wordt voor mensen om te bepalen wat of wie verantwoordelijk is voor de schade die ze hebben ervaren. Tot slot hebben mensen geen toegang tot rechtsmiddelen omdat ze niet over de sociale en economische middelen beschikken om ze te gebruiken. Vanuit het oogpunt van datasolidariteit is het essentieel dat mensen die schade ondervinden van het gebruik van data toegang hebben tot ondersteuning, onafhankelijk van waar ter wereld ze zich bevinden. Eén manier om dit te doen is het oprichten van organisaties voor schadebeperking, in het Engels 'Harm Mitigation Bodies'. Harm Mitigation Bodies (HMB) zijn onafhankelijke organisaties die beroepen beoordelen van mensen die beweren schade te hebben ondervonden door datagebruik. De wet zou kunnen voorschrijven dat elke organisatie boven een bepaalde omvang aangesloten moet worden bij een HMB. Grote organisaties, zoals multinationals, zouden hun eigen HMB kunnen oprichten, terwijl kleinere bedrijven zich zouden kunnen onderwerpen aan het toezicht van een HMB op regionaal, nationaal, supranationaal of zelfs internationaal niveau.

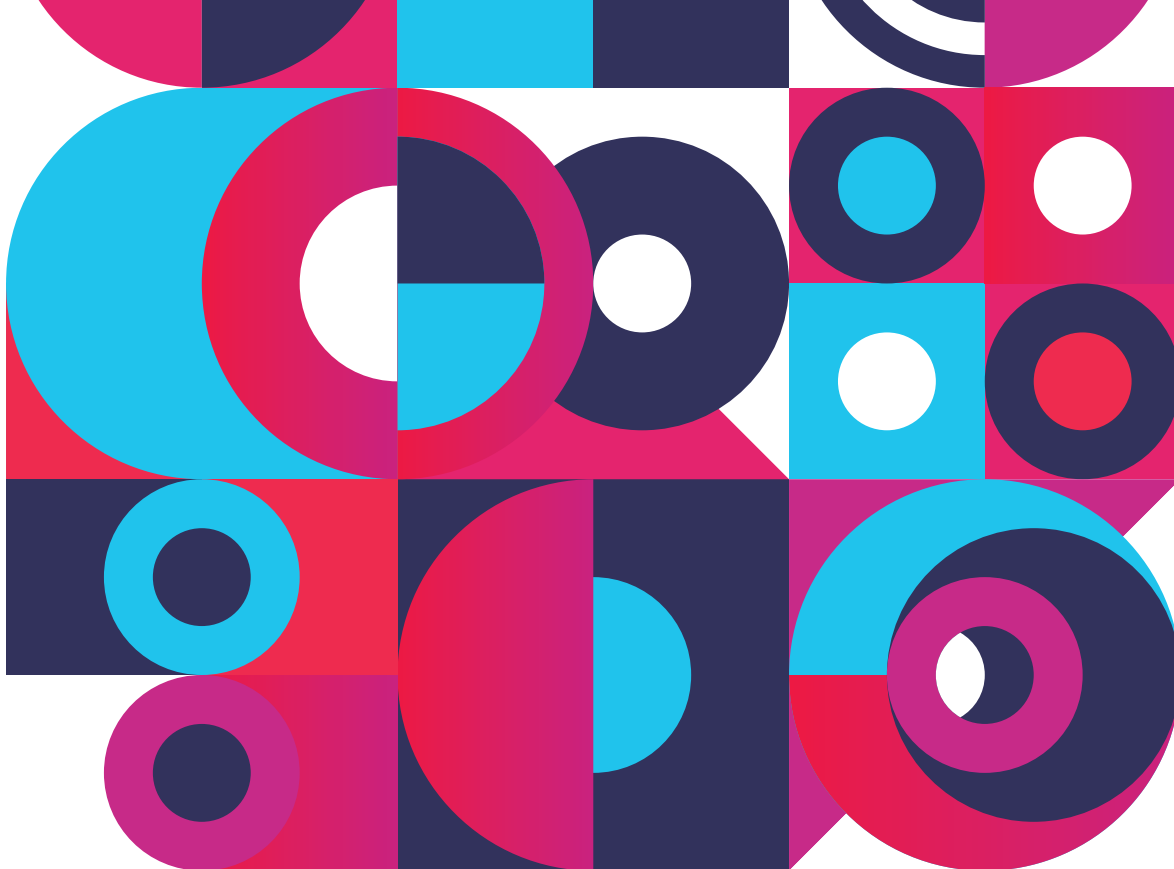
HMBs zouden drie primaire functies moeten vervullen. Ten eerste zouden ze een de facto toezichthoudende instantie zijn vanwege de schade die mensen melden. Databeheerders (of bewaarders of rentmeesters) en overheidsinstanties kunnen dan toegang krijgen tot die

informatie om de werking van systemen voor data governance te verbeteren. Ten tweede, in specifieke gevallen, wanneer mensen financiële schade hebben geleden en niet in staat waren om elders steun te krijgen, moeten ze ook financiële steun kunnen bieden. Anders dan in formele juridische mechanismen, is er geen vereiste om wangedrag of directe juridische causaliteit van de geleden schade te bewijzen. Ten derde zouden HMBs toezicht houden op waar in het algemeen belang data niet tijdig en met de vereiste kwaliteit wordt verstrekt. In dergelijke gevallen zou de HMB de potentiële impact op gemeenschappen van het niet-gebruik van data kwantificeren en in staat zijn om passende herstelmaatregelen te treffen.

Naast HMBs zijn er ook andere maatregelen voor schadebeperking. Ze omvatten respons plannen voor datalekken, waarin implementatieplannen voor inperking, onderzoek en herstel van datalekken worden uiteengezet. Audits en beoordelingen na een incident kunnen helpen om de oorzaken van de schade in specifieke gevallen te begrijpen en als gevolg daarvan de data governance te verbeteren. Het rectificeren en wissen van data biedt mechanismen waarmee getroffen personen foutieve data kunnen corrigeren en hun persoonlijke data kunnen laten wissen om verder misbruik te voorkomen.

Welke maatregelen er ook worden gekozen, schadebeperking moet worden opgezet als een aparte, aanvullende maatregel naast risicominimalisatie en moet gemakkelijk toegankelijk zijn.

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



Deel 3: Delen van data

3.1 Digitale commons en data commons

In de context van datasolidariteit zijn commons één manier om collectief toezicht op en eigendom van data en digitale infrastructuren te vergroten. Commons zijn sociale instellingen voor het beheer van gemeenschappelijke hulpbronnen - dat wil zeggen hulpbronnen die toegankelijk zijn voor meerdere mensen (ze zijn 'gemeenschappelijk') en waarvan het moeilijk is om iemand uit te sluiten van gebruik (ze zijn 'niet uit te sluiten'). Gemeenschappelijke hulpbronnen worden bestuurd door de principes van waarden als eerlijkheid, gelijkheid, rechtvaardigheid en duurzaamheid.

Commons hebben een lange juridische en historische traditie op gebieden die variëren van het gebruik van landbouwgrond tot bossen en lesmateriaal. Er zijn discussies

geweest over de mate waarin commons toegepast kunnen worden op immateriële hulpbronnen zoals digitale data. Sommige auteurs gebruiken het begrip commons in een nog ruimere betekenis, onder meer onder het label van digitale commons (data, informatie, cultuur en kennis) die online gecreëerd en/of onderhouden worden en die voor publiek gebruik bestemd zijn. Een dergelijke brede opvatting van commons heeft de neiging om commons-regimes, waarbij mensen gezamenlijk eigenaar zijn van de bron en beslissen over het gebruik ervan, gelijk te stellen met open toegang regimes ('Open Access'), waarbij iedereen de bron kan gebruiken zoals hij wil en niemand uitgesloten kan worden.

De digital commons beweging was vooral sterk in de nasleep van de bankencrisis

van 2008, maar ook toen de toegang tot wetenschappelijke literatuur steeds duurder werd, rond het jaar 2010. Overall ter wereld ontstonden nieuwe vrijwilligersorganisaties, nieuwe digitale vormen van participatie, niet-commerciële infrastructuren om middelen te delen en nieuwe sociale ruimten. Hun bedoeling was om een alternatief te creëren voor de heersende machtsstructuren en markten in een netwerkmaatschappij. Het succes van deze initiatieven kwam in het gedrang door de commercialisering van veel open kennisbronnen en ook omdat actoren in de context van onderzoek het zich gemakkelijker konden veroorloven om hun data en bronnen 'open te stellen' en ook beter gebruik konden maken van data en bronnen die anderen hadden opengesteld. Deze kwesties illustreren eens te meer de beperkingen van 'commons'-concepten die in feite open toegang regelingen zijn, die de neiging hebben om een Matteüs-effect te ontplooiën: als alles voor het grijpen ligt, kunnen degenen die al meer macht en middelen hebben, meer van de open bron nemen.

Datasolidariteit ondersteunt commons als een manier voor mensen - op lokaal, regionaal, nationaal of transnationaal niveau - om gezamenlijk hulpbronnen te bezitten en te beheren. Het steunt geen 'commons' die open toegang regimes zijn, wat betekent dat er geen collectief eigendom van de bron is en iedereen het kan nemen zoals hij wil.

Digitale commons en data commons die verenigbaar zijn met de geest van datasolidariteit kunnen worden geïmplementeerd door platforms op te zetten waar data collectief worden beheerd door iedereen die data bijdraagt, waarbij transparantie en billijk gebruik worden gewaarborgd. Een opkomende trend in deze context is het opzetten van 'gevirtualiseerde data commons' in vertrouwde netwerken van medewerkers. In dergelijke gevallen worden de data niet gekopieerd of geconsolideerd in één enkele data opslag. In plaats daarvan blijven de data bij de bron en zijn beschikbaar in het netwerk via een overeengekomen collectief zoekmechanisme. Dergelijke gevirtualiseerde data trusts (zie [3.3 Data trusts](#)) ondersteunen gefedereerd leren. Deze netwerken houden zich aan gemeenschappelijke eisen voor het hele netwerk op het gebied van juridische, bestuurlijke en data interoperabiliteit. Daarnaast is er een vereiste voor beleidscontroles, training en stakeholderbetrokkenheid om te leren en vertrouwen te behouden. Dergelijke gevirtualiseerde data trusts zullen steeds vaker voorkomen bij transnationale partnerschappen, zoals bijvoorbeeld in de European Health Data Space..

Referenties: 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.

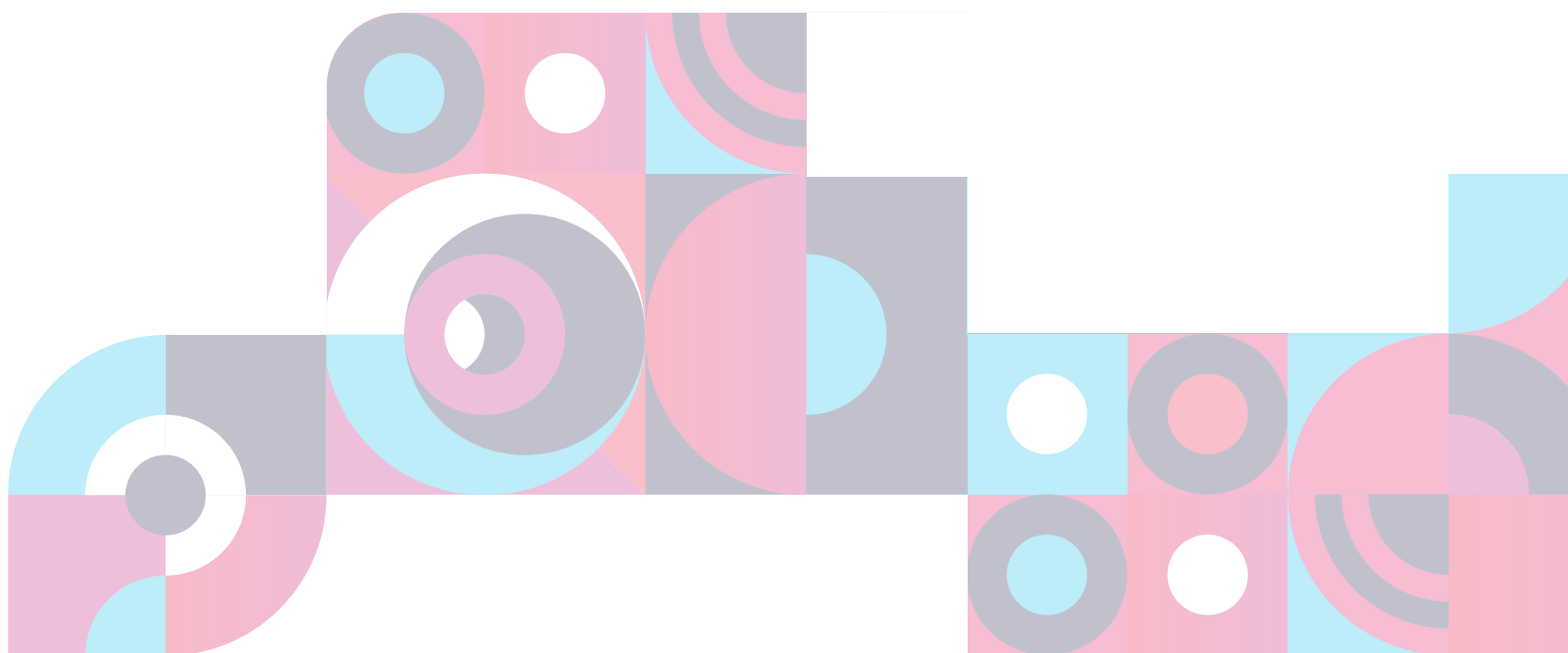


3.2 Data coöperaties

Over het algemeen zijn data coöperaties organisaties waar mensen hun data bundelen tot wederzijds voordeel. Deze term wordt vaak synoniem gebruikt met data commons. Beide vertegenwoordigen collectieve vormen van het bezitten en beheren van data. Als er een verschil wordt gemaakt tussen data commons en data coöperaties, dan is dat om de volgende kenmerken te benadrukken die coöperaties kenmerken: vrijwillig lidmaatschap, democratische controle, economische participatie, autonomie ten opzichte van andere commerciële of publieke entiteiten en een oriëntatie op publieke waarde. Door hun krachten te bundelen, kunnen

leden betere voorwaarden bedingen bij dataverzamelaars en toegang krijgen tot diensten die gebruikmaken van hun collectieve data, terwijl ze meer controle houden over het gebruik ervan. Terwijl sommige data coöperaties zich primair richten op het creëren van publieke waarde, hebben andere (ook) als doel mensen te helpen hun data te gelde te maken. Net als data commons kunnen data coöperaties helpen om datasolidariteit te realiseren als de oriëntatie op publieke waarden niet wordt overstemd door particularistische of winstgerichte belangen..

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



3.3 Data trusts

Data trusts zijn juridische structuren die zijn ontworpen om het gebruik van data te beheren en overzien namens een groep begunstigden, zoals individuen, gemeenschappen of de samenleving als geheel. Data trusts worden bestuurd door trustees die beslissingen nemen over het gebruik en beheer ervan op basis van de belangen van de begunstigden. De trustees hebben de fiduciaire plicht om in het belang van de begunstigden te handelen en ervoor te zorgen dat de data verantwoord en ethisch worden gebruikt. Data trusts kunnen worden opgericht om verschillende problemen op het gebied van data governance aan te pakken, waaronder privacybescherming, toegang tot data en de garantie dat data worden gebruikt ten behoeve van de samenleving. Ze bieden een mechanisme voor individuen en gemeenschappen om enige controle over hun data te houden terwijl het gebruik ervan op eerder overeengekomen manieren mogelijk blijft.

Zogenaamde datakluisen kunnen dienen als de technische architectuur die ten grondslag ligt aan data trusts, waardoor organisaties data veilig kunnen opslaan en tegelijkertijd vertrouwde partijen toegang kunnen geven tot de benodigde informatie, met behoud van transparantie en verantwoordelijkheid. Ze zijn een soort magazijn-modelleringsmethodologie die is ontworpen om grootschalige data-omgevingen te verwerken, met name die omgevingen die zich snel moeten aanpassen aan nieuwe vereisten of veranderingen. Ze richten zich op schaalbaarheid, flexibiliteit en consistente integratie van data uit meerdere bronnen.

Het belangrijkste verschil tussen data commons en -coöperaties aan de ene kant en data trusts aan de andere kant, ligt in hun bestuurs- en eigendomsstructuren.

In het geval van data commons en data coöperaties worden data - op zijn minst moreel of zelfs juridisch - beschouwd als gezamenlijk eigendom van alle leden. Data trusts daarentegen kunnen dienen als datakluisen waarin individuele mensen hun data kunnen deponeren voor een entiteit (de trustees) die namens hen wordt bestuurd. Dit betekent dat hoewel data coöperaties en data commons kunnen worden beschouwd als een manier om data te bezitten en te besturen die indruist tegen data-individualisme en de prioritering van financiële winst, dienen sommige data trusts precies deze laatstgenoemde doelen. Ze behandelen data niet als gemeenschappelijk bezit, maar als individuele activa. Als zodanig behoren data trusts niet tot de beleidsinstrumenten die worden gepromoot door datasolidariteit, tenzij ze dezelfde solidaire principes afdwingen als data commons.

Een voorbeeld voor het laatste uit het domein of onderzoek zijn zogenaamde vertrouwde onderzoeksomgevingen (trusted research environments, TRE's), die dienen als veilige platforms binnen data trusts, waardoor onderzoekers toegang kunnen krijgen tot gevoelige data en deze kunnen analyseren terwijl de privacy en naleving van ethische normen worden gewaarborgd. Deze omgevingen implementeren strenge toegangscontroles, technieken voor het anonimiseren van data en audit mechanismen om data van individuen te beschermen tegen misbruik. Door transparantie en verantwoordingsplicht te bevorderen, bouwen TRE's vertrouwen op bij betrokkenen en belanghebbenden, waardoor een verantwoord gebruik van data voor wetenschappelijke en publieke doeleinden mogelijk wordt.

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

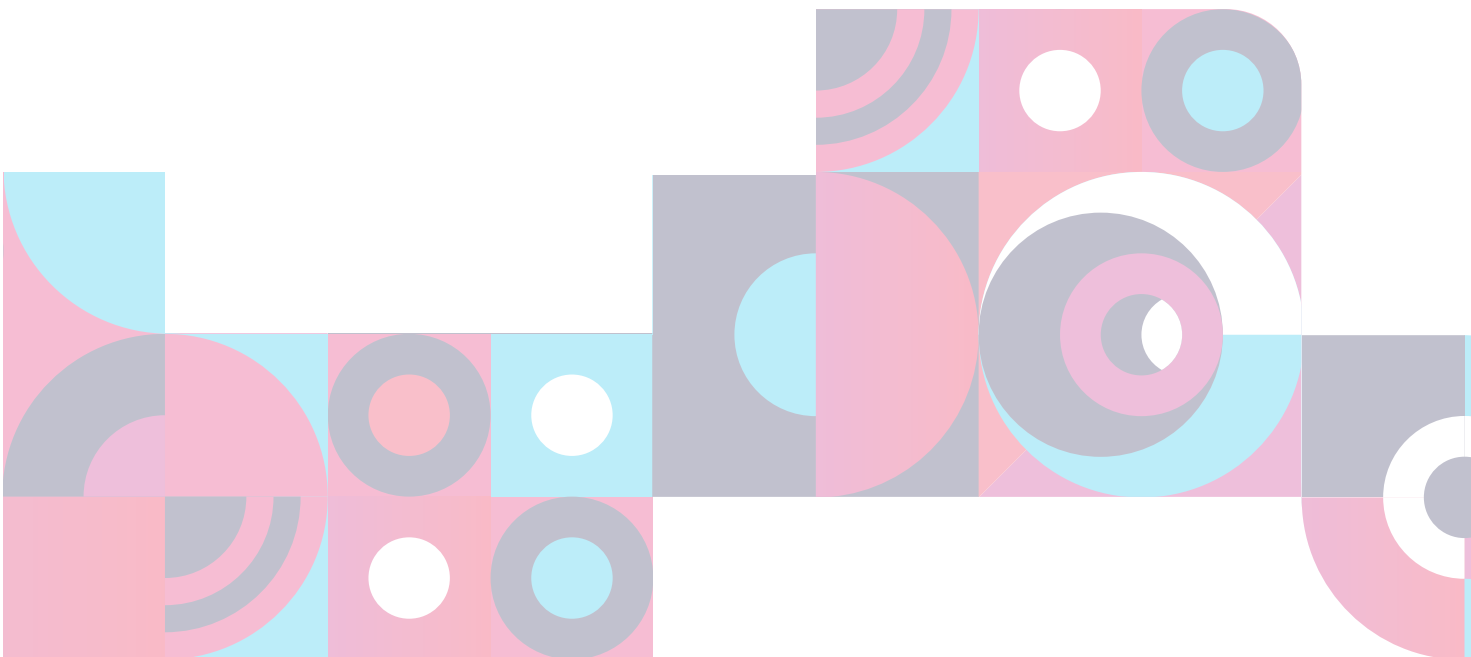
3.4 Data delen

Een breed scala aan uiteenlopende activiteiten - van onderzoekinstellingen die geïnterpreteerde resultaten van genomisch onderzoek beschikbaar stellen aan deelnemers, tot klanten die online bedrijven toestemming geven om informatie te gebruiken over hoe zij hun diensten gebruiken - vallen allemaal onder het delen van data. Het omvat dus het kopiëren van data en toegang tot de brondata zonder een kopie te maken. Een ander nadeel van deze inclusieve definitie is dat het onmogelijk is om onderscheid te maken tussen gevallen van het delen van data die publieke waarde creëren en ten goede komen aan mensen en samenlevingen en gevallen die alleen dienen voor het maximaliseren van commerciële winsten. Voor datasolidariteit daarentegen is dit onderscheid cruciaal.

Datasolidariteit wordt soms verward met het delen van data, wat onjuist is. Het delen van data verwijst naar het beschikbaar stellen van data aan derden, ongeacht het

doel waarvoor de data worden gebruikt en tot wiens voordeel. Datasolidariteit daarentegen heeft als doel de schade en voordelen die voortkomen uit digitale praktijken eerlijker te verdelen. Hoewel sommige gevallen van delen van data een uitdrukking of een resultaat van datasolidariteit kunnen zijn, zijn andere (zoals data altruïsme) dat niet. Soms kan datasolidariteit zich uiten in het niet beschikbaar stellen van data aan specifieke entiteiten. Het kan zich ook uiten door bepaalde aspecten van het lichaam en het leven van mensen überhaupt niet in data vast te leggen.

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



3.5 Data altruïsme

Data altruïsme staat centraal in de Data Governance Act van de Europese Unie, die op 30 mei 2022 door de Europese Unie werd aangenomen. Deze verordening heeft tot doel een kader te creëren voor data governance binnen de EU, waarbij de nadruk ligt op het veilige hergebruik van overheidsdata en het creëren van een gelijk speelveld in de data economie door het delen van data te bevorderen en belemmeringen voor de toegankelijkheid van data te verminderen. In deze verordening wordt altruïsme gedefinieerd als “data die door individuen of bedrijven vrijwillig beschikbaar worden gesteld voor het algemeen belang” (hoofdstuk IV). In dit hoofdstuk wordt beschreven hoe individuele personen en bedrijven vrijwillig data beschikbaar kunnen stellen voor het algemeen belang en worden mechanismen vastgesteld waarmee organisaties die zich bezighouden met dergelijke activiteiten zich kunnen registreren als ‘Data Altruïsme Organisaties erkend in de EU’. Om dit te kunnen doen, moet een organisatie zonder winstoogmerk opereren en onafhankelijk zijn van entiteiten met winstoogmerk. De organisatie moet ook kunnen garanderen dat haar activiteiten op het gebied van data altruïsme plaatsvinden via een wettelijk erkende onafhankelijke structuur, los van andere activiteiten die het heeft ondernomen.

Het perspectief van de Europese Commissie op ‘altruïsme’ lijkt gebaseerd te zijn op specifieke aannames over hoe mensen gemotiveerd kunnen worden om hun data ‘gratis’ beschikbaar te stellen. Het valt nog te bezien of de extra winst van ‘gecertificeerde betrouwbaarheid’ van geregistreerde altruïstische data organisaties en sjablonen voor toestemmingsformulieren voldoende prikkels zullen creëren voor het delen van data.

Afgezien van de specifieke context van EU-regelgeving, bestaat er in de bredere juridische, beleidsmatige en ethische literatuur geen gemeenschappelijke opvatting over wat altruïsme met betrekking tot data inhoudt. Sommige auteurs gebruiken het als een algemene term om te verwijzen naar een reeks waarden en praktijken die nauw verbonden zijn met de concepten van data donatie en data deling. Vanuit het perspectief van datasolidariteit is het begrip altruïsme in verschillende opzichten problematisch: Ten eerste omdat het veronderstelt dat mensen hun belangen in de data die ze delen moeten opgeven, wat - vooral in verband met gezondheidsdata - niet logisch is. Weinig mensen zouden serieus beweren dat patiënten die hun gezondheidsdata delen niet langer het recht zouden hebben om deze data te controleren. Het begrip solidariteit, dat de nadruk legt op een voortdurende relatie tussen betrokkenen en gebruikers van data, lijkt meer passend in dit opzicht. Een ander probleem met het raamwerk voor altruïsme van data is dat hele instellingen het stempel van goedkeuring kunnen krijgen, ervan uitgaande dat ze in het algemeen belang werken. Zo’n brede benadering gaat voorbij aan de noodzakelijke nuances die komen kijken bij verschillende vormen van datagebruik, ongeacht wie de gebruiker van de data is. Daarom verbindt datasolidariteit wettelijke consequenties aan verschillende soorten datagebruik, na een beoordeling van zowel de risico’s als de potentiële voordelen, waarbij ook wordt gekeken voor welke groepen deze risico’s en voordelen zich het meest waarschijnlijk zullen voordoen.

Referenties: 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 donatie

Juridische definities van het concept schenking, die teruggaan tot het oude Romeinse recht, richten zich op de eigenaar van een ding die het overdraagt aan een andere persoon of entiteit zonder er iets voor terug te verwachten. Dit laatste aspect - dat iets wordt gegeven zonder er iets voor terug te vragen of zelfs maar te verwachten - zegt ons twee dingen over schenkingen. Ten eerste dat er geen economisch winst oogmerk verbonden is aan een overdracht. Ten tweede dat donaties niet wederkerig zijn op een directe en lineaire manier - ook al zijn ze, net als andere giften, ingebed in netwerken van wederzijdse morele en sociale verplichtingen. In plaats daarvan zijn donaties indirect wederkerig. Bovendien zijn donaties rivaliserend en consumeerbaar: Als iemand geld doneert aan een ziekenhuis, dan kunnen ze niet hetzelfde geld geven aan rampenbestrijding. Als iemand een nier doneert aan één persoon, kan hij dezelfde nier niet aan iemand anders doneren. Van oudsher houden donaties in dat er een verbruiksgoed is dat wordt overgedragen van de ene entiteit naar de andere.

De vraag is of hetzelfde kan worden gezegd van digitale data, waaronder gezondheidsdata. Gezien het feit dat digitale data zich op meer dan één plaats tegelijk kunnen bevinden en dat ze vaak sporen achterlaten, zelfs als ze 'verwijderd' zijn, rijst de vraag waar een donatie begint en eindigt. Worden alle kopieën van een dataset gedoneerd of kan een kopie door de oorspronkelijke betrokkene worden bewaard? Het concept van data

donatie is vooral verwarrend wanneer het wordt gebruikt in een context waarin mensen iets aan anderen geven waar ze toegang tot blijven houden - zoals wanneer iemand toestaat dat data uit zijn stemmingsdagboek worden gebruikt voor onderzoek.

Vanwege deze dubbelzinnigheden vermijdt de benadering van datasolidariteit het concept van donatie in de context van data. Voor zover andere auteurs of beleidsmakers de term data donatie gebruiken, hangt het af van de motivatie van de persoon die de data beschikbaar stelt en van de doeleinden en contexten waarvoor de data worden gebruikt of een specifiek geval van data donatie ook solidair is. Omdat het doneren van iets doorgaans betekent dat de persoon die doneert geen rechten of belangen meer heeft in het gedoneerde, is het gebruik van de term donatie met name problematisch in de context van gezondheidsdata. Het zou niet ethisch en in sommige gevallen ook illegaal zijn om te eisen dat mensen die hun gezondheidsdata beschikbaar stellen voor gebruik door anderen, er geen toegang meer toe hebben.

Het concept van data donatie kan echter heel nuttig zijn als het gaat om de vraag wat er met de data van een persoon gebeurt na zijn dood. In de meeste wetgevingen zijn data over en eigendom van overleden personen grotendeels ongereguleerd. Data donatie kan een manier zijn voor mensen om te beslissen over het lot van hun data zolang ze nog in leven zijn.

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

3.7 Open data / Open science

Open data beschrijft alle data die vrij toegankelijk zijn, (her)gebruikt en gedeeld kunnen worden door iedereen zonder beperkingen. Open data heeft zich de afgelopen decennia ontwikkeld als een beweging en heeft geleidelijk het overheidsbeleid op nationaal en internationaal niveau beïnvloed. De primaire focus ligt op het vergemakkelijken van de openbaarmaking van openbare data in open repositories in een machine leesbaar formaat. Hiertoe ontwikkelen landen Open data portalen en Application Programming Interfaces die bedrijven en onderzoekers in staat stellen om toegang te krijgen tot administratieve data en deze efficiënt te verwerken. Open data wordt beschouwd als een middel om wetenschap, technologie, innovatie en de economie te ontwikkelen. In deze context is het ook erkend door de Verenigde Naties als een initiatief dat aanzienlijk kan bijdragen aan het behalen van de Duurzame Ontwikkelingsdoelen.

Open data is nauw verbonden met Open science. Deze laatste combineert verschillende concepten, bewegingen en praktijken die erop gericht zijn wetenschappelijke kennis openlijk beschikbaar en toegankelijk te maken voor iedereen. Openheid verwijst in de eerste plaats naar de afwezigheid van kosten barrières, maar ook naar informele barrières met betrekking tot de vindbaarheid van data, digitale vaardigheden en beschikbare middelen. Wat openlijk beschikbaar moet worden gemaakt zijn voornamelijk de middelen en output van kennisproductie, met name academische publicaties en wetenschappelijke data.

Recentere beleidsinstrumenten zijn ook van toepassing op algoritmen, broncodes, software en workflows. Het begrip Open science is ook nauw verbonden met de open source beweging. Open source verwijst naar elk programma waarvan de broncode beschikbaar wordt gesteld voor gebruik of aanpassing naar goeddunken van gebruikers of andere ontwikkelaars. In tegenstelling tot proprietary software is open source software computer software die ontwikkeld is als een open publieke samenwerking en vrij beschikbaar is voor het publiek.

Vooral voor zover het gaat om het faciliteren van datagebruik dat een significante publieke waarde creëert, delen de Open data, Open science en Open source bewegingen belangrijke doelen met datasolidariteit. Tegelijkertijd is openheid, zoals kritische wetenschappers benadrukken, geen doel op zich. Vooral in gevallen waarin openheid gericht is op formele gelijkheid in toegang, leidt dit er vaak toe dat economisch machtigere actoren beter gebruik kunnen maken van de openbaar beschikbare middelen dan anderen. Hierdoor neemt de ongelijkheid toe in plaats van af. Als Open science niet in dienst wordt gesteld van inhoudelijke doelen zoals het vergroten van gelijkheid en rechtvaardigheid, kan het slechts cosmetische effecten hebben en zelfs bijdragen aan het verergeren van de kloof tussen onderzoekers en het publiek in contexten met en zonder hulpbronnen.

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

3.8 European Health Data Space (EHDS)

De European Health Data Space (EHDS) is een initiatief van de Europese Unie om de toegankelijkheid, interoperabiliteit en uitwisseling van gezondheidsdata tussen de lidstaten te verbeteren. Met een eerste ontwerp dat in mei 2022 werd gepubliceerd, is het besproken in verschillende EU-instellingen. Als het wordt aangenomen, kan het al in 2025 van kracht worden.

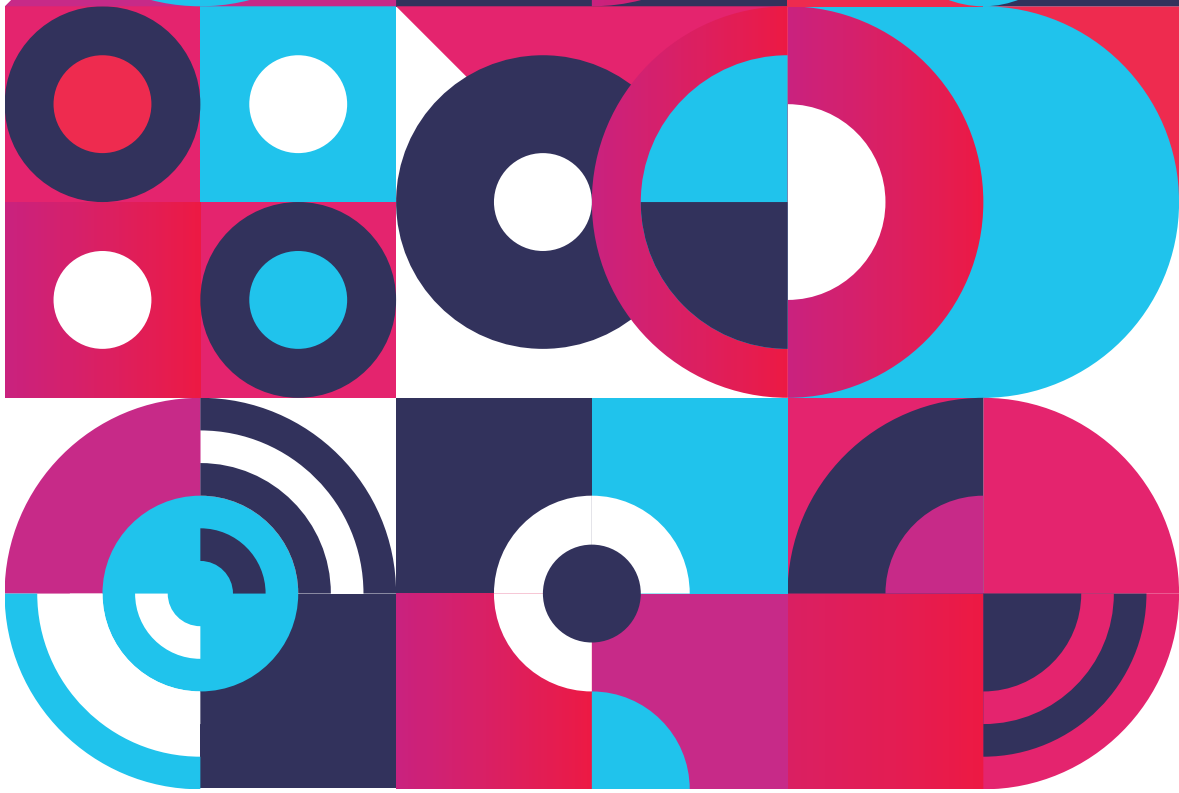
De EHDS streeft ernaar het potentieel van digitale gezondheidstechnologieën te benutten om de levering van gezondheidszorg, onderzoek en innovatie te verbeteren en tegelijkertijd databescherming en privacy te waarborgen. Het doel is een gemeenschappelijk kader en infrastructuur te creëren voor het veilig uitwisselen van gezondheidsdata, waaronder elektronische patiëntendossiers, genomische data en real-world data van gezondheidszorgsystemen, onderzoeksinstellingen en andere bronnen. Door de naadloze uitwisseling van gezondheidsdata te vergemakkelijken, wil de EHDS een effectievere planning van de gezondheidszorg, gepersonaliseerde geneeskunde en initiatieven op het gebied van gezondheidsonderzoek ondersteunen, wat uiteindelijk bijdraagt aan betere gezondheidsresultaten voor Europese burgers. Tijdens het Franse voorzitterschap van de Raad van de Europese Unie in 2022 werden ethische principes voor het gebruik van digitale gezondheid voorgesteld: baseer digitale gezondheid op humanistische waarden; stel individuen in staat hun digitale gezondheid en data te beheren; maak digitale gezondheid inclusief; en implementeer ecologisch verantwoorde digitale gezondheid.

Critici hebben hun bezorgdheid geuit over de mogelijke risico's voor de privacy van het individu en de veiligheid van

gezondheidsdata, vooral met betrekking tot de gecentraliseerde opslag en uitwisseling van gevoelige informatie. Er zijn ook uitdagingen met betrekking tot het waarborgen van de interoperabiliteit van verschillende gezondheidsdata systemen in de lidstaten, aangezien verschillende landen verschillende normen en protocollen voor data uitwisseling kunnen hebben. Daarnaast zijn er vragen gesteld over de bestuursstructuur van het EHDS en de betrokkenheid van belanghebbenden, waaronder patiënten en zorgverleners, bij besluitvormingsprocessen. Er is betoogd dat er meer transparantie en verantwoording nodig is om deze zorgen weg te nemen en ervoor te zorgen dat de EHDS de voordelen van het delen van data effectief in evenwicht brengt met de bescherming van de rechten en belangen van individuen. Ook de notie van data altruïsme binnen het EHDS is bekritiseerd als problematisch (zie [3.5 Data altruïsme](#)).

Vanuit het perspectief van datasolidariteit zijn er verschillende problemen met het EHDS-voorstel, waaronder het sterke gebruik van de term altruïsme. In tegenstelling tot solidariteit, een relationeel concept dat de wederzijdse behoeften en verantwoordelijkheden tussen verschillende actoren benadrukt, zou altruïsme kunnen suggereren dat degenen die data delen dit doen om puur onbaatzuchtige redenen en bereid zijn hun belang in de data op te geven. Bovendien zijn er zorgen dat de bepalingen van de EHDS grote bedrijven ten goede zouden kunnen komen om nog gemakkelijker toegang te krijgen tot data en zo de asymmetrie in macht en invloed tussen grotere en kleinere entiteiten in data-economieën zouden kunnen vergroten.

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



Section 4: Ethiek en macht

4.1 Digital and data ethics

Digitale en data ethiek (inclusief ethische AI) zijn belangrijke aanvullingen op datasolidariteit. Digitale en data ethiek richt zich op de morele verplichtingen die alle maatschappelijke actoren hebben (of zouden moeten hebben) bij het verzamelen, genereren, analyseren en verspreiden van zowel gestructureerde als ongestructureerde data, data die door mensen worden aangeleverd als ook het benutten van bestaande databases, inclusief beslissingen die worden aangestuurd door geautomatiseerde/kunstmatige intelligentie (AI) met betrekking tot data in het algemeen en persoonlijke data in het bijzonder. Het heeft betrekking op algemene principes waarop onze samenlevingen zijn gebouwd en is zeer relevant voor het opbouwen van vertrouwen en het waarborgen van eerlijkheid.

De ontwikkeling van digitale gezondheid roept legitieme en specifieke vragen en zorgen op over het gebruik van data, beveiliging en soevereiniteit kwesties. Op het gebied van gezondheid is het bijzonder belangrijk om een betrouwbaar kader op te bouwen rond het gebruik van data met het oog op de snelle ontwikkeling van dataficatie in de gezondheidszorg. Het is essentieel om de ontwikkeling van digitale gezondheid in te kaderen met humanistische en burgerlijke waarden, om deze op een concrete manier te implementeren en om de geboekte vooruitgang op een transparante manier aan de burgers te communiceren.

Sommige actoren beschermen of gebruiken data niet op ethische wijze. Veel techplatforms delen bijvoorbeeld data die door hun gebruikers is gegenereerd

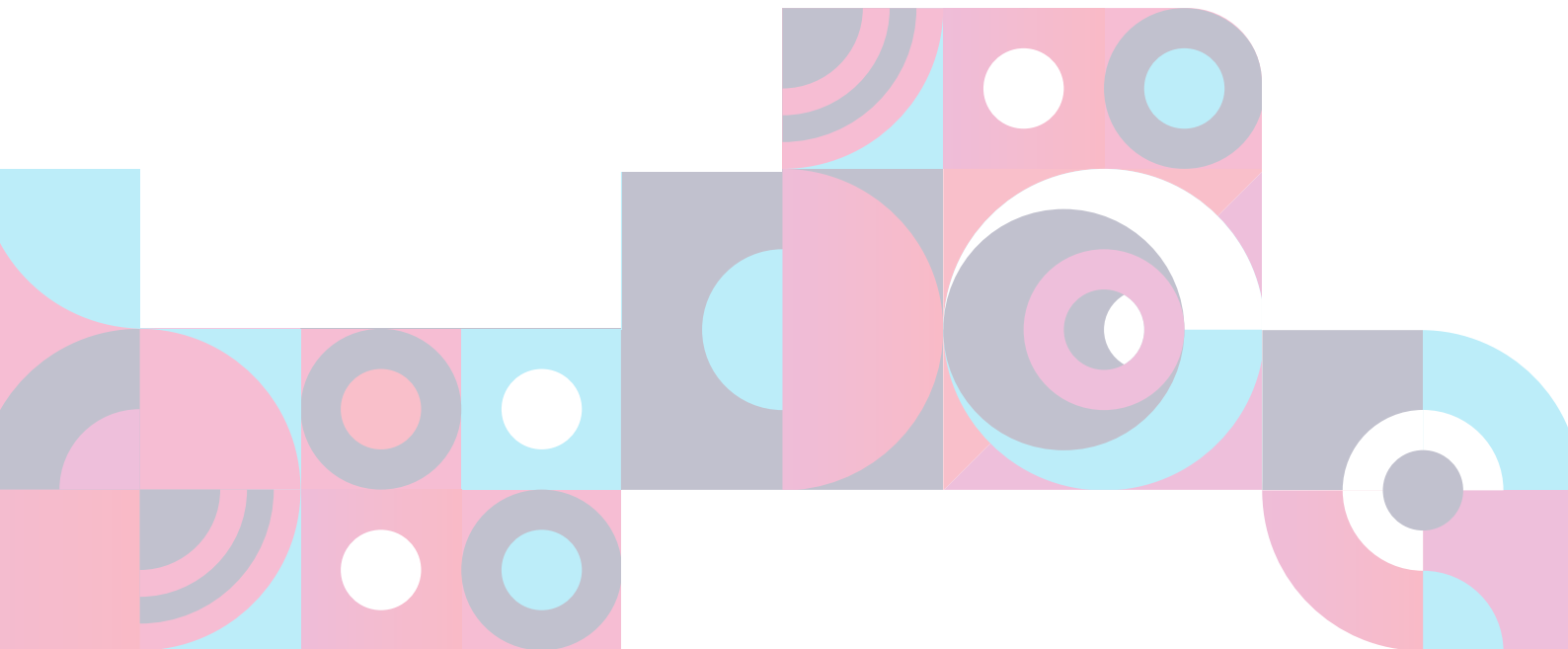
met derden; hun bedrijfsmodel is zelfs gebaseerd op de verkoop van deze data – de verzamelde data gaan veel verder dan persoonlijke data en omvatten het delen van de vriendenlijst van een gebruiker, etc. Veel algoritmen discrimineren tegen minderheden en kwetsbare groepen in de samenleving. Maar bovenal zijn veel actoren nalatig in het naleven van procedures.

Voorstellen voor data governance bevatten doorgaans een verwijzing naar ethische principes, waaronder transparantie, eerlijkheid, verantwoordingsplicht, individuele zeggenschap en data privacy. Overheidsrisico-instanties – zoals NIST, de Amerikaanse organisatie voor technologische normen en DataEthics.eu – hebben richtlijnen gegeven voor praktische toepassing, rekening houdend met mogelijke schade aan mensen, organisaties en systemen. Een belangrijke stap is het invoeren van interne beoordelingsprocessen en -commissies om toezicht te houden op ethische data governance. Er zijn vijf kritieke punten voor de beoordeling van ethische data governance voorgesteld. Bij het onderzoeken van nieuwe projecten

die betrekking hebben op data, moeten bedrijven zich richten op vijf cruciale kwesties, naast privacy: de herkomst van de data, het doel waarvoor ze worden gebruikt, hoe ze worden beschermd, hoe de privacy van de dataleveranciers wordt gewaarborgd en hoe de data worden voorbereid voor gebruik. Er is behoefte aan een overstap van beleidsdiscussies naar praktische technologische ethiek-by-design-oplossingen die deze principes in de praktijk integreren.

Digitale ethiek en data-ethiek staan centraal in datasolidariteit, ook in de zin dat ze benadrukken dat regelgeving met betrekking tot digitale technologieën niet alleen gaat over het beschermen van de privacy of veiligheid van data. Het gaat ook om het beschermen van burgers, klanten en gebruikers tegen data gebruiken van zowel de publieke als de private sector die een negatieve invloed hebben op mensen en de samenleving.

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



4.2 Digitaal humanisme

Beïnvloed door de historische notie van humanisme tijdens de Renaissance en de Verlichting, wordt humanisme tegenwoordig vaak beschouwd als een leidend principe voor menselijke interactie. In de context van digitale praktijken wordt het vaak gebruikt om te verwijzen naar mens machine-interactie die gericht is op het welzijn van mensen en die waarden zoals privacy, waardigheid of solidariteit respecteert.

Wetenschappers en praktijkmensen op het gebied van digitaal humanisme werken aan een reeks vragen zoals: Hoe kunnen humanistische waarden worden vertaald in instrumenten voor het besturen van data gebruiken in de publieke en private sector? Welke eisen moeten bijvoorbeeld gelden voor de toepassing van algoritmische besluitvorming om te voorkomen dat het streven naar technologische efficiëntie en economische groei ten koste gaat van fundamentele mensenrechten? Deze vragen maken de bescherming van mensenrechten tot een cruciaal onderwerp van data governance.

Een voorbeeld hiervan is het Vienna Manifesto on Digital Humanism (2019). Dit document, waaraan wetenschappers en praktijkmensen uit een breed scala aan vakgebieden heeft bijgedragen, definieert digitaal humanisme als het verbinden van humanistische idealen met kritische gedachten over technologische vooruitgang. Het definieert het als een interdisciplinaire benadering voor het begrijpen en vormgeven van het samenspel van technologie en de mensheid voor een betere samenleving. Een digitaal

humanistisch perspectief daagt ook een aantal gangbare veronderstellingen uit, zoals het idee dat geautomatiseerde systemen beter presteren dan menselijke wiskundige en analytische vaardigheden.

Digitaal humanisme verzet zich tegen een dergelijke opvatting van vermeende 'autarkische technologische ontwikkeling'. Digitaal humanisme benadrukt het exclusieve menselijke vermogen om de doelen van computationele probleemoplossende mechanismen te bepalen door de premissen en waarden die erin worden toegepast vorm te geven. Beleidsmakers zouden zich moeten richten op de mogelijkheden die digitale technologieën bieden om de leefomstandigheden van mensen te verbeteren. Met andere woorden, digitaal humanisme verwerpt datagedreven praktijken niet, maar het wil digitale praktijken die worden gebruikt om "mensen de mogelijkheid te geven zich te concentreren op wat essentieel is en bij te dragen aan een meer humane en rechtvaardige toekomst voor de mensheid".

Hoewel datasolidariteit veel gemeen heeft met digitaal humanisme, is het niet beperkt tot humanisme als het gaat om de inhoudelijke waarden waar het zich op baseert. Het is georiënteerd op een breder scala aan waarden zoals gelijkheid, rechtvaardigheid en, natuurlijk, solidariteit.

Referenties: 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 discriminatie

Data discriminatie is een van de schadeposten in digitale samenlevingen die datasolidariteit wil voorkomen. Nu er elke dag enorme hoeveelheden data worden gegenereerd, worden steeds meer beslissingen - ook in de gezondheidszorg - beïnvloed door data-analyses en algoritmen. Deze situatie wordt nog verergerd door het gebruik van generatieve AI op steeds bredere terreinen van het leven en werk. Ondanks de vaak veronderstelde neutraliteit van technologie, kunnen AI systemen discriminerende effecten hebben wanneer ze worden gebruikt voor het nemen van beslissingen. In Europa benadrukt de General Data Protection Regulation (GDPR) de noodzaak om discriminatie als gevolg van geautomatiseerde besluitvorming te voorkomen en geeft het mensen het recht op 'zinvolle informatie' over de logica die ten grondslag ligt aan geautomatiseerde besluiten.

Er is sprake van data discriminatie wanneer individuen of groepen oneerlijk worden behandeld vanwege kenmerken of eigenschappen die zijn geïdentificeerd door het verzamelen en analyseren van hun data. De introductie en toepassing van big data vindt plaats binnen de context van historische ongelijkheid in gezondheid en gezondheidszorg - de discriminatie kan voortkomen uit de databronnen die worden gebruikt om AI-systemen te trainen, de manier waarop de systemen worden gebruikt en de manier waarop ze zijn ontworpen. Dit kan leiden tot het bestendigen van sociale ongelijkheid en het creëren van nieuwe patronen van discriminatie in de gezondheidszorg, bijvoorbeeld op basis van leeftijd, geslacht, etniciteit, religie, seksuele voorkeur of

genetisch materiaal kenmerken. Zorgen met betrekking tot ethiek, eerlijkheid, billijkheid en transparantie bij de ontwikkeling van big data tools moeten worden aangepakt. Dit kan het beste gebeuren door betrokkenheid van en open communicatie met belanghebbenden. In het geval van de gezondheidszorg staat er bijzonder veel op het spel, aangezien het leven en de gezondheid van gemarginaliseerde en achtergestelde groepen in gevaar kunnen komen.

Structurele ongelijkheden, vooroordelen en racisme in de samenleving worden gemakkelijk gecodeerd in datasets en in de toepassing van datawetenschap. Wanneer deze data worden gebruikt om software te trainen, wordt de vooringenomenheid gerepliceerd. Het is daarom belangrijk om de lage diversiteit in de wetenschap van gezondheidsdata en de competenties van data stewards (de mensen die verantwoordelijk zijn voor het beheer van en het toezicht op de data van een organisatie) te vergroten, zodat datasystemen groepen niet oneerlijk discrimineren, al dan niet opzettelijk. De AI wet van de Europese Unie bevat een bepaling die organisaties in staat stelt om speciale datacategorieën te gebruiken voor het auditen van hun AI systemen om ervoor te zorgen dat ze niet discrimineren.

Datasolidariteit onderschrijft het doel om data discriminatie te bestrijden. In bredere zin wil het ervoor zorgen dat alle schade - niet alleen discriminatie - en alle voordelen eerlijker worden verdeeld over en binnen samenlevingen.

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

4.4 Data extractie

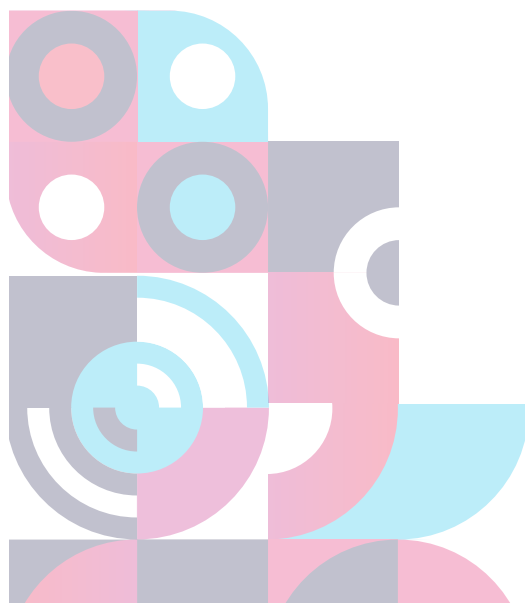
Data extractie verwijst naar het proces van het verzamelen of ophalen van verschillende soorten data uit verschillende bronnen, waarvan er veel slecht georganiseerd of volledig ongestructureerd kunnen zijn, om ze vervolgens toe te passen voor analytische verwerking voor specifieke doeleinden, bijvoorbeeld marketing. Dit wordt web scraping genoemd met databronnen zoals gebruik van sociale media, gedragsregistratie, webpagina's, e-mails en een breed scala aan documenten. Data extractie in onderzoek omvat het verzamelen en ophalen van relevante data uit verschillende bronnen voor analyse, interpretatie en het afleiden van conclusies.

Het extraheren van patronen uit grote hoeveelheden ongestructureerde data wordt datamining of data analytics genoemd. Steeds vaker gebeurt dit via methoden zoals kunstmatige intelligentie en machinaal leren, zowel voor winst als voor het gebruik van algoritmes ten behoeve van de uitvoer van beleid en publiek bestuur. In de gezondheidszorg speelt data extractie een steeds belangrijkere rol in patiëntenzorg en voorspellende geneeskunde, evenals in medisch onderzoek. De vraag naar betrouwbare gezondheidsinformatie nam bijvoorbeeld aanzienlijk toe tijdens de COVID-19-pandemie. Veel gezondheidssystemen konden echter niet zorgen voor de stroom van noodzakelijke data en informatie tussen zorgverleners en volksgezondheid instanties, waardoor het moeilijk werd patronen te ontdekken en deze te interpreteren om bruikbare inzichten te verkrijgen. Data extractie levert dus commerciële en andere voordelen op, maar brengt ook risico's met zich mee. Het centrale doel van datasolidariteit is ervoor te zorgen dat deze voordelen en risico's eerlijker worden verdeeld dan nu het geval is.

Zoals bij alle vormen van datagebruik, roept data extractie vragen op over privacy, ethiek, politiek en ernstige juridische kwesties. Dit is het geval geweest in verschillende programma's die algoritmisch bestuur hebben toegepast op het welzijnssysteem. Het samenvoegen en combineren van data kan de analyse vergemakkelijken, maar kan ook de identificatie van data op individueel niveau mogelijk maken, zelfs als de data oorspronkelijk anoniem waren, wat kan leiden tot datalekken. Het kan ook nieuwe vormen van uitbuiting inhouden wanneer data worden geanalyseerd en te gelde gemaakt zonder toestemming of zelfs medeweten van de mensen van wie de data afkomstig zijn - ten gunste van actoren die winst maken. Dit vergroot de macht asymmetrie tussen betrokkenen (de mensen die hun data delen) en organisaties die data gebruiken, waarbij de laatste veel meer mogelijkheden hebben om economisch voordeel te halen uit de data en de eerste bijna alle risico's dragen.

Datasolidariteit streeft ernaar de risico's van data extractie te verminderen. Het probeert er ook voor te zorgen dat de resterende risico's en de voordelen die voortvloeien uit het extraheren, gebruiken en hergebruiken van data eerlijk worden verdeeld binnen en tussen samenlevingen.

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



4.5 Data kolonialisme

Data kolonialisme heeft als doel een ontwikkeling vast te leggen die niet langer wordt gedefinieerd door de winning van natuurlijke hulpbronnen of arbeid, maar is gebaseerd op de toe-eigening van menselijk leven door middel van data.

Het begrip data kolonialisme omvat alle digitale praktijken waarbij individuen en gemeenschappen (zoals inheemse volkeren en gemeenschappen) gemarginaliseerd of onteigend worden door de extractie, controle en het gebruik van hun data door machtigere actoren, zowel privé als publiek, uit winstbejag of voor politieke controle. Dit proces heeft veel kenmerken gemeen met de koloniale winning van hulpbronnen gekoppeld aan territoriale veroveringen.

Data kolonialisme werkt op vele niveaus. Het beïnvloedt gebruikers via de gebruiksvoorwaarden waarmee ze instemmen voor hun online interacties en de manieren waarop data over hun dagelijkse activiteiten worden gebundeld en te gelde gemaakt. Het verwante concept van surveillance kapitalisme analyseert de manieren waarop menselijke gedragingen, lichamen en omgevingen worden veranderd in een bron die wordt omgezet in data en dus in winst. Generatieve AI kan data kolonialisme bestendigen door data te onttrekken aan makers van inhoud zonder eerlijke compensatie, waardoor de controle en voordelen in de handen van een paar mensen komen en de wereldwijde ongelijkheid toeneemt.

Een ander extractief proces is het globaal vastleggen van data - data van iedereen, overall - waar nog geen serieus mondiaal bestuur op heeft gereageerd. We hebben

nog niet voldoende rekening gehouden met de impact van nieuwe data methoden en -systemen die gebaseerd zijn op het Global North en die worden geïntroduceerd en versterkt door mondiale instellingen – bijvoorbeeld de Statistische Commissie van de VN – zonder voldoende aandacht te besteden aan nationale en lokale contexten. Data vormen de basis voor internationale rapportage over ontwikkelingsvoortgang, zoals de Duurzame Ontwikkelingsdoelen en definiëren de toewijzing van middelen. De toenemende afhankelijkheid van data uit deze processen voor besluitvorming verergert het probleem: verschijnselen en factoren die niet kunnen worden gemeten en weergegeven in de vorm van data zijn onzichtbaar voor beleidsmakers.

Geloofwaardige en betrouwbare data zijn bijzonder relevant voor de wereldwijde gezondheid - vooral tijdens uitbraken en pandemieën. Landen moeten volledig kunnen vertrouwen op de mechanismen voor het delen van data en vooral op de waarde ervan voor lage- en middeninkomenslanden in het licht van grote ongelijkheid. De WHO heeft voorgesteld om wereldwijde gezondheidsdata te behandelen als een publiek goed, maar datasolidariteit is nog niet geaccepteerd als aanpak. Er zijn ook zorgen geuit met betrekking tot wereldwijde rapportagevereisten zoals het Global Burden of Disease Report, omdat het macht overdraagt van instellingen in lage-inkomenslanden naar instellingen in hoge-inkomenslanden, de ontwikkeling van nationale gezondheidsinformatiesystemen belemmert en bepaalde vormen van kennis boven andere bevoorrecht.

Referenties: Birch, 2023; IHME, undated; Kim et al., 217; Mitchell, 2021; Shiffman & Shawar, 2020; Universität Bern, 2021; Zuboff, 2019.



Section 5: Vooruit kijken

5.1 Digitale transformatie van de zorg

Digitale technologieën en kunstmatige intelligentie (AI) vormen nu de kern van gezondheid - niet in de laatste plaats omdat ze alomtegenwoordig zijn in het dagelijks leven. In 2021 publiceerden The Lancet en de Financial Times Commissie een dringende oproep aan beleidsmakers op het gebied van gezondheid en digitaal beleid om ervoor te zorgen dat digitale transformaties worden ingegeven door publieke waarde in plaats van particuliere winst en de missies van volksgezondheid, universele gezondheidszorg en gezondheid voor iedereen ondersteunen. De commissie stelde voor om de term digitale gezondheid alleen te gebruiken voor duidelijk gedefinieerde toepassingen in gezondheid en geneeskunde en om inzicht te ontwikkelen in de bredere impact van digitale technologieën. Ethische

perspectieven op digitale transformaties in de gezondheidszorg vereisen een uitbreiding van bio-ethiek naar socio-technische ethiek die de bredere impact van technologieën op gezondheid en gezondheidszorg beoordeelt.

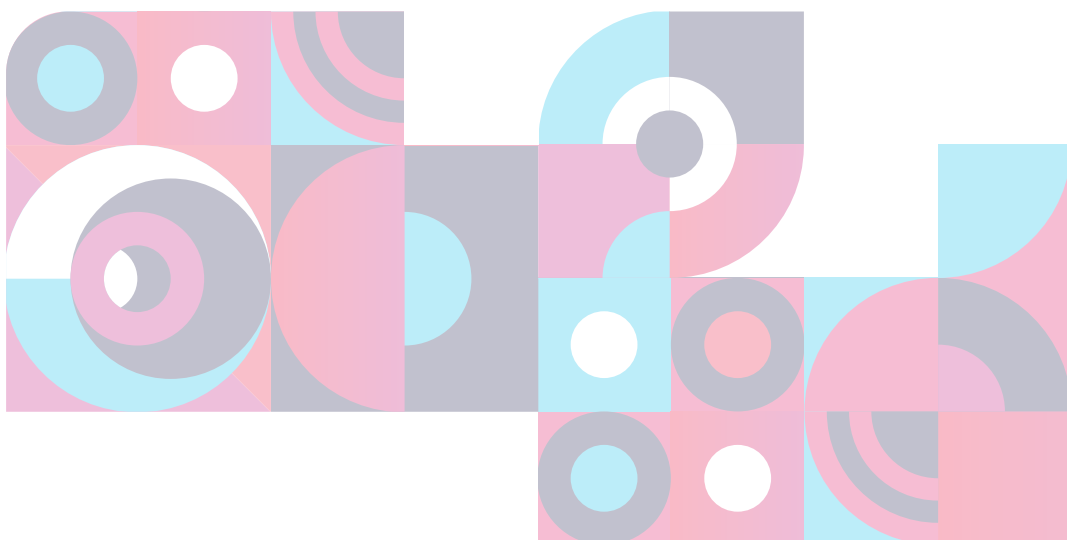
Digitale transformaties zijn determinanten die in wisselwerking staan met grotere politieke, maatschappelijke en economische dynamieken. Ze zullen steeds meer het dominante prisma worden waardoor we denken over gezondheid en welzijn, aangedreven door de dataficatie van gezondheid, inclusief AI en datagestuurde analyses binnen genomica. Geneeskunde is altijd gedreven geweest door wetenschappelijke doorbraken en technologische innovatie. Maar de aard van de technologie, gekoppeld aan de mate van

convergentie die we nu zien en de snelheid van verandering, zijn ongekend. Er is ook een toenemende convergentie tussen digitale transformaties en volksgezondheid, versterkt door de COVID 19 pandemie. De pandemie liet zien hoe gezondheid, data en de kracht van digitale connectiviteit over grenzen gaan, maar tegelijkertijd bestaande ongelijkheden en discriminaties versterken. De pandemie benadrukte ook de invloed van de grote, wereldwijde digitale aanbieders en platforms, waarvan velen al snel de gezondheidszorg betraden en nu steeds relevanter werden.

De grenzen van digitale transformaties in de gezondheidszorg worden steeds sneller verlegd, vaak zonder rekening te houden met de gevolgen voor de rechtvaardigheid op gezondheidsgebied en de mensenrechten. De snelle toegang tot realtime informatie en de intensiteit van het digitale debat vereisen voortdurende waakzaamheid en actualisering.

Zonder inzet voor solidariteit, rechtvaardigheid en nieuwe vormen van digitaal gezondheidsburgerschap, zou gezondheid een bevoorrechte toegangspoort kunnen worden ter ondersteuning van nieuwe vormen van surveillance kapitalisme, data kolonialisme of digitale welzijns dystopieën. (Zie [4.5 Data kolonialisme](#)) Na een massale toename van surveillance tijdens de pandemie zijn we nu al getuige van dergelijke ontwikkelingen in verschillende landen over de hele wereld. De meest uitdagende dimensie van de extreme onbalans in wie profiteert van de digitale transformatie is wat Shoshana Zuboff 'surveillance kapitalisme' heeft genoemd. Datasolidariteit streeft naar het maximaliseren van de waarde die gezondheidsdata en andere digitale data creëren voor het publiek, maar niet ten koste van mensen en gemeenschappen.

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





5.2 Vertrouwen in data en platformen

The Lancet en *Financial Times* Commissie heeft gesteld dat het opbouwen van vertrouwen tussen alle belanghebbenden van het digitale gezondheid ecosysteem een van de meest urgente gebieden is voor actie, aangezien omgevingen met weinig vertrouwen risicovolle omgevingen zijn voor de gezondheid. Datasolidariteit, een benadering van data governance die streeft naar een eerlijker verdeling van de voordelen en risico's van digitale praktijken, kan helpen om vertrouwen op te bouwen in data gebruiken.

Data kunnen een kwestie van leven of dood zijn in een gezondheidscrisis - ze vormen ook een reeks van uitdagingen op het gebied van ethiek en mensenrechten. We zagen tijdens COVID 19 hoe het ontbreken van data over de etnische achtergrond van mensen die kritisch ziek worden met COVID, leidde tot ongeoorloofde verschillen in gezondheidsresultaten. Het gebrek aan geharmoniseerde normen voor dataverzameling maakte vergelijking van epidemiologische informatie tussen landen onnodig lastig. Misinformatie over gezondheid is een ander bekend gevolg van slechte data governance. Omdat mensen het gevoel hadden dat ze geen toegang kregen tot diensten of betrouwbare informatie, ging hun vertrouwen in bestaande systemen en informatiebronnen verloren.

Zorgen over privacy, veiligheid en schendingen van rechten dragen bij

aan een gebrek aan vertrouwen tussen gemeenschappen, gezondheidswerkers en andere groepen. Dit beperkt de toepassing van potentieel nuttige innovaties en het delen van data en oplossingen tussen mensen, landen en digitale gezondheidsactoren - en leidt tot een gebrek aan op feiten gebaseerde besluitvorming voor de gezondheid.

Maar zonder vertrouwen - tussen mensen, instellingen en naties - om data te delen op lokaal, nationaal, regionaal en mondiaal niveau, zal de samenleving niet kunnen profiteren van de enorme hoeveelheden gezondheidsdata die er zijn om de gezondheid, de gezondheidszorg en de besluitvorming te verbeteren. Innovaties met de mogelijkheden om de doelen van de volksgezondheid te bevorderen blijven zo beperkt.

Zoals opgemerkt, is solidariteit op het gebied van data een manier om het vertrouwen te vergroten - niet door het van mensen te eisen of het belang ervan te benadrukken, maar door de echte betrouwbaarheid van het gebruik van data te vergroten. Door ervoor te zorgen dat bijzonder riskant datagebruik wordt verboden en deze verboden effectief worden gehandhaafd en door maatregelen te introduceren om schade te beperken, proberen ze mensen effectiever te beschermen dan voorheen het geval was. Bovendien probeert datasolidariteit ook ongelijkheid op mondiaal niveau aan te pakken.

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

5.3 Dataficering van zorg

Dataficatie transformeert verschillende aspecten van ons leven en onze gezondheid in (vaak) grote hoeveelheden data die kunnen worden verzameld, opgeslagen, geanalyseerd, gedeeld en gebruikt om inzichten te verkrijgen en AI te trainen. Op het gebied van de gezondheidszorg heeft dataficatie het klinisch onderzoek en de ontwikkelingsprocessen voor medicijnen veranderd. Het ondersteunt zorgprofessionals bij het nemen van geïnformeerde beslissingen en het personaliseren van zorg, maakt de analyse mogelijk van geaggregeerde en ongeïdentificeerde gezondheidsdata voor bevolkingsonderzoek en bewaking van de volksgezondheid. Dataficatie kan een rol spelen bij het verbeteren van de patiëntenzorg en het vergroten van de efficiëntie in gezondheidszorgsystemen. De toenemende dataficatie van ons leven en onze omgeving is een belangrijke reden waarom datasolidariteit nodig is.

Een doorbraak in dataficatie is gekomen met de introductie van draagbare apparaten die gebruikers kunnen helpen hun vooruitgang te monitoren, patronen te identificeren, afwijkingen te detecteren en op data gebaseerde beslissingen te nemen over hun gezondheid en welzijn, gebaseerd op real-time feedback. Dit wordt door sommigen ook met zorg bekeken, omdat het betekent dat kwalitatieve aspecten van gezondheid en welzijn worden omgezet in gekwantificeerde data. Mensen - die foto's maken en calorieën en andere data van hun maaltijden registreren - leggen een belangrijk aspect van hun gezondheid vast dat voorheen niet werd geregistreerd. Terwijl patiënten vroeger met hun eigen stem verslag deden van deze aspecten van hun leven, vertellen hun data nu het verhaal. Bovendien zijn veel soorten data zeer gevoelig zijn, wat betekent dat ongeoorloofd gebruik door derden veel schade kan aanrichten, variërend van het verlies van toegang

tot (privé)gezondheid en andere data, tot het verlies van de toegang tot het zorgverzekeringen tot, in extreme gevallen, verlies van banen en ernstige sociale stigmatisering. Bovendien kunnen zelfs onschuldige datareeksen, wanneer ze gekoppeld worden aan andere datareeksen, leiden tot conclusies over individuen die kunnen leiden tot discriminerende of andere schadelijke acties. Soms komt dit doordat de algoritmes die worden gebruikt voor data analyse problematische vooroordelen weerspiegelen; soms komt dit doordat bestaande wetten en beleid mensen onvoldoende beschermen tegen de schade van voorspellende analyses en andere analyses. Dit is niet alleen een probleem in het bedrijfsleven, maar in sommige landen ook in de publieke sector waar voorspellende analyses zijn gebruikt ten nadele van mensen. Het Robodebt-schandaal in Australië en het Nederlandse toeslagenschandaal illustreren belangrijke problemen met het gebruik van data door overheidsinstanties, met ernstige gevolgen voor de getroffen individuen.

Tegen deze achtergrond streeft datasolidariteit, naast databeveiliging en privacy, ervoor te zorgen dat mensen voldoende controle hebben over data waar ze belang bij hebben. Dit houdt ook in dat mensen zeggenschap krijgen - individueel of als onderdeel van gemeenschappen waartoe ze behoren - over welke soorten kennis en informatie überhaupt mogen worden gedataficeerd. Datasolidariteit probeert er ook voor te zorgen dat commerciële winsten die worden behaald met data van mensen eerlijk worden gedeeld met gemeenschappen.

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

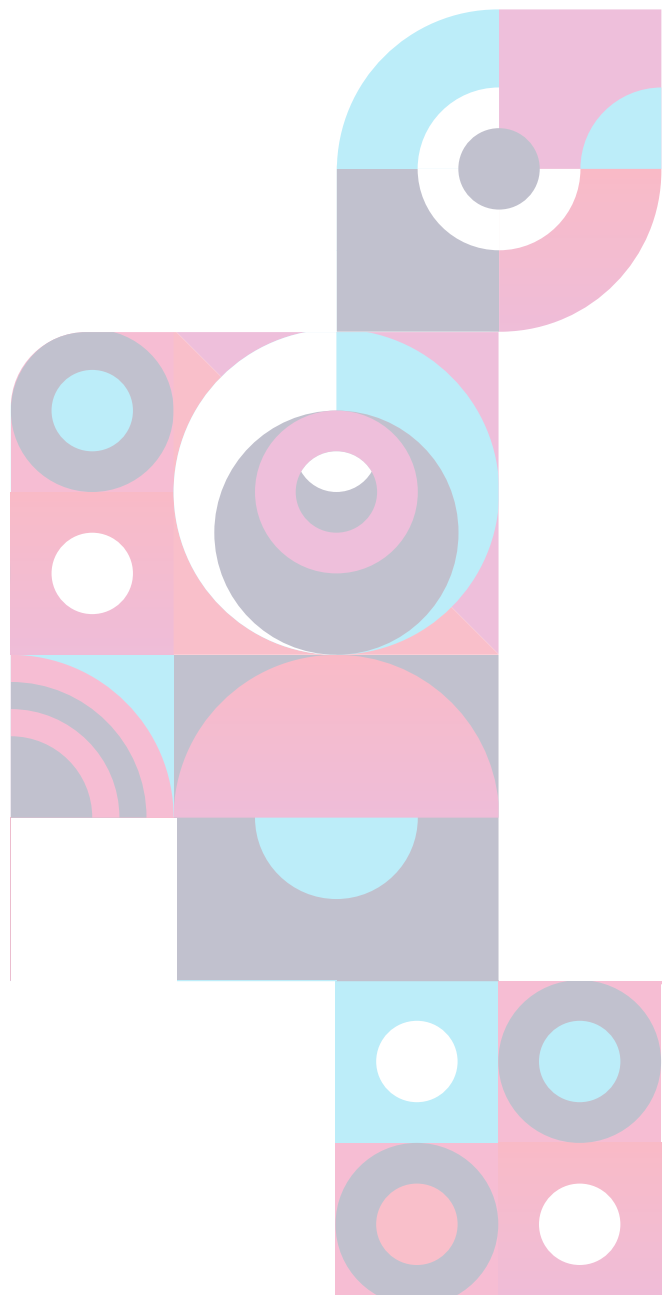
5.4 Digitale gezondheidsvaardigheden

Algemene gezondheidsvaardigheden worden al lang gezien als een belangrijke determinant van gezondheid - een lage gezondheidsvaardigheid vormt een groot risico voor de gezondheid. Naarmate de digitale transformatie vordert, hebben digitale geletterdheid en digitale gezondheidsvaardigheden ook aan relevantie gewonnen, vooral bij het aanpakken van de digitale kloof op gezondheidsgebied. Omdat ongelijkheden in digitale toegang en digitale geletterdheid van invloed zijn op de toegang van mensen tot gezondheidsinformatie en gezondheidsdiensten, zijn ze van invloed op de gezondheidsresultaten. We weten dat de vraag naar digitale basisvaardigheden en geavanceerde digitale vaardigheden voor patiënten en zorgverleners aanzienlijk zal toenemen naarmate zorgorganisaties meer gebruik gaan maken van digitale technologieën, waaronder kunstmatige intelligentie. Maar uit een rapport over digitale gezondheid van de Europese regio van de WHO blijkt dat maar heel weinig landen actief investeren in digitale gezondheidsvaardigheden. Dit zal leiden tot toenemende problemen en ongelijkheden - bijvoorbeeld als gevolg van aanzienlijke demografische verschuivingen.

Een nuttige benadering van de vele dimensies van digitale gezondheidsvaardigheden is het transactionele model van e-health vaardigheden dat vier competentieniveaus voor digitale gezondheidsvaardigheden schetst: functioneel, communicatief, kritisch en translationeel. In de context van datasolidariteit zijn kritische digitale gezondheidsvaardigheden van bijzonder belang omdat ze verwijzen naar het “vermogen om de relevantie, betrouwbaarheid en risico’s te beoordelen van het delen en ontvangen van gezondheidsgelateerde informatie via het digitale ecosysteem”. Maar er is ook

een zeer belangrijke component van communicatieve gezondheidsvaardigheden die is vervat in het begrip “civiele geletterdheid”- het richt zich op de kennis en het vermogen om deel te nemen en verwijst naar hoe mensen communiceren in digitale contexten en hoe bewust ze zijn van hun rechten en verantwoordelijkheden in het digitale ecosysteem. Digitale gezondheidsvaardigheden zijn daarom van groot belang voor het uitoefenen van digitaal gezondheidsburgerschap. (Zie [5.5 Digitale gezondheidsburgerschap](#))

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.



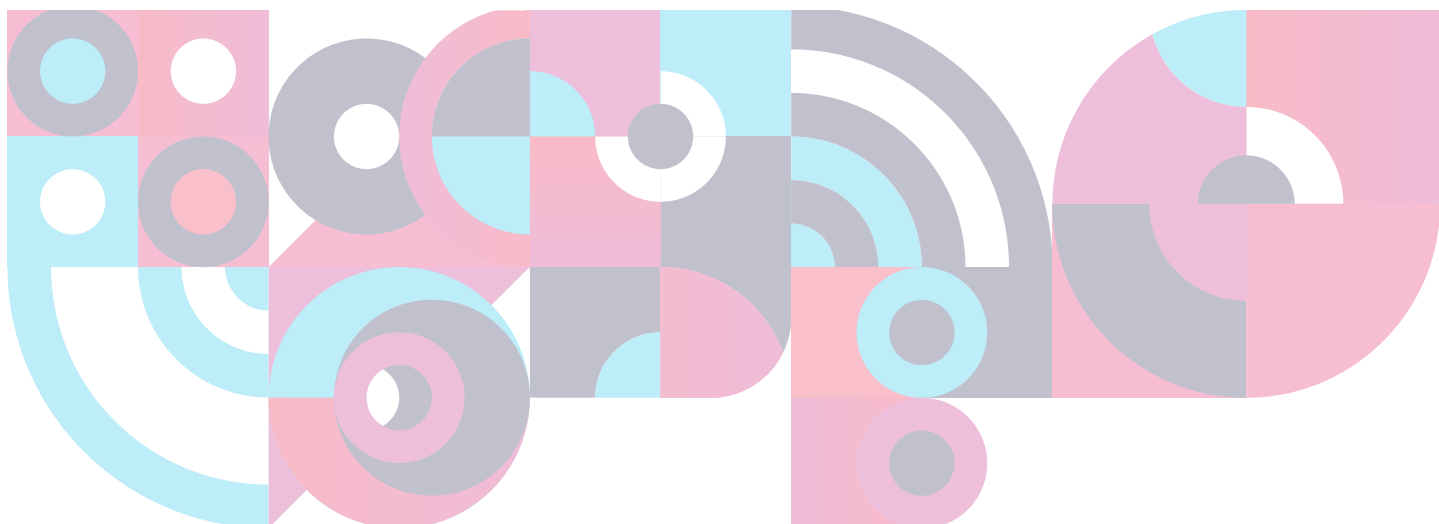
5.5 Digitale gezondheidsburgerschap

Digitaal gezondheidsburgerschap definieert niet alleen een reeks rechten en verantwoordelijkheden die ontstaan door het gebruik van digitale technologie (bijv. gezondheidsapps en -platforms) voor gezondheidsgelateerde doeleinden, maar ook het proces en de vormen van interactie en participatie die ontstaan in de digitale gezondheidsruimte.

Er is een sterke behoefte aan data governance die democratischer is en zorgt voor gelijke toegang tot middelen. Individuen en groepen moeten in staat zijn om actief deel te nemen aan en mee te werken aan het ontwerp en de implementatie van beleid en technologieën op het gebied van digitale gezondheid en om feedback te geven aan besluitvormers, ontwikkelingsinstanties, particuliere bedrijven en ontwikkelaars. Hierbij gaat het onder meer om kaders voor gelijkheid bij de ontwikkeling van technologie en digitale ruimtes, en om het vergroten van de veerkracht van gemeenschappen

tegen de negatieve gevolgen van digitale transformaties. Een op waarden gebaseerde en mensgerichte benadering van het besturen van digitale transformaties voor de gezondheid bouwt voort op digitaal gezondheidsburgerschap om tegenwicht te bieden aan wat surveillance kapitalisme is genoemd.

Het digitale ecosysteem is afhankelijk van de deelname van zijn gebruikers - het werkt alleen als patiënten en anderen bereid zijn om hun data bij te dragen. Het zou gebruikers beschermen tegen het extraheren van hun data en de voortdurende algoritme-aanpassingen die de drijvende kracht vormen achter online gedrag. Het digitale ecosysteem biedt nieuwe ruimten voor politieke participatie en maatschappelijk debat, ook over gezondheidskwesties. Maar eerlijke gezondheidsvoordelen kunnen alleen worden gerealiseerd als burgers zich kritisch kunnen opstellen, zich beschermd voelen tegen verkeerde informatie en discriminatie en weloverwogen keuzes kunnen maken met betrekking tot hun data. Participatieve data governance moet een bepalend kenmerk zijn van het 21e-eeuwse digitale gezondheidsburgerschap. Dit kan betekenen dat, waar data over het lichaam van mensen of zeer persoonlijke aspecten van hun leven betreft, mensen rechtstreeks inspraak hebben in hoe de data worden



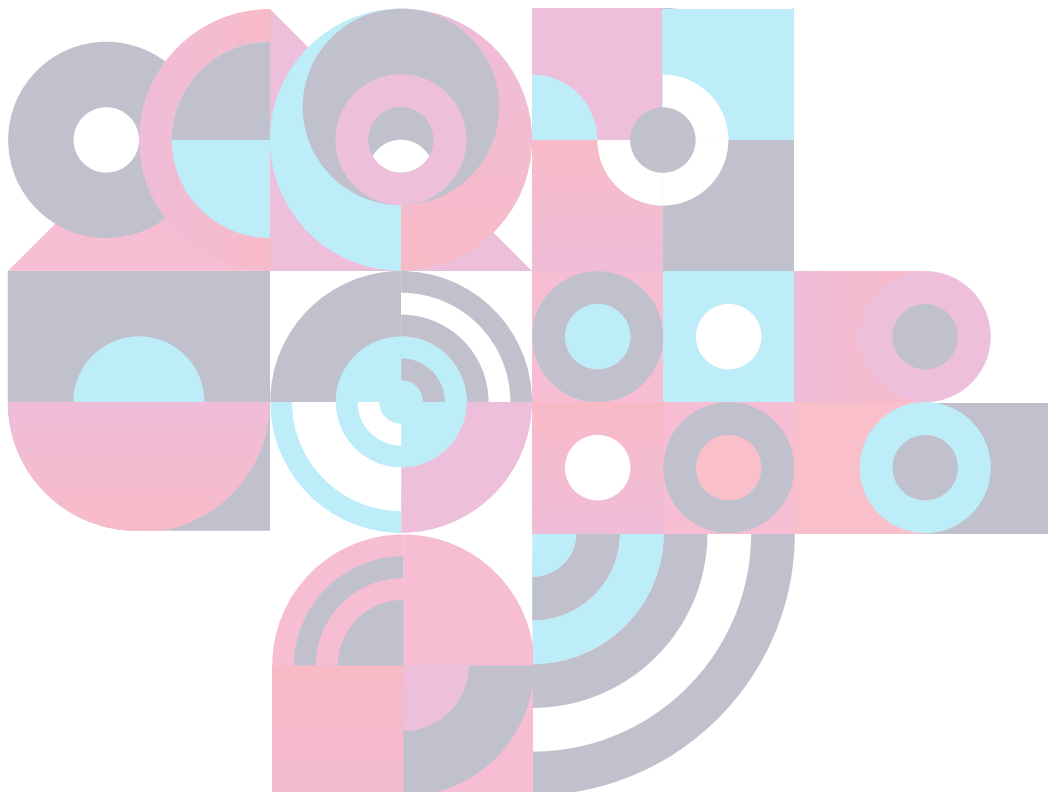
gebruikt. De datasolidariteit benadering stelt ook voor om meer gebruik te maken van collectieve vormen van toezicht en het versterken van geïnstitutionaliseerde solidariteit. Maar tot nu toe hebben nog maar weinig regeringen gewerkt aan het versterken van de democratische en solidariteitsprikkels en voordelen van het ecosysteem voor digitale gezondheid.

Onderzoek naar het nieuwe 'digitale gezondheidsburgerschap' toont de bereidheid van mensen om informatie, ervaringen en data te delen - maar vaak weten ze niet of ze dit doen op een openbaar of non-profit platform of op een commercieel platform en welke rol algoritmen spelen bij het maken van hun keuzes en wat er gebeurt met de data die ze delen. Digitaal gezondheidsburgerschap vereist competenties op het gebied van gezondheidsvaardigheden, digitale geletterdheid en bredere democratische vaardigheden. en civiele geletterdheid. Civiele technologie-modellen, die in het algemeen verwijzen naar de co-creatie (tussen gebruikers, tech

ontwikkelaars, enz.) en het gebruik van digitale technologieën om de deelname van het publiek aan democratische en besluitvormingsprocessen te verbeteren, worden steeds meer gezien als een middel om het overheidsbeleid en de dienstverlening te verbeteren, ook in de gezondheidszorg.

Actief digitaal gezondheidsburgerschap wordt vaak beperkt door de digitale kloof. De ongelijkheid wordt versterkt; het zijn vaak dezelfde mensen en gemeenschappen die geen internetverbinding hebben, die laaggeletterd zijn en die de minste toegang hebben tot hoogwaardige gezondheidszorg. Collaboratieve bestuursmodellen die verschillende sectoren - publiek en privaat - samenbrengen, moeten ook dergelijke gemeenschappen omvatten om de daaruit voortvloeiende rechtvaardigheidsproblemen aan te pakken.

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



Bibliografie

- Adecco Group. (2023). *Understanding Digital Justice: How Can We Fight for Fair Technological Practices*. [Online] <https://www.adeccgroupp.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). *Informational 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](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](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*, 135104861. <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., Leshner, 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. *Perspect 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](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](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>

Szozskiewicz, 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. & Mascalonzi, 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>

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

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/gsdhdaa2a9f352b0445bafbc79ca799dce4d.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