Check for updates

Original Research Article

Governing artificial intelligence means governing data: (re)setting the agenda for data justice

Dialogues on Digital Society
1–18
© The Author(s) 2025

Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/29768640241306800
journals.sagepub.com/home/dds


Linnet Taylor
TILT, Tilburg University, the Netherlands

Siddharth Peter de Souza #
TILT, Tilburg University, the Netherlands

Aaron Martin
University of Virginia, USA

Joan López Solano
TILT, Tilburg University, the Netherlands

Abstract

The field of data justice has been evolving to take into account the role of data in powering the field of artificial intelligence (AI). In this paper we review the main conceptual bases for governing data and AI: the market-based approach, the personal–non-personal data distinction and strategic sovereignty. We then analyse how these are being operationalised into practical models for governance, including public data trusts, data cooperatives, personal data sovereignty, data collaboratives, data commons approaches and indigenous data sovereignty. We interrogate these models' potential for just governance based on four benchmarks which we propose as a reformulation of the Data Justice governance agenda identified by Taylor in her 2017 framework. Re-situating data justice at the intersection of data and AI, these benchmarks focus on preserving and strengthening public infrastructures and public goods; inclusiveness; contestability and accountability; and global responsibility. We demonstrate how they can be used to test whether a governance approach will succeed in redistributing power, engaging with public concerns and creating a plural politics of AI.

Keywords

Data justice, artificial intelligence governance, data commons, data trusts, data protection, data governance, indigenous data sovereignty, data sovereignty

Introduction

The field of data justice has since its emergence focused primarily on surfacing the risks of datafication for rights and social justice (Dencik et al., 2016; Gangadharan et al., 2018; Taylor et al., 2023). However, over the last decade the rhetoric of 'data'

Siddharth Peter de Souza is currently affiliated with the University of Warwick, and the University of Johannesburg. He was previously affiliated with TILT, Tilburg University.

Corresponding author:
Linnet Taylor, TILT, Tilburg University, Tilburg, the Netherlands.
Email: l.e.m.taylor@tilburguniversity.edu

as a source of power and hierarchy has evolved into artificial intelligence (AI). This still-loosely-defined object is both a rhetorical device allowing the branding and marketing of particular data systems as new phenomena, and an assemblage that relies on data, and specifically statistical modelling using data (Aradau and Blanke, 2015; Kitchin, 2014). It also, however, denotes a particular category of political, commercial and social interventions that are related to, but do not map perfectly onto, the power and problems of data. 'AI' has come to involve additional levels of material and cloud infrastructures beyond those that shaped the power of datafication (Gürses et al., 2020; Gürses and Van Hoboken, 2017). It has also come to denote classes of statistical models which take the formalisations of social complexity that datafication has provided a step further. These models' defining characteristic is their optimisation of private and public sector operations, from social media to welfare systems, for particular interests. 'AI' is 'big data' *in motion*: it adds new layers of actors and interests, offers new ways of structuring the power and financial benefits of data, and by doing so, aggregates and shapes the power to intervene (European Parliament, 2022).

There is a debate about how the purpose of data governance is changing with the growth of an AI economy. Much of the data protection, business and public administration scholarship argues that the role of data governance is to provide a legally compliant, reliable and accessible basis for 'trustworthy AI' (Díaz-Rodríguez et al., 2023; Janssen et al., 2020; O'Hara and Hall, 2018). Information systems research has gone further to propose that AI should be used to perform and organise data governance (Yandrapalli, 2024). In contrast, Morozov, among other critical scholars, has argued that targeting data as the focus of governance is a mistake because it diverts attention from governing AI as a source of political and economic domination (Morozov, 2023).

Both positions make important points. While the AI field presents a new layer of challenges for technology governance, it also requires rethinking of the governance of data as an essential condition for AI's political and economic power. AI supercharges the risks of datafication by making categorisation and sorting simultaneously more dynamic and more probabilistic, and by integrating these capacities into the backgrounds of everyday systems – that is, part of (digital) infrastructures. The growth of the sector and its economic promise have placed industry as central to governance discussions, de-emphasising governing for individual rights and for the legitimacy of technological intervention (Taylor, 2021). The shift has also led to a new imperative to maximise data collection and data flows, which categorically conflicts with data protection's core ethos of minimisation and purpose limitation. This claim is made more urgent by the business strategy of embedding AI into existing platforms and services on which many sectors already rely, thus enlisting the users of those services as producers and consumers of AI-based services and also as providers of ongoing data streams for AI training models. Together, these strategies have defined a new level of infrastructural power and dominance that are shaping the global landscape of technology. This dominance also poses a new set of questions for those interested in promoting just modes of governing the data that forms the basis for the AI economy: how can the power to govern be (re)distributed to those affected? What constitutes just governance at the intersection of data and AI? And how can the hierarchies and concentrations of power created by the AI economy be contested?

This paper argues that data's evolution into the field of AI brings with it new potential for commercial and political domination, with implications for the capture of public goods and the marketisation of the public sphere. For these reasons, even though the field of data governance has largely transformed into the field of AI governance, it is even more important to think about how to govern data in line with social justice. The connections between data and AI governance are clearly visible in the current scramble for data: the field of AI governance features debates about intellectual property in relation to large datasets (Appel et al., 2023), 'data spaces' and data stewardship (Calzada, 2019; Purtova and van Maanen, 2023), and control over how everyday data flows into AI models (or does not) (Brittain, 2023), among

many others. AI models, and advanced AI models in particular, are made of data. The proposal to train generative AI models on synthetic datasets either generated or shaped by other AI models does not yet convince technical specialists (Shumailov et al., 2023) due to the threat of 'poisoning' the destination models with data that has no reference point in ground truth, eventuating their collapse.

We address 'AI' as both an economic and epistemic imaginary that is being used to brand states' development strategies and to exert claims of sovereignty and hegemony on the diplomatic level, and a real commercial power that is bringing together corporate and state interests on the national and international levels. As such, its governance deserves to be carefully constructed and continually interrogated as a determinant of private power. We make the case that for data, and by extension AI, to be governed in the interests of those they represent (de Souza and Taylor, forthcoming), we must examine the notion of publicness, and how to better define it given the threats posed by the AI economy.

Our analysis focuses centrally on governance: by this we mean the whole political and commercial landscape of power in relation to data and AI, including how it is claimed, acquired and negotiated among different actors. We envisage data as the basis for the power of AI, and as the primary challenge that many nations are still dealing with. At the same time, the richest states are negotiating power over data from the perspective of the AI economy, so we balance our analysis of data with an exploration of the governance challenges that are particular to AI.

Starting from research on data justice and drawing on an examination of current data governance models, we propose four benchmarks for just data governance: (a) preserving and strengthening public infrastructures and public goods, (b) inclusiveness, (c) contestability and accountability and (d) global responsibility. We look at the principal ways in which data is currently understood – as a tradeable asset, as a commons, as a strategic national asset and as a component of individual identities – and demonstrate how these different conceptualisations interact in governance models from various regions around the world. The analysis is based on two related pieces of research. First, a study and report commissioned by the European Parliament's Panel for the Future of Science and Technology (European Parliament, 2022) to inform deliberations on data and AI governance (European Parliament, 2022). Second, a European Research Council-funded project based at the Tilburg Institute for Law, Technology and Society involving 5 years of interviews and fieldwork on specific data governance projects across different sectors, participant observation at international and national data governance events, joint projects with civil society and policy bodies on current questions of data governance, and a series of convenings with civil society groups that took place in South Asia, South America, the US, Sub-Saharan Africa and Europe (see de Souza et al., 2024; de Souza and Taylor, 2024; López et al., 2021; www.globaldatajustice.org).

Governing data

This section will firstly explore different conceptual bases for governing data. Secondly, it will discuss modular approaches through which institutions and principles are being proposed to govern data, and thirdly it will make the case for a justice-oriented approach to data governance.

Conceptual bases for the governance of data

There are three main assumptions that underpin the governance of data. First, prevalent on the state level, is that data is a strategic national asset: a key resource for population control and influence, for surveillance and monitoring both domestically and abroad, and for stimulating a domestic digital economy. In short, data is central to controlling citizens and to building digital power on the international level (Pohle and Thiel, 2020). In China, for example, this manifests in a state-led data economy where population control and state security are both supported through data regulation (Covington, 2021). Similarly, Russia's data governance model prioritises state and security interests, while also providing a framework for regulating the way businesses process data about people. India has also flirted with this model: a 2021 legislative report (Lok Sabha Secretariat, 2021) noted

that data was an asset of 'national importance' and argued for both data localisation and infrastructural investment to support it. In all these cases, the interests of domestic digital businesses and the state are placed above big tech, for instance by regulating social media platforms as publishers of online information so that they can be subjected to state control.

The second type of assumption identifiable amongst both state and private actors is that data is a proprietary asset that behaves like private property, and that can be more or less fully commodified (World Economic Forum, 2011). This property-based assumption is underpinned by the adoption of the individual (or 'legal person', such as a company) lens for defining rights and claims, rather than, for example, groups or society as a whole. This claim is based on the notion that, if individuals (or legal persons) are properly compensated with rights over data and (sometimes) financial or other utility, data can constitute both a kind of capital and a commodity that can be freely traded. This in turn is the basis for digital markets around the world and is a key feature of data governance propositions on the global level (for example, by the G20 and World Trade Organisation (WTO)) due to its importance to economic growth. The US, Canada, Singapore and, to a lesser extent, the European Union are typical examples of international actors who lead with this assumption, focusing on building markets and international businesses around data. This in turn offers opportunities for states to serve as hubs for powerful market actors' data transactions, as in the case of Singapore. This asset-focused approach to data governance is supported by international diplomacy. The G20, WTO and other international organisations such as the United Nations Conference on Trade and Development align with the assumption that free international trade in data is a core priority for global data governance, and advocate for a light-touch approach to rights where data trade comes first, and data protection and other rights are a desirable extra (Heseleva et al., 2020). They also align around treating AI technologies as products (OECD, 2024; Veale and Zuiderveen Borgesius, 2021), rather than systemic and public technologies. This perspective occludes the view that people may resist AI technology and infrastructures on the basis that they constitute a form of governmentality premised on certain values, with which many groups (as we explore below) do not align.

The last assumption we see motivating approaches to data and AI governance is the notion that there is something essentially different about personal and non-personal data – one so embedded in most data governance discussions that it tends to become invisible. It is worth surfacing, however, for two reasons. First, because it is the conceptual basis for many claims embedded in models and instruments of data governance, many of which become dysfunctional without it – for example that data should be governed in line with human rights which themselves are based on the liberal ideal of the rational, empowered individual. Second, because we are currently seeing a destabilisation of the personal/non-personal distinction just at the point where data governance has come to rely most heavily on it as a way to channel large quantities of deidentified data to developers of AI models.

Other approaches towards governing data

Beyond these mainstream assumptions, it is also important to make visible alternative visions which are frequently used to contest the notion that data constitutes a national security or market asset, and that people can only have rights over data that relates to them when that relation makes them identifiable. For instance, critical scholarship, civil society advocacy and labour organising have variously claimed that data can be classified as labour when people provide their attention and engagement to social media platforms (Fuchs, 2014), become building blocks in the AI economy (Pasquinelli and Joler, 2021) or directly engage as workers labelling data for AI models or content moderation (Perrigo, 2022). Data has also been defined as embodied human social relations, community and by extension, a form of territory (de Souza et al., 2024; Lehuedé, 2022; Tierra Común, 2021). Lastly, data is a source of claims to rights and equity, whether economic (Gurumurthy and Chami, 2022a), political (Wylie et al., 2018) or cultural (Kukutai and Taylor, 2016), and thus an

embodied claim to identity on the part of the marginalised and oppressed.

These critical analyses are often translated and operationalised into different governance models for data, namely public data trusts, data collaboratives, data commons (including semi-commons), data cooperatives and different notions of data sovereignty, that is, personal and indigenous.

In public data trusts, a public institution is formed or tasked to manage citizens' data collected from diverse actors including commercial companies based on a trust relationship for promoting innovation and policymaking (Micheli et al., 2020; Morozov and Bria, 2018). An example of a limited version of a data trust is the DECODE initiative, with pilots in Barcelona, where residents used environmental sensors to collect data to share it anonymously with their communities in their own terms, as well as in Amsterdam, where people prove their age without sharing full identity information (Bass and Old, 2020; Kortlander and Espuny Contreras, 2019; Sagarra et al., 2019). In such a model, the main agreement between data subjects and public actors is a trust relationship that depends on public engagement based on consultations, strong accountability mechanisms and collective benefits. The main value of this model is the public interest that could translate into the use of public data for policymaking, social innovation and to address social challenges (McDonald, 2019; Micheli et al., 2020; Wylie et al., 2018).

Data collaboratives are based on the idea is that private data collected by companies can be pooled with public data through an independent third party to generate public value (GovLab, 2024; Mozilla Insights et al., 2020). The data collaboration could take the form of a multi-stakeholder partnership that governs access to, sharing and use of data (Mozilla Insights et al., 2020). In these cases data can be effectively siloed by producers to keep it from other commercial uses, although it will still flow through, and thus profit, larger proprietary infrastructures at various points in its journey. One example of this is the recently proposed Intelligence Community Data Co-op (OSINT Foundation, 2024) in the US, which aims to collect and share commercially available and open source data for the entire US intelligence community. Data collaboratives are more developed than other models covered. The NYU GovLab has created a database with more than 200 cases of data collaboratives, mainly from the health, transportation and humanitarian sectors (GovLab, 2024).

Another model that can interact congruently with that of the free data market is the data commons, a powerful imaginary in technology policy and data governance (Purtova and van Maanen, 2023), where various parties aim to create data commons in relation to health, energy, financial and other domains of data. The commons vision involves making data available through shared infrastructures in ways which make it less excludable by economic interests. This potentially offers alternatives that could work in parallel to the neoliberal market model, still allowing for markets for data to exist and for innovation to be prioritised. An example of a data commons in formation comes from the New Hanse project based in Germany, which has produced a 'blueprint' aimed at enabling 'cities and communities to access and use urban data to gain better democratic control of urban space and provide more effective public services' (New Hanse Project, 2023: 2). The idea of the data commons has its roots in the fundamental work done by Ostrom and others (Ostrom and Hess, 2007) on how to keep public goods available to the public. Ostrom, however, warns anyone interested in institutionalising commons-oriented approaches that such an approach needs to be combined with contextual and domain-relevant instruments to make sure that the resource behaves in the interests of the expected beneficiaries (Ostrom and Hess, 2007: 1). Applying this work to the digital realm has mainly resulted in the idea that some kinds of data can usefully be defined as 'common pool resources' – owned by a particular community, where that community can restrict access by outsiders. Gurumurthy and Chami (2022b), for instance, argue for a 'semi-commons' approach where individuals, public agencies and legal persons such as corporations or data altruism organisations all have different and conditional rights over data, within the parameters of privacy

rights. They examine the notion of the commons in the Indian proposal for non-personal data governance (Government of India, 2023), which states that such data 'are a nation's or community's collective resources as arising from their natural and/or social spaces, and should be governed as such'. The authors argue in line with Ostrom, however, that a commons-based data stewardship model, if shaped by corporate interests, could both legitimise corporate claims to ownership of data with public value, and reinforce inequality of access to – and power over – data by centering guardianship with the most powerful interests.

In contrast to the larger-scale commons, data cooperatives are models in which data subjects or data holders' organisations are the main actors that voluntarily provide data to the pool to be used, shared and accessed through a collective of particular groups or communities. The main value of this model is the public interest that translates into collective protection and, if organised in the right ways, empowerment of the community. As such, cooperatives may be platforms that provide collective services in relation to data (such as the Dutch BO Akkerbouw project (BO Akkerbouw, 2024), aimed at providing farmers with individual data spaces), or data cooperatives where datasets (or data derivative) can be shared by the group. Cooperatives emerged as a response to the problems caused by defining data as a market commodity, and the top-down, platformised and opaque nature of other governance models (Micheli et al., 2020; Mozilla Insights et al., 2020; Mulgan and Straub, 2019). Such cooperatives tend to be diverse, with interests ranging from privacy and labour to social aims such as autonomy and sustainability (Micheli et al., 2020; Mozilla Insights et al., 2020).

The model of personal data sovereignty fits with the overall market approach to data in which data subjects are defined as market agents who aim to control the access to, use and sharing of their data (Micheli et al., 2020). The model is dependent on new intermediaries within the data economy. It is increasingly being translated from a set of aims, based in the libertarian political ideology commonly found in the communities working on decentralised technologies, into a set of technical tools aimed at realising greater interoperability between consumer services and individualised rather than collective forms of data governance, both of which form business models where the developers of those tools and infrastructures can provide them commercially. The advent of cryptographic technologies and the libertarian values of the crypto community have been influential for this model, but so far the vision of 'trustless trust' has not been widely adopted by those producing data in their everyday lives. The provision of these personal data stores is in parallel, however, rather than an alternative to, the use of data outside of them by for-profit or state actors. The most prominent example of personal data sovereignty comes from the proposal of 'digital identity wallets' by the European Commission (European Commission, 2024), where self-sovereign identity model is clearly influential, despite the projected end product being a very large-scale identity management system.

Lastly, work on indigenous data sovereignty is not like the other governance models on this list. Rather than being a model per se, it is more a principle used to advance a different proposed basis for governing data. The CARE principles, which advocate for collective benefit, authority to control, responsibility and ethics, are designed to centre indigenous peoples' interests, world views and rights. They are designed to address lacunae in the FAIR principles (findability, accessibility, interoperability, and reusability) which place an emphasis on findability, accessibility, Interoperability and Reusability, but as indigenous data sovereignty experts argue do not address challenges of power, including those centred on historical contexts (Carroll et al., 2020). Data from indigenous communities is one of many resources that have historically been used by colonial powers to exercise control over the lives of indigenous people. Therefore, the indigenous data sovereignty movement promotes the idea of managing information about their peoples, territories, lifeways and natural resources according to their laws, practices and values. Its claims are legally based on Articles 18 and 19 of the United Nations Declaration on the Rights of Indigenous Peoples, which state that indigenous peoples have the right to participate in the matters that affect them through their means and procedures (Taylor and Kukutai, 2016).

Why we need a justice-oriented approach to governing data and AI

So far, we have described governance approaches toward state or business power, building public-sector resources or limiting access to particular actors, as well as different institutional, as well as principle-based structures for operationalizing data governance. Overall, any model for data governance is a statement about who should benefit from data and how. Hence, if we wish to think about data governance in relation to the power to automate, optimise and scale up interventions through AI systems, perhaps the most important issue becomes data's lifecycle. Datasets determine the practical capacities and effects of AI models, and their continual repurposing is of central relevance to the developing AI economy. To get a grip on data's ever-evolving lifecycle, however, it is necessary to go beyond the focus of data protection on individual identifiability and thus bypass one of the core tools of data governance worldwide. This is, however, both a political and a practical challenge given the centrality of data protection – and thus the personal/non-personal binary – to current thinking about what data may flow, and for what purposes.

In practice, what creates data's economic value is the ability to transform and reuse it. This is both of central importance to understanding how data enters AI assemblages and how it fuels their impacts on people. For example, all over the majority world, the fintech industry's 'alternative credit models' ingest a huge variety of non-financial data about people, from mobile device usage data to the characteristics of their social networks (Aitken, 2017). Meanwhile in the US, Customs and Border Protection and Immigrations Customs Enforcement officials have demanded telematics data from the companies that collectively track the movements of tens of millions of vehicles on a daily basis (Brewster, 2021).

These cases demonstrate just a few of the myriad ways in which apparently innocuous metadata from people's everyday devices or deidentified data becomes potentially highly sensitive as soon as it is subjected to particular research practices. Ironically, these practices usually begin with the deidentification and aggregation of the data, removing it from the purview of data protection. The examples also highlight how, when data flows between institutions that have different functions and different modes of independence and accountability to the public, the capacity of those affected to interrogate the data changes. Data collected from people in one context may be used against their interests in another. Once the overarching rubric of data protection is no longer present, the formal connection between data and risk or vulnerability is entirely lost, and data is free to use and redeploy.

Despite data protection's notion of vulnerability as rooted in the innate characteristics and attributes of people, it therefore makes sense to think of data and data technologies, including AI, as potentially creating new vulnerabilities rather than just exploiting existing ones. If, as we argue, data now changes categories in terms of its effects and risks depending on who has access to it, what their purpose is, and what analytical methods are used, then there is no way to cover this kind of fluidity without declaring all social data potentially sensitive and remaking data governance to deal with this risk – something that has already been argued by data protection scholars (Purtova, 2018).

Our intent is not to argue that data is too complex to govern effectively, or that it will always escape from measures taken to control it. Instead, these examples demonstrate that data has a lifecycle during which it is likely to transform multiple times with diverse meanings, purposes and effects, that it may travel between jurisdictions while doing so, and that these attributes matter for attempts to regulate and shape both data flows and ensuing uses.

We therefore advocate for justice-oriented data governance. This approach has a temporal dimension: data that is controllable at one point in its trajectory, or for a particular group involved in generating it, may quickly escape control as soon as it travels onto large infrastructures for purposes of interoperability, sharing or monetisation. Therefore checks and controls are needed at points where data's use or users change, which may occur throughout the open-ended lifecycle of data, across its different sectoral uses, and in line with the different aims of the actors using it – for instance ways to opt in and out of different datafied communities (de Souza and Bhardwaj, 2024). It also has a spatial dimension, in that as data flows

between sectors, institutions or markets, there is a recalibration in terms of access, use and perceived ownership. Tackling this multidimensionality is therefore critical to ensure that data's mutability does not subvert or destabilise the conditions and rules designed to protect people from misuse.

Benchmarks for just data governance

This section proposes benchmarks for the just governance of data and AI following the discussions over the dominant conceptualisations of data and the alternative approaches and its operationalisation in ideal type governance models. It draws from the 2017 outline of fundamental conditions for just data governance (Taylor, 2017), based on work in the field of data justice by both academic researchers and civil society organisers, which focused on (in) visibility, technological autonomy and responsibility for preventing harm. This work took place against a background of data justice research involved in analyses of harm (Redden, 2018), of data's role in the development sector (Heeks and Renken, 2018) and in the reconfiguration of social welfare systems (Eubanks, 2018), and the use of data in the majority world for purposes of both oppression and emancipation (Kazansky et al., 2019; Ricaurte, 2019). The field has been characterised overall by its focus on connecting datafication to broader questions of social and economic justice (Gurumurthy and Singh, 2005) and by attempts to re-focus discussions of technology explicitly on these questions (Gangadharan and Niklas, 2019).

The evolution of data into additionally forming the basis for AI models increases both its potential and its risks. As such, we propose a reformulated agenda that sets benchmarks for just governance at the intersection of data and AI. A benchmark is, like our original proposal, not a tool or a set of guidelines. It is not the ceiling that AI governance should seek to reach, but the floor. The benchmarks we propose are as follows.

Preserving and strengthening public infrastructures and public goods

> Does the data or AI governance model proposed channel benefits principally toward the public, and does it prioritise the integrity of public infrastructures and related public goods?

The notion of AI as a product, upon which many AI regulations appear so far to be based, is problematic because it orients attention away from the public and systemic nature of most large-scale AI systems that affect us and instead posits that standardisation and self-assessment can make these technologies just and beneficent. It also positions the public as consumers rather than (as in the EU's General Data Protection Regulation (GDPR), for example) affected by systems in ways which require control and oversight. In order to adequately conceptualise AI as a public, as well as a private, set of technologies, it is necessary to provide checks and balances at the design and procurement stage to assess whether a given system is in line with the public interest and how the public can influence this discussion.

One example of this kind of influence is the stand taken by Dutch university leadership on public digital infrastructures (Maex, 2021, n.61 sect.4). Another is India's 'Janta Parliament' discussions where a coalition of civil society organisations came together to organise civil society deliberation on issues such as enforcing civil liberties and shaping digital rights (Janta Parliament, 2020). Another example is from the public data trusts introduced earlier. In these kinds of trust, data is not siloed from commercial or exploitative uses unless the data used is collected by and only flows through the public provider's servers. Instead, it promises a pool of data curated for public uses. Similarly to public data trusts, in a data collaborative, unless the data is proprietary to public actors from the start of its lifecycle, a collaborative will run in parallel to different uses of data by the companies involved.

These claims on the part of public institutions and publics affected by technologies have the common feature that they link concerns about public institutions and services directly to civil and political rights, and that they bring cases of emergent effects and harms from technology that are not yet articulated in law or within the portfolio of regulators. This has so far been largely the task of

civil society, given that data law addresses fairly broad categories of risk (of discrimination, for example, or breaches of confidentiality) so that addressing emergent harms, particularly in relation to civil and political rights, is only indirectly the task of oversight. The models described above mainly reinforce this problem of oversight, except for the indigenous data sovereignty movement which is entirely shaped by the experience of datafied harm, and takes as its starting point the nonsharing of data with actors who have historically harmed indigenous communities.

Second, mechanisms are needed to provide ways for individuals affected by AI to contest its deployment where necessary. This is particularly important given that most people affected negatively by AI are not aware that it is AI causing the harm in question, because it is used within an intermediary such as a commercial firm (e.g. a bank) or the police. The challenge of public data trusts, even when they aim for higher accountability mechanisms, is the lack of direct and visible points of connection between algorithmic technologies and the public necessitate new architectures of accountability beyond those provided by data protection or consumer protection law.

Third, mechanisms are needed to make it possible to identify and tackle problems that emerge from the deployment of an AI model or system during its entire lifecycle, including when it is reconceptualised or repurposed along the way. In order for AI systems to evolve through different use cases without harmful effects and the diversity of models and conceptions that reimagine collective representation and ownership over data, AI regulations should include mechanisms for both individual and collective complaints to be brought directly against deployers of AI, and should operate in relation to public and administrative law wherever appropriate, rather than within the framing of product liability and consumer rights.

This issue goes to the equitable distribution of resources, but also to the preservation of the functionality of public (digital) infrastructures which in turn provide public goods. Examples of these infrastructure-related goods include the social safety net, scientific knowledge, publicly accessible education and healthcare, access to justice, fair electoral processes and just law enforcement. Data and AI are predominantly used in neoliberal contexts to optimise for exclusion, marginalisation and regressive forms of provision, with an attendant redistribution of power over these public resources to for-profit actors. As well as being key in this transformation toward the private provision of public goods, data (in the form of information about service provision) is also an important tool for creating or denying accountability on the part of providers. The urgent need to render private technology providers more accountable is seen in relation to public systems around the world (BBC, 2021; Cokayne, 2021), as are efforts to build and preserve public digital infrastructures that allow for alternative uses and conceptions over data outside of dominant narratives of national security or market asset, whether for population statistics (Greaves et al., 2024), higher education (University World News, 2021) or welfare systems (López, 2021).

Establishing governance models for data and AI therefore also represents a statement of the public interest: it requires a position on the extent to which public services should be provided through public infrastructures and what 'public' should mean in practice for instance in terms of transparency policies, monitoring mechanisms and avenues for the redress of grievances (Mhlambi, 2020). This by extension also informs architecture development: it determines who has the right to construct infrastructures that directly impact the public, whether and how these should be made accountable to the public and how publicly owned systems should interact with privately owned ones, and to whose benefit (López, 2021). Engaging with this notion of 'publicness' also means to discern how the treatment of data or AI as a commodity result in subjecting it to skewed market power where the dominance of a few players sets the agenda for others within the economy. Building a level playing field requires ensuring not just that certain functions retain a public character, but also that there remains a capacity for other actors such as civil society to challenge the publicness of functions. Thereby, if they fall short in their standards such as in terms of accountability there remains a capacity to respond and monitor.

Similarly, governing data and AI primarily through private standards bodies and certification

by private actors would tend to privilege a neoliberal vision of the public interest which is subject to market-driven interests, and which cannot be easily updated to deal with new applications and systems. Finding a way to extend democratic process to technology governance is one of the priorities for the coming decades since without it, any governance model cannot be tested against the notion of the public interest and – given the prevailing power of technology giants and their interest in shaping governance – will suffer challenges to its legitimacy.

Inclusiveness

> Does the model envision rights and values as universally applicable, or does it prioritise rights-holders who are also citizens or geographically close to the institutions governing data? Does it conceptualise non-citizens and people in other regions of the world as relevant communities for the values and protections it establishes? Does the understanding of rights and values account for the fact that people have different capacities to claim these rights and entitlements, and explicitly account for these social-political contexts?

An inclusive perspective on data governance – on the global level, to match the level at which the data and AI economy operates – demands that any model centre the interests of all who will be affected by it, rather than simply a body of citizens in a particular state or region. This broad definition of whose data matters therefore includes, for instance, non-citizens including migrants, people who are suspected of crime or considered security risks and people who are beneficiaries of social welfare programs – all groups whose agency and interests are commonly disregarded when it comes to developing and deploying data analytics and AI. Data regulation tends to have dual priorities: human rights, which aligns well with a social justice-oriented governance model, and market efficiency, which does not. A social justice perspective starts from the assumption that all societies are unequal playing fields where people's circumstances give them different degrees of agency and ability to claim their rights. Following the examples of indigenous data sovereignty and data cooperatives, a just data governance model should conceptualise *who* matters and *how*, rather than only *what* data matters.

Drawing from indigenous data sovereignty in the Māori context, we see key elements of building such an inclusive model. These include exploring who are working to enforce authority over their data; to maintain the relationships of their data to the indigenous context; to create obligations for balancing individual rights with collective interests and accountability; to build capacity amongst Māori people; to create reciprocity with non-Māori authorities in terms of consent and respect of the Māori culture, and to establish guardianship over data (Taylor and Kukutai, 2016).

Every data governance model is rooted in a particular place and history, including the commodified vision of the G20 which repeats the history of many of its' members' global hegemony and the extractive dynamics that accompanied it. The challenge of inclusivity therefore requires some rethinking of the assumptions around the nature of data and its ownership recounted in Section 2 above (Arora, 2019). Even if we try to disconnect digital technologies from their history, the long-term continuities between these technologies and archival and statistical practices are present in the way in which data is collected, organised, shared and used (Aronova et al., 2017). The prediction of exploitation and discrimination of certain groups therefore originates in the legacies of exclusion rather than in futuristic claims about AI as a source of universal progress.

An inclusive governance model demands more inclusive ways of conceptualising vulnerability in relation to technology, going beyond the notion of vulnerability as an inherent condition (as, for example, in data protection's framing) to that of people's vulnerabilisation through unequally distributed technological power and agency. An inclusive vision of protection from data or AI harms is also an important component of an inclusive governance regime. The contexts in which data causes harm have changed radically over time, from the analogue and early digital privacy harms of the twentieth century to a set of harms including facial recognition (Chen, 2019), pseudoscience such as physiognomic AI (Stark and Hutson, 2022) and

collective and more political threats such as deepfakes and online health-related misinformation (D'Ignazio et al., 2022), as well as material conditions of labour (Pasquinelli and Joler, 2021), so that governance needs to both expand and become more responsive if it is to address these risks.

Contestability and accountability

> Does the governance model assume that people may disagree, resist, refuse and bring claims which need forms of redress? Are there mechanisms to allow data and AI policy to respond to social and political change, and does the model offer ways of recognising and negotiating about dissent and contestation? Does the model align with principles and processes of democratic accountability through the institutional mechanisms it offers?

Contestability and accountability are key to the functionality of a data governance model as exemplified by the ideal types of the public data trust, data cooperatives and indigenous data sovereignty. They are linked: if there are structures for accountability then people who are negatively affected will make this known, and conversely, it is only through claims that contestability is realised. Even where contestability is internal within companies or public bodies, it still needs to be linked to broader political and legal forms of accountability in order to have meaning following the aspirations of public data trusts and indigenous data sovereignty. Whether this happens or not, however, is largely dependent on people's legal standing. For instance, in the sphere of international humanitarianism accountability for harms relating to data or AI is missing because international organisations are principally accountable to states rather than the affected groups they serve (Hilhorst et al., 2021). Similarly, migrants subjected to intrusive or excessive processes of datafied border control could in theory claim that the technologies in question are illegitimate, but do not have the standing to do so (this problem is explored in detail by, e.g. Brouwer, 2021; 2023; Kluttz et al., 2020).

These issues of legal standing and geopolitical positionality are essential to understanding when issues such as data literacy and the transparency and explainability of systems are relevant, and when they are simply window dressing for systems that are not designed to be accessible to contestation. The challenge for public data trusts and data cooperatives is conceptualising AI technologies as public or collective in their fundamental nature would mean rethinking the nature of contestation and tying it to both democratic process and other meaningful forms of representation, depending on the location and the population involved, instead of devising and formalising ever-more complex forms of technical transparency. If contestation is not possible for those in the most disadvantaged position, there is no meaningful contestability.

This test for contestability demands that industry and governance authorities think beyond the classic neoliberal tropes of the explainability of credit decision making, or of who is shown which online advertisements. As far as explainability goes, the rubber hits the road with regard to systems that are designed to be unexplainable for political reasons: migration and asylum processing, risk profiling in law enforcement, antifraud measures in welfare systems. Contestability is a question of power, not design, and many attempts at standardisable, politically sanitised forms of explanation and transparency on a systemic level serve as useful signals that administrative violence is being committed.

Following the lessons of indigenous data sovereignty struggles, the final aspect of contestability is the more fundamental ability of affected groups to resist the power of markets and private actors to shape data and AI governance priorities. Challenging the market-based framing for policy relevance in governance debates, questioning why certain courses of action are deemed irrelevant, impractical or infeasible by market actors and fundamentally questioning the role of markets in setting the vision and terms for future governance is a form of contestation that currently has little place in what is recognised as technology governance. Accusations of anticompetitive practices or consumer rights violations do not provide appropriate ways to challenge the power of private actors, in particular, to co-opt technology governance at scale. A data justice perspective therefore demands that we

broaden our conceptualisation of contestability beyond claims based on competition and consumer protection regulation.

Global responsibility

> Does the model only look inward, on a national or regional level, or does it take into account norm-making effects on external actors in the global, political and economic landscape?

This question reframes what is termed the 'Brussels effect', where the EU plays a de facto role in international standard-setting because other nations have to align with the norms conveyed by its legislative instruments in order to trade with the bloc – an effect that is a central aim of Europe's digital strategy. This regulatory convergence means that the norms contained in the EU's data and AI governance models will have practical effects on decision making elsewhere (positive or negative) and therefore have a diplomatic character as well as an internal one. For example, when WhatsApp announced a change in its privacy policy in 2021 regarding sharing data with Facebook, Europeans were allowed an opportunity to opt out of it due to the GDPR (Yasmin, 2021), while users in most other regions could not. In India for instance, WhatsApp users moved in large numbers to other platforms such as Signal (Hariharan, 2021). The Indian Government asked WhatsApp to remove its discriminatory policy citing the fact the Indian customers did not have the opportunity to opt out and using the European case as a benchmark. We do not argue for global responsibility in terms of data and AI governance as a responsibility to offer templates and transplants of how to build governance frameworks for different regions around the world. Instead, we advocate for an acknowledgment that the decisions taken by powerful blocs have a lifecycle and effects that go beyond governing within their jurisdictions.

This notion of the responsibility held by powerful actors in data and AI governance is potentially most enforceable in the area of trade agreements, which seem set to reproduce the historically unfair constructions seen in other areas of trade. The agreements being made by the G20 and formed in the WTO (WTO and WEF, 2022) allow firms to access data from the majority world to exploit it and, at the same time, externalise the privacy damages of aggressive data technology development (Scassera et al., 2024). For similar reasons, the notion of rule of law is a highly contested concept and has different meanings in different regions (Krygier, 2011). It cannot be relied upon as a basis for cross-border claims to data or to justify its uses. Instead, a more just and sustainable system for trade in data would involve mediating the discussions between parties to identify where agreements will have uneven effects, or create systemic incompatibilities which will in practice create dysfunction in the transnational governance of AI

Reorientating data governance towards data justice

These pillars were not proposed as new ethical principles for the already extensive list of codes and guidelines, but instead posited the possibility of reorienting the overall understanding of data governance and the emergent ideal types of models toward principles that are foundational to work on social justice. As multiple collective models show, the notion of control over one's own visibility – touches on both privacy and representation. It asserts that people should be represented through their data when it is in their interests, for example when registering to vote, receiving benefits and entitlements, and in contexts where public health or safety is at stake. However, they should also be able to withdraw their participation in systems which render them visible in exploitative ways, for instance extractive practices of commercial profiling, unwarranted surveillance by government or commercial firms, and systems (such as the commercial uses of data based on national identification infrastructures) that channel public goods into private wealth.

In the examples of public data trusts, data cooperatives and the claims of data sovereignty, it is clear that technological autonomy is necessary in relation to adopting or refusing particular technologies and

in relation to control over one's terms of engagement with data markets. This implies establishing means of collecting and using data that do not serve the business models of big technology firms, as exemplified by the efforts of data cooperatives, and in turn that non-commercial institutions and organisations, especially civil society organisations which legitimately represent the interests of groups and communities, must play a central role in data governance.

Finally, we proposed a shift in the responsibility for preventing harm, namely that people should not be made solely responsible for identifying and protecting themselves from exploitation through datafied (or automated) systems, given that these are generally invisible to those they affect. Where people cannot be aware of the paths their data is travelling, or the basis on which decisions are being made about them, it becomes the responsibility of those handling data and building models to ensure that the public is protected, both individually and collectively. The key difference to existing frameworks is that, as public data trusts aim, accountability should be produced through public and (where possible) democratic architectures, rather than defined by those responsible for the harms in question.

These pillars offer a normative underpinning for any governance model, but also guidance for reorienting some of the current ideal types of alternative and collective-leaning models. A model that has the effect of channelling power and profit toward the best-resourced and most powerful actors, whether governmental or corporate, is by definition not in line with principles of social justice and requires reorienting. Equally, one that does not countenance contestation and reshaping – however pressing the public needs it addresses – requires further thinking and development. Perhaps most importantly, exemplified by some proposals of data collaboratives, commons and personal data sovereignty, if a model proposes structures for accountability, but these are technology-specific rather than aligned with the existing architectures through which civil society asserts its agency, the model is unlikely to produce just outcomes.

Conclusion: what constitutes just governance for data and AI?

This paper has asked how we can take data governance, and by extension the governance of AI, beyond its current genuflection toward what has been termed a 'trade-related, market-friendly paradigm of human rights' (Baxi, 1998: 127). We have laid out the benchmarks that we might use to test AI governance regimes in particular for their ability to take account of plurality, beyond-local responsibility for their effects, refusal and contestation, and the value of publicness. This is not an update to the framework for thinking about data justice in the context of data governance proposed by Taylor (2017). Instead, it is an extension to that thinking, offered as a way to take account of the AI field's existential hunger for data, the perverse incentives posed by the incorporation of AI businesses into the exponential growth strategies of tech multinationals, and the infrastructural power and dominance that shape the global landscape of technology.

Our key message is that thinking about justice in relation to data and AI has to take place in relation to threats to just outcomes. Perhaps the most prominent of these threats are coloniality, authoritarianism and the pervasiveness and resilience of big tech's infrastructural power, which tends to ensure that both technology and governance are shaped in the interests of the most powerful. All three are political problems, and the first two, at least, have evolved and been honed over a very long period of time. The third acts as an amplifying factor, creating greater reach and depth for those dynamics. It is also a lens through which we both experience, and potentially resist, the first two.

It is for this reason that data governance is both a public problem, and one worth paying attention to: controlling datafied power offers a handle on many of its other political and economic forms, since these are increasingly exerted through data technologies like AI. Interrogating how different configurations of data governance provide or limit access to datafied power can therefore tell us something useful about the business models that feed economic and political forms of power.

What constitutes 'good' data governance is therefore highly dependent on one's position in relation to industry. Struggles over infrastructural sovereignty, the collectivisation or privatisation of public goods, the ability to conduct oversight of state or private systems and the ability to control a population at scale all relate to data and, increasingly, how it is used in AI models. The power to govern data is the power to govern many of the things we collectively think about when we think about justice. It is for this reason that we argue for resisting commodification and promoting public rights over data: the way we organise datafication in different countries and regions worldwide has become a mirror for the way in which we organise politics, and with it access to recognition, representation and resources. If we cannot govern datafication justly, the hope that we can find justice in other ways is diminished. Fortunately, however, the reverse is also true.

Declaration of conflicting interests

The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The authors disclosed receipt of the following financial support for the research, authorship and/or publication of this article: This work was supported by the H2020 European Research Council (grant number 757247), and received additional support from the European Parliament's Science and Technology Options Assessment Panel (STOA).

ORCID iDs

Siddharth Peter de Souza https://orcid.org/0000-0003-4299-4878
Joan López Solano https://orcid.org/0000-0001-5068-7494
Aaron Martin https://orcid.org/0009-0000-4073-9182

Bibliography

Aitken R (2017) "All data is credit data": Constituting the unbanked. *Competition & Change* 21(4): 274–300.

Appel G, Neelbauer J and Schweidel DA (2023) Generative AI has an intellectual property problem. *Harvard Business Review*, 7.

Aradau C and Blanke T (2015) The (big) data-security assemblage: Knowledge and critique. *Big Data & Society* 2(2): 2053951715609066.

Aronova E, Oertzen C and Sepkoski D (2017) Introduction: Historicizing big data. *Osiris* 32(1): 1–17.

Arora P (2019) Decolonizing privacy studies. *Television & New Media* 20(4): 366–378.

Bass T and Old R (2020) Common knowledge: Citizen-led data governance for better cities. Available at: https://www.decodeproject.eu/publications/common-knowledge-citizen-led-data-governance-better-cities (accessed 25 April 2022).

Baxi U (1998) Voices of suffering and the future of human rights. *Transnational Law and Contemporary Problems* 8: 125.

BBC (2021) Post Office scandal explained: What the Horizon saga is all about. Available at: https://www.bbc.com/news/business-56718036 (accessed 24 April 2024).

BO Akkerbouw (2024) Data-intensieve akkerbouw. Available at: https://www.bo-akkerbouw.nl/dit-doen-wij/data-intensieve-akkerbouw (accessed 11 November 2024).

Brewster T (2021) These companies track millions of cars—Immigration and border police have been grabbing their data, *Forbes*, 4 January. Available at: https://www.forbes.com/sites/thomasbrewster/2021/04/01/these-companies-track-millions-of-cars-immigration-and-border-police-have-been-grabbing-their-data/ (accessed 26 April 2022).

Brittain B (2023) Google hit with class-action lawsuit over AI data scraping. *Reuters*, 12 July. Available at: https://www.reuters.com/legal/litigation/google-hit-with-class-action-lawsuit-over-ai-data-scraping-2023-07-11/ (accessed 23 April 2024).

Brouwer E (2021) Schengen and the administration of exclusion: Legal remedies caught in between entry bans, risk assessment and artificial intelligence. *European Journal of Migration and Law* 23(4): 485–507.

Brouwer E (2023) Challenging bias and discrimination in automated border decisions: Ligue des droits humains and the right to effective judicial protection.

Verfassungsblog. 11 May 2023. Available at: https://verfassungsblog.de/pnr-border/ (accessed 11 December 2024).

Calzada I (2019) Data spaces and democracy. *RSA Journal* 165(2)(5578): 40–43.

Carroll SR, Garba I, Figueroa-Rodríguez OL, et al. (2020) The CARE principles for indigenous data governance. *Data Science Journal* 19(1): 43.

Chen A (2019) This is how you kick facial recognition out of your town. Available at: https://www.technologyreview.com/s/614477/facial-recognition-law-enforcement-surveillance-private-industry-regulation-ban-backlash/ (accessed 16 December 2019).

Cokayne R (2021) We could be stumbling into a digital welfare dystopia. Available at: https://techcentral.co.za/we-could-be-stumbling-into-a-digital-welfare-dystopia-open-secrets/205646/ (accessed 24 April 2024).

Covington (2021) China released updated draft data security law and personal information protection law for public comments. Available at: https://www.cov.com/-/media/files/corporate/publications/2021/05/covington-alert–china-released-updated-draft-data-security-law-and-personal-information-protection-law-for-public-comments-may-3-2021.pdf (accessed 28 April 2022).

Dencik L, Hintz A and Cable J (2016) Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society* 3(2): 205395171667967.

de Souza SP and Bhardwaj K (2024) India's conception of community data and addressing concerns for access to justice. *Digital Society* 3(1): 16.

de Souza SP, Smith HM and Taylor L (2024) Decolonial data law and governance. *Technology and Regulation* 2024: 1–11.

de Souza SP and Taylor L (2024) Rebooting the global consensus: Norm entrepreneurship, data governance and the inalienability of digital bodies. Available at: https://osf.io/download/66d5b198f0bc77f36b5face9/ (accessed 13 December 2024).

Díaz-Rodríguez N, Del Ser J, Coeckelbergh M, et al. (2023) Connecting the dots in trustworthy artificial intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion* 99: 101896.

D'Ignazio C, Cruxên I, Val HS, et al. (2022) Feminicide and counterdata production: Activist efforts to monitor and challenge gender-related violence. *Patterns* 3(7).

Eubanks V (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press.

European Commission (2024) A digital ID and personal digital wallet for EU citizens, residents and businesses. Available at: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/ (accessed 11 November 2024).

European Parliament: Directorate-General for Parliamentary Research Services, Lopez Solano J, Martin A, et al. (2022) *Governing Data and Artificial Intelligence for All – Models for Sustainable and Just Data Governance*. European Parliament. https://data.europa.eu/doi/10.2861/915401.

Fuchs C (2014) Digital prosumption labour on social media in the context of the capitalist regime of time. *Time & Society* 23(1): 97–123.

Gangadharan SP and Niklas J (2019) Decentering technology in discourse on discrimination. *Information, Communication & Society* 22(7): 882–899.

Gangadharan SP, Petty T, Lewis T and Saba M (2018) Digital defense playbook: Community power tools for reclaiming data. Available at: https://www.odbproject.org/wp-content/uploads/2019/03/ODB_DDP_HighRes_Single.pdf (accessed 13 December 2024).

Government of India (2023) Revised draft non-personal data governance framework. Available at: https://prsindia.org/policy/report-summaries/revised-draft-non-personal-data-governance-framework (accessed 24 April 2024).

GovLab (2024) Data collaboratives explorer. Available at: http://localhost:4000/explorer.html (accessed 24 April 2024).

Greaves LM, Lindsay Latimer C, Muriwai E, et al. (2024) Māori and the integrated data infrastructure: An assessment of the data system and suggestions to realise Māori data aspirations [Te Māori me te integrated data infrastructure: He aromatawai i te pūnaha raraunga me ngā marohitanga e poipoia ai ngā wawata raraunga Māori]. *Journal of the Royal Society of New Zealand* 54(2): 190–206.

Gürses S, Dobbe R and Poon M (2020) Programmable infrastructures. Available at: https://www.tudelft.nl/en/tpm/programmable-infrastructures/ (accessed 24 August 2020).

Gürses S and Van Hoboken J (2017) Privacy after the agile turn. In: Selinger E, Polonetsky J and Tene O (eds)

The Cambridge Handbook of Consumer Privacy. Cambridge: Cambridge University Press, 579–601.

Gurumurthy A and Chami N (2022a) Beyond data bodies: New directions for a feminist theory of data sovereignty. Available at: https://www.datagovernance.org/files/research/1641621845.pdf (accessed 13 December 2024).

Gurumurthy A and Chami N (2022b) Governing the resource of data: To what end and for whom? Available at: https://itforchange.net/sites/default/files/1741/WP23-Governing-the-Resource-of-Data-AG-NC.pdf (accessed 13 December 2024).

Gurumurthy A and Singh PJ (2005) Political economy of the information society: A southern view. In: Instituto del Tercer Mundo (ITeM) *Information Society for the South: Vision or Hallucination*. Montevideo: ITeM, 103–116.

Hariharan S (2021) WhatsApp's privacy policy pushes users to Signal, Telegram. *The Times of India*, 9 January 2021. Available at: https://timesofindia.indiatimes.com/business/india-business/whatsapps-privacy-policy-pushes-users-to-rivals/articleshow/80178485.cms (accessed 28 April 2022).

Heeks R and Renken J (2018) Data justice for development: What would it mean? *Information Development* 34(1): 90–102.

Heseleva K, Ramos VJ and de Oliveira AI (2020) Towards a multilateral consensus on data governance. Available at: https://www.global-solutions-initiative.org/policy_brief/towards-a-multilateral-consensus-on-data-governance/ (accessed 23 April 2024).

Hilhorst D, Melis S, Mena R, et al. (2021) Accountability in humanitarian action. *Refugee Survey Quarterly* 40(4): 363–389.

Janssen M, Brous P, Estevez E, et al. (2020) Data governance: Organizing data for trustworthy artificial intelligence. *Government Information Quarterly* 37(3): 101493.

Janta Parliament (2020) 'Press release – Technology and surveillance session'. Available at: https://jantaparliament.wordpress.com/2020/08/23/press-release-technology-and-surveillance-session/ (accessed 6 May 2024).

Kazansky B, Torres G, van der Velden L, Wissenbach K and Milan S (2019) 14: Data for the social good: Toward a data-activist research agenda. In: Daly A, Devitt K and Mann M (eds) *Good Data*. Amsterdam: Institute for Network Cultures, 244–259.

Kitchin R (2014) Big data, new epistemologies and paradigm shifts. *Big Data & Society* 1(1): 205395171452848.

Kluttz DN, Kohli N and Mulligan DK (2020) Shaping our tools: Contestability as a means to promote responsible algorithmic decision making in the professions. In: Werbach K (ed) *After the Digital Tornado: Networks, Algorithms, Humanity*. Cambridge: Cambridge University Press, 137–152.

Kortlander M and Espuny Contreras M (2019) Final report on pilots Amsterdam and sustainability plans. Available at: https://decodeproject.eu/file/700/download.pdf (accessed 13 December 2024).

Krygier M (2011) Four puzzles about the rule of law: Why, what, where? And who cares? *Nomos* 50: 64–104.

Kukutai T and Taylor J (2016) *Indigenous Data Sovereignty: Toward an Agenda*. Canberra: ANU Press.

Lehuedé S (2022) Territories of data: Ontological divergences in the growth of data infrastructure. *Tapuya: Latin American Science, Technology and Society* 5(1): 2035936.

Lok Sabha Secretariat (2021) 'Report of the joint committee on the personal data protection bill'. Available at: https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf (accessed 28 April 2022).

López J (2021) The case of the solidarity income in Colombia: The experimentation with data on social policy during the pandemic. In: *COVID-19 from the Margins: Pandemic Invisibilities, Policies and Resistance in the Datafied Society*. Amsterdam: Institute of Network Cultures, 126–128.

Maex K (2021) Protect independent and public knowledge. Available at: https://s3.nl-ams.scw.cloud/pstorage-amster-45168546/26011517/DigitalUniversityAct.pdf (accessed 5 June 2024).

McDonald S (2019) Reclaiming Data Trusts, Centre for International Governance Innovation. Available at: https://www.cigionline.org/articles/reclaiming-data-trusts/ (accessed 28 November 2021).

Mhlambi S (2020) From rationality to relationality: Ubuntu as an ethical and human rights framework for artificial intelligence governance. *Carr Center for Human Rights Policy Discussion Paper Series* 9: 31.

Micheli M, Ponti M, Craglia M and Berti Suman A (2020) Emerging models of data governance in the age of datafication. *Big Data & Society* 7(2): 205395172094808.

Morozov E (2023) The true threat of artificial intelligence. Available at: https://www.nytimes.com/2023/06/30/opinion/artificial-intelligence-danger.html# (accessed 10 April 2024).

Morozov E and Bria F (2018) *Rethinking the Smart City: Democratizing Urban Technology*. New York: Rosa Luxemburg Stiftung.

Mozilla Insights, van Geuns J and Brandusescu A (2020) Shifting power through data governance. Available at: https://assets.mofoprod.net/network/documents/ShiftingPower.pdf.

Mulgan G and Straub V (2019) The new ecosystem of trust: How data trusts, collaboratives and coops can help govern data for the maximum public benefit. *Nesta*. Available at: https://www.nesta.org.uk/blog/new-ecosystem-trust/ (accessed 11 December 2024).

New Hanse Project (2023) *Blueprint: Governing Urban Data for the Public Interest*. Hamburg: The New Hanse.

OECD (2024) OECD working party and network of experts on AI. Available at: https://oecd.ai/en/network-of-experts/working-group/1148 (accessed 24 April 2024).

O'hara K and Hall W (2018) Four internets: The geopolitics of digital governance. Available at: https://www.cigionline.org/publications/four-internets-geopolitics-digital-governance/ (accessed 13 December 2024).

OSINT Foundation (2024) ODNI issues RFI for intelligence community data co-op (ICDC). Available at: https://www.osintfoundation.com/NewsBot.asp?MODE=VIEW&ID=30744 (accessed 10 September 2024).

Ostrom E and Hess C (2007) Private and common property rights. In: *Encyclopedia of Law and Economics*. New York: Edward Elgar Publishing Limited, 4830.

Pasquinelli M and Joler V (2021) The nooscope manifested: AI as instrument of knowledge extractivism. *AI & Society* 36(4): 1263–1280.

Perrigo B (2022) Why Timnit Gebru isn't waiting for big tech to fix AI's problems'. *Time*, 18 January 2022. Available at: https://time.com/6132399/timnit-gebru-ai-google/ (accessed 26 April 2022).

Pohle J and Thiel T (2020) Digital sovereignty. *Internet Policy Review* 9(4).

Purtova N (2018) The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology* 10(1): 40–81.

Purtova N and van Maanen G (2023) Data as an economic good, data as a commons, and data governance. *Law, Innovation and Technology* 16(1): 1–42.

Redden J (2018) The harm that data do. *Scientific American* 319(5).

Ricaurte P (2019) Data epistemologies, the coloniality of power, and resistance. *Television & New Media* 20(4): 350–365.

Sagarra O, Hoffmann X, Clotetet X, et al. (2019) Final report on the Barcelona pilots, evaluations of BarcelonaNow and sustainability plans. Available at: https://decodeproject.eu/file/702/download.pdf (accessed 7 October 2024).

Scassera S, Martinez Elebi C and Buxton N (2024) *Digital colonialism: Analysis of Europe's Trade Agenda*. Amsterdam: Transnational Institute.

Shumailov I, Shumaylov Z, Zhao Y, Gal Y, Papernot N and Anderson R (2023) The curse of recursion: Training on generated data makes models forget. *arXiv*. Available at: https://arxiv.org/abs/2305.17493 (accessed 13 December 2024).

Stark L and Hutson J (2022) Physiognomic artificial intelligence. *Fordham Intellectual Property, Media and Entertainment Law Journal* 32(4): 922–978.

Taylor J and Kukutai T (2016) *Indigenous Data Sovereignty*. Canberra: ANU Press.

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

Taylor L (2021) Public actors without public values: Legitimacy, domination and the regulation of the technology sector. *Philosophy & Technology* 34(4): 897–922.

Taylor L, Martin A, de Souza SP, et al. (2023) Why are sector transgressions so hard to govern? Reflections from Europe's pandemic experience. *Information, Communication & Society*. DOI: 10.1080/1369118X.2023.2264919.

Tierra Común (2021) Interventions for data decolonization. Available at: https://www.tierracomun.net/en/home (accessed 16 November 2023).

University World News (2021) New EU law needed to protect universities from big tech. Available at: https://www.universityworldnews.com/post.php?story=20210115122001617 (accessed 24 April 2024).

Veale M and Zuiderveen Borgesius F (2021) Demystifying the draft EU artificial intelligence act — Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International* 22(4): 97–112.

World Economic Forum (2011) Personal data: The emergence of a new asset class, World Economic Forum.

Available at: https://www.weforum.org/reports/personal-data-emergence-new-asset-class/ (accessed 4 July 2022).

WTO and WEF (2022) The promise of TradeTech policy approaches to harness trade digitalization. Available at: https://www.wto.org/english/res_e/publications_e/tradtechpolicyharddigit0422_e.htm (accessed 5 April 2024).

Wylie B, McDonald S and Maher S (2018) Data trusts–Defining what, how and who can use your data. *Democracy*.

Yandrapalli V (2024) AI-powered data governance: A cutting-edge method for ensuring data quality for machine learning applications. In: *2024 second international conference on emerging trends in information technology and engineering (ICETITE)*, Vellore, India, 22–23 February 2024, pp.1–6. IEEE.

Yasmin A (2021) Why WhatsApp users in Europe can opt-out of New WhatsApp privacy policy but users in India cannot? Available at: https://www.indiatoday.in/technology/news/story/why-whatsapp-users-in-europe-can-opt-out-of-new-whatsapp-privacy-policy-but-users-in-india-cannot-1793555-2021-04-21 (accessed 28 April 2022).