UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks

Bodó, B.; Irion, K.; Janssen, H.; Giannopoulou, A.

DOI
10.14763/2021.3.1581

Publication date
2021

Document Version
Final published version

Published in
Internet Policy Review

License
CC BY

Link to publication

Citation for published version (APA):
Bodó, B., Irion, K., Janssen, H., & Giannopoulou, A. (2021). Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1581

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:17 Nov 2026

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 10 **Issue** 3

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks

Balázs Bodó *University of Amsterdam* bodo@uva.nl
Kristina Irion *University of Amsterdam***Heleen Janssen** *University of Amsterdam*
Alexandra Giannopoulou *University of Amsterdam* a.giannopoulou@uva.nl

DOI: https://doi.org/10.14763/2021.3.1581

Published: 30 September 2021
Received: 21 February 2021 **Accepted:** 21 May 2021

Funding: The article writing was supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under grant agreement No 759681.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.
Licence: This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. https://creativecommons.org/licenses/by/3.0/de/deed.en
Copyright remains with the author(s).

Citation: Bodó, B. & Irion, K. & Janssen, H. & Giannopoulou, A. (2021). Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1581

Keywords: Data governance, Data ordering, GDPR, Data intermediaries, Data sovereignty

Abstract: The technological infrastructures enabling the collection, processing, and trading of data have fuelled a rapid innovation of data governance models. We differentiate between macro, meso, and micro level models, which correspond to major political blocks; societal-, industry-, or community level systems, and individual approaches, respectively. We focus on meso-level models, which coalesce around: (1) organisations prioritising their own interests over interests of other stakeholders; (2) organisations offering technological and legal tools aiming to empower individuals; (3) community-based data intermediaries fostering collective rights and interests. In this article we assess these meso-level models, and discuss their interaction with the macro-level legal frameworks that have evolved in the US, the EU, and China. The legal landscape has largely remained inconsistent and fragmented, with enforcement struggling to keep up with the latest developments. We argue, first, that the success of meso-logics is largely defined by global economic competition, and, second, that these meso-logics may potentially put the EU's macro-level framework with its mixed internal market and fundamental rights-oriented model under pressure. We conclude that, given the relative absence of a strong macro level-framework and an intensive competition of governance models at meso-level, it may be challenging to avoid compromises to the European macro framework.

This paper is part of **Governing "European values" inside data flows**, a special issue of *Internet Policy Review* guest-edited by Kristina Irion, Mira Burri, Ans Kolk, Stefania Milan.

Note: all authors contributed equally to the development of ideas and to the writing of this article.

1. Introduction

Data can be extracted and processed by private parties and governments at unprecedented scales, speed and efficiency. Such data's fate is under intense debate, which takes place at multiple levels, ranging from the individual, micro-level strategies, via the meso-level approaches experimented by data sharing organisations, such as firms and municipalities, to how countries, competing on the global level, define strategic frameworks around data at the macro-level. Albeit data is not entirely lawless, there is much uncharted terrain opening spaces for competing logics of data governance.

1.1. Levels of data strategies: micro-, meso- and macro-level approaches

While the production, use and trade in data may seem intransparent at best, chaotic at worst, it is certainly not without structure. In the last decade a number of different data governance models emerged, both at the macro-level, and on the more context-specific meso-level. On the macro level, there are substantial political differences between the United States (US), the European Union (EU), and for example China, about the role data is envisioned to play in the economy, or in the or-

ganisation of the social-political order (e.g. Aaronson and Leblond, 2018; O'Hara and Hall, 2018; Goldfarb and Trefler, 2018). These differences play out in the political, legal and economic frameworks that define (personal) data governance at the macro-level, such as the EU General Data Protection Regulation (GDPR) (Granger and Irion, 2019), the piecemeal, sector-specific, but generally business-friendly approach which characterises the US (Chander, 2014), or the Chinese approach which harnesses its social credit system as a disciplinary mechanism (Backer, 2019; Mac Mac Síthigh and Siems, 2019).

At the meso-level, there is considerable variation in technical, legal and normative frameworks that govern the production, extraction and exploitation of data. Different firms, industries, governments and municipalities, and a diverse group of techno-legal driven communities came up with their own data governance practices, frameworks, technologies, such as data sharing agreements, data trusts and cooperatives, or distributed ledgers and personal data stores. The large variations between approaches to govern data can be attributed to the field being relatively nascent, and the fact that 'good' governance of data (Mann, Devitt, and Daly, 2019) depends on the highly specific conditions in which data is being extracted, used and traded. This paper is looking at data from a broad perspective, and it interrogates how different meso-level data governance regimes develop in the context of their macro-environment.

Various stakeholders have defined their own approaches to how they organise their data related practices. The bulk of meso-level governance regimes were developed by economic actors, often before any overarching macro-level framework emerged, and are shaped by technical capacities, and business interests. A second set of data governance logics emerged in the public sector. The making available of public sector information to the public in general, and for commercial uses, has released large caches of information with relatively few restrictions. Last but not least, a number of governance models, such as distributed ledgers or data commons, have emerged as counter-practices, defined in opposition to dominant public or private data regimes. Some of these counter-initiatives are heavily technological in nature, such as individual data control technologies developed by crypto-libertarian communities.

By now, we may have entered a next stage of consolidation, where economic, geopolitical and ideological differences over data play out, and are contested to the point where more successful data governance frameworks crowd out others. We argue that this consolidation process is also a product of the interaction between vertical layers of data governance: the macro-level political regimes can

favour particular meso-level strategies at the expense of others, while pressure from organisations operating at meso-level influence macro-level legal) frameworks on data.

1.2. Moving forward at macro-level is largely shaped by meso-level approaches to data

Despite all the variety, the dominant meso-level practices seem to suffer from serious shortcomings, independent of how the data is being treated. On the one hand, the problems with the dominant data appropriation logics are well known. A substantial part of our social and economic interactions take place within often private, and often inaccessible and largely opaque technological and business-driven ecosystems. The fact that this happens at scale, creates immense social, economic and political power, and information asymmetries between those who control data *vis-à-vis* other businesses, governments, individuals and communities. On the other hand, even in those cases where data is on the move, and widely traded, serious issues have emerged. The current macro-level data governance frameworks for data trade have largely failed to produce transparent and functioning data markets. It is nearly impossible to ensure that individual rights are not breached in the course of, or as a result of such transactions, and there are indications of irregular and shady data markets, while regular practices of data sharing and trade may remain underdeveloped. In short, the current macro-level data governance regimes produce inadequate results both when the data is static, and when it is the subject-matter of transactions.

1.3. Research objective and plan

The hypothesis of this work is that any solution to the aforementioned issues must appear as an alternative data governance logic at the meso-level. European policy-makers, public and private sector organisations and civil society have to focus on exactly this data governance space between macro-level data governance frameworks and data producers, because this is where the different logics, visions of data ordering and governance are competing for social, political and economic recognition, adoption, and success. The research was carried out to underpin this scientific statement. This article uses socio-political-legal research methods and literature review to interrogate the interaction between macro- and meso-level governance of personal data. That said, we do not attempt to conceptualise an all-encompassing global data governance framework. Our discussion paints a rather limited picture of macro- and meso-level data governance regimes, whereby our work focuses on personal data protection and flows thereof.

The article is structured as follows. In section 2, we introduce leading macro-level regimes that govern personal data and their interactions, with a special focus on the EU approach. In section 3, we turn to the discussion of meso-level data governance frameworks. We start with spelling out the expectations vis-à-vis *a good enough* data governance framework, then we match the currently competing alternatives against this background. In section 4, we conclude with an analysis of how the macro- and meso-level frameworks may interact, so the outcome of the competition at the meso-level results in successful governance frameworks that map closely the characteristics of good enough data governance.

2. Macro-level approaches to governing personal data

In the digital era, data emerged as a key asset in the global economic competition among world powers. Especially macro-level regimes on personal data catalyse ideological differences. On the one hand, the treatment of personal data carries the often pre-digital social, economic, political conditions which produced data-related regulation in the past. On the other hand, the national, regional ambitions, strategies, priorities in the global competition for economic power, political hegemony, innovation play-out over the macro-level approaches to personal data.

Whilst the interconnectedness of the global digital ecosystem generates increasing interdependence between countries and regions, distinct approaches to data ordering and governance remain. It has been argued that the US, China, and the EU have construed contrasting data realms (Aaronson and Leblond 2018) where domestic legal traditions and variations of capitalism have configured a distinct approach to data governance. O'Hara and Hall (2018) label the US approach libertarian and commercial, that of China authoritarian, and that of the EU, which emphasises human dignity, as—indeed—"bourgeois", whereby this framing suggests a certain fallacy in the sense that the EU tries to compete on ethics and values instead of unleashing the economic power of data.

Goldfarb and Trefler (2018) who attest to a fundamental regulatory tension between countries' approaches to data see a comparative economic and innovation advantage for countries with a lax regulatory framework for data. Strict data privacy protection, for example, is often considered fundamentally at odds with the insatiable appetite of big data and machine learning applications for exactly that data (O'Hara and Hall, 2018). Yet, in championing fundamental rights, the EU is largely regulating digital platforms and online services that are supplied from outside the EU, notably from the US. This export of EU rules is contested by political and commercial stakeholders who emphasise digital innovation and the free flow

of (personal) data that can help evade claims of authority and jurisdiction (Irion, 2021).

We now provide a brief overview of these approaches to personal data governance in the EU, the US and China in order to highlight the dynamics between the macro- and meso-levels. On the one hand, macro-level legal regimes pre-structure meso-level data governance by public and private entities in these jurisdictions. On the other hand, stakeholders seek to influence macro-level outcomes that endorse their preferred meso-level approach to data governance. This tension is most explicit in the EU context of personal data rules and its contestation.

2.1. EU macro-level data governance approach

Europe conceives of the digital world through its history and commands respect for fundamental rights and European values as a basis for forging trust in the digital transformations that European societies are undergoing. To the European Commission (2020a) "this digital Europe should reflect the best of Europe - open, fair, diverse, democratic, and confident". EU policy on data seeks to design governance models that enable regulators, industries, communities and others engaging in the processing of data for their own and/or other interests, in line with democratic standards, the rule of law, and societal needs more generally. The EU envisions trustworthy data governance that reconciles responsible and human centric data governance, subject to full compliance with the EU's strict data protection rules, *while* enabling data governance to foster innovation, and to drive economic growth (European Commission 2020a).

2.1.1. The EU mixed approach: fundamental rights and free flow of data

The data strategies of the EU and its member states (European Commission 2020a) put data at the centre of the digital transformation. As the European data strategy (ibid.) stipulates: "In order to release Europe's potential, we have to find our European way, balancing the flow and wide use of data, while preserving high privacy, security, safety and ethical standards". In broad strokes, the macro-level approach of the EU is characterised by strong fundamental rights safeguards, an EU internal market in which data can circulate freely and, increasingly, data sharing obligations either for specific types of data or sectors. In the following, we will briefly revisit the main features of European data law, which pre-structure the data governance regimes in Europe.

2.1.2. Fundamental rights approach to personal data

Article 8 of the EU Charter of Fundamental Rights enshrines the fundamental right

to data protection, among a range of other fundamental rights, such as the right to privacy, non-discrimination, or freedom of expression rights. The right to data protection is given further substance at ordinary legal EU-level, in the General Data Protection Regulation (GDPR; (EU) 2016/679), which guarantees fundamental rights of individuals while contributing to the EU's internal market objective. The GDPR guarantees a high-level personal data protection by offering individuals transparency and mechanisms to control the processing of their data, including rights pertaining to their data, while imposing a range of obligations and responsibilities on those who are determining the purposes and means of the processing of personal data. The GDPR applies across nearly all sectors in society, both public and private.

As a key concept, Article 4(1) of the GDPR defines personal data as "any information relating to an identified or identifiable natural person ('data subject')". The tendency to apply a broad interpretation in defining personal data is aligned with the CJEU's repeated affirmations of "ensuring effective and complete control of data subjects", which is the aim of data protection law (CJEU, 2014; Irion, 2016). However, the concept of personal data "comes with considerable legal uncertainty" (Drexl, 2019), as it relates to another unclear concept—namely that of identifiability. As the contours of the concept of identifiability remain foggy, it has been claimed that this broad interpretation of personal data—even if welcome—could lead to all data being considered as personal, inherently triggering the application of data protection law (Purtova, 2018). This regime can be simultaneously applicable to other data types along with other data regulatory regimes, such as machine-generated data, public sector data, or derivative data. As a result, the distinction between personal and non-personal data is far from clear-cut (Finck and Pallas, 2020).

2.1.3. Open data and data sharing

Open data and data sharing are a central policy objective in the EU framework. The reuse of public sector data, including from public undertakings, and data from publicly funded research for re-use is regulated by the Open Data Directive (EU) 2019/1024). Data sharing in the private sector is based on emerging, circumstantial or sector-specific arrangements, addressing for example payment service providers, electricity network data or agricultural data. New initiatives by the European Commission (2020a) aim to extend this model to the establishment of European data spaces, where data can seamlessly flow across sectors and domains, in compliance with EU norms.

2.1.4. Digital sovereignty

Recently EU policy has become more concerned over digital sovereignty which refers to Europe's ability to act independently in the global digital environment (Madiega, 2020; Roberts et al., 2021). The EU and member states highlight many digital sovereignty issues across domains and sectors, such as computing power, control over EU data and secure connectivity. The EU 'Strategy for Data' (European Commission 2020a) stresses the link between digital sovereignty and jurisdiction. In the global interconnected digital ecosystem, there are increasingly competing claims of jurisdiction, for example with non-EU companies, stemming from extraterritorial disclosure requests by third country governments (Irion, 2012; Madiega, 2020). At the EU level, there is now more attention to jurisdiction in the cross-border supply of digital services, especially in the field of cloud services (European Union, 2020; Roberts et al., 2021). Meanwhile, European policy is still inconclusive as to how better recognition for data sovereignty can be reconciled with cross-border data flows and digital trade.

2.2. US macro-level data governance approach

In contrast to the EU approach, the US approach lacks a federal level, comprehensive data protection regulation for the private sector (Chander, Kaminski, and McGeveran, 2021). Instead, federal law on privacy is specific to particular sectors and activities, such as for example the Children's Online Privacy Protection Act (COPPA), the Gramm Leach Bliley Act (GLBA) concerning data collected by the financial service industry, the Fair Credit Reporting Act (FCRA) concerning credit data; the Health Information Portability and Accountability Act, protecting health information. Their sectoral regulation (instead of overarching federal legal provisions), the fact that the federal legislative branch has largely been weakened, and their (partly) 'lenient' legislative approach to data privacy is often seen as one of the drivers that has facilitated the emergence of a multibillion-dollar data industry in just a few years (Chander, 2014; Willis et al., 2018).

The outcome is a particular techno-legal hybrid, in which lenient data privacy legislation permits sophisticated private regimes that maximise value extraction from personal data. Consider for example the growth of marketing tech firms from 150 in 2011 to more than 8,000 in the year 2020 (Brinker, 2020). This industry grows on, enables, and nearly exclusively profits off data extraction, analyses, and sharing of data. Their highly sophisticated technological solutions move around and monetise data with extreme efficiency. This is possible because there are few legal hurdles hindering such data flows. In the beginning there have been little restric-

tions on the export of personal data and often these rules were rather malleable to business needs.

In the international context the US business-led paradigm on personal data has not only taken a commercial stronghold domestically, it has moreover been able to expand at a global scale. Online platforms which have become paradigmatic of today's digital ecosystem testify to the powerful economies of scale and scope that can be built on data. Political scientists caution against the concentration of data in very large corporations who can scale-up their data-based operations for their private benefit (Spiekermann et al., 2019). Also, the European Commission states that "in the US, the organisation of the data space is left to the private sector, with considerable concentration effects" (European Commission 2020a). This concentration of centrally held data, in walled gardens of large internet companies (e.g. online platforms), is increasingly seen as an impediment for an open competition in a global, data-agile economy (European Commission, 2020a).

In recent years, there has been a surge of data privacy laws at the state level, with the 2018 adoption of the California Consumer Privacy Act (CCPA) being the most influential legislative initiative (Chabinsky and Pittman, 2020; Chander, Kaminski, and McGeveran, 2021). State legislation on data privacy is believed to spur the US legislator's efforts to pass a federal consumers' data privacy law that would in turn preempt state laws. The latest developments signify a re-valuation of an individual's right to data privacy in commercial settings; however, legislation is not believed to go as far as the EU's GDPR (Chander, Kaminski, and McGeveran, 2021).

2.3. China's macro-level approach to personal data

The Chinese macro-level approach to data is currently an inward-facing regime, which combines private sector interests with the coercive powers of an authoritarian state. The Chinese social credit system personifies the inward facing direction of a data regime that serves as a totalitarian, reputation-based control of all aspects of life of a billion-plus population (Mac Síthigh and Siems, 2009). The system is based on the reputation ratings of individuals, businesses, public and private institutions, which are then aggregated through a tightly controlled cooperation of public and private entities. Positive and negative ratings can be accumulated through bad, or good behaviour: such as late payment of bills or blood donations, liquor or contentious books purchases and customer satisfaction, regime-critical or supportive social media posts. These ratings are then used to regulate access to a growing number of private and public services, from childcare, to high speed travel and even low interest rates. This approach substitutes "governance through mea-

surement, assessment, and reward for obligation to obey the command of statute, regulation, or administrative decision" (Backer 2019, p 210).

The Chinese social credit system prioritises social control, communal interests, integrity, transparency, and accountability at the expense of the privacy and personal autonomy of the individual. It is argued that the system rewards honesty with economic opportunities, such as financial credit, while the blacklists may encourage individuals, such as debtors, to comply with court judgments (Mac Síthigh and Siems, 2009). All the while the same system is purportedly designed to keep government officials impartial, transparent and accountable. This use of data serves to reinforce and enforce norms that already exist in the country's legal and extralegal norm system, and that it addresses the shortcomings and inefficiencies of the traditional state institutions (Dai, 2020). In a more skeptical interpretation, it extends and reinforces the powers of an authoritarian state to all aspects of the individual and the social.

Besides, China's 2017 Cybersecurity Law has imposed several restrictions which aim to safeguard cyber security, protect cyberspace sovereignty and national security (Gao, 2021). Among others, this law requires operators of critical information infrastructure to locally store personal information and important data collected and generated in their operations within China (ibid.). What constitutes critical information infrastructures is broadly defined and covers many online activities. As a result, most personal data collected by Chinese online operators has to be locally stored in China. That means that Chinese operators can receive personal data in the context of their domestic and international activities but this data cannot leave China unless there is a government permission. In late 2020, the Chinese government published the draft of a new comprehensive data protection law. This draft contains several GDPR-style principles, such as transparency, fairness, purpose limitation, data minimisation, limited retention, data accuracy and accountability (Yin and Zhang, 2020).

2.4. EU's interface with other macro-level data governance approaches

In the presence of a global digital ecosystem, the EU regime on personal data does not operate in isolation but co-exists and interacts with legal regimes in other parts of the world. Data can easily be moved across EU borders and regions, and be stored and processed in a decentralised manner, while becoming accumulated and oftentimes turned into a "proprietary" resource. There are different approaches to governing personal data and the flow of data across borders.

The GDPR has been heralded as a successful global standard-setter, rendering it an often-cited example for the so-called "Brussels effect" (Bradford, 2012; Gady, 2014). Clearly the GDPR has inspired data protection legislation elsewhere in the world (Greenleaf, 2012); however, the EU approach has also been contested for its procedural formalism when protecting personal data, and for a certain lack of effective enforcement (Bamberger and Mulligan, 2011; Granger and Irion, 2018). It is unlikely that a US approach to consumer data privacy will converge with the EU's fundamental rights approach to personal data protection. The US is rather believed to incubate its own template for consumer privacy protection (Chander, Kaminski, and McGeveran, 2021). Also, the Chinese initiative to introduce better protection for personal data in the private sector would not be about individuals' empowerment and fundamental rights, as it does not aim to reduce *government's* control over all public and privately held personal data.

It turns out that the interaction between different legal regimes at the meta-level also matters for data governance given that certain approaches are clearly designed to extract data from other regimes whenever possible. The US data governance framework is the most open, however bearing in mind that it dominates the commercial internet and has incubated the platform economy. The EU would be regarded semi-open because it seeks to maintain the fundamental right's protection by placing conditions on the export of personal data (European Commission, 2017). China, by contrast, treats the personal data its local digital technology companies have gathered as a national resource. This creates particular dynamics among each of these jurisdictions where the US private sector still benefits most from the flow of personal data across borders, China does not partake and instead aims to incubate its own digital champions, and the EU struggles to reconcile its high level of personal data protection with cross-border data flows.

In this context, the semi-open EU data protection law appears rather exposed and inconsequential because it did not yet forge usable legal interfaces with other data realms that would prevent circumvention of its rules. For meso-level data governance approaches embedded in EU data law, incubating good enough data governance practices has been a challenge, just like anywhere else. It is possible that the macro-level governance of personal data in the EU does not stimulate enough meso-level approaches that internalise the protection of personal data differently than the prevailing business logics.

3. Meso-level approaches to govern data

Technological innovation yielded highly sophisticated technological infrastruc-

tures to collect, store, analyse, and trade vast amounts of data, and their derivatives. These developments fuelled a rapid, parallel innovation of meso-level data governance approaches. Though still fluid and dynamic, meso level governance practices started to coalesce around a number of basic models: (1) business and platform logics to data governance; (2) public sector information logics; (3) technological and legal mechanisms that seek to empower individuals; and (4) community-based data logics.

In this section, these models of what a 'good governance' perspective entails, will be introduced, compared and assessed. The section starts from the assumption that the approaches are in essence competing with each other for adoption by data subjects, businesses, and communities. Their success in this process depends on a number of factors: compliance with the EU macro-framework, cost, ease of use, and/or efficiency. But, as we spell out in this section, good data governance is more than that, and as the US macro framework shows, if data governance approaches compete nearly exclusively on business efficiency terms, the most successful approach may not be the socially most beneficial, just or desirable. We first present a tentative list of desirable data governance properties, based on relevant literature. Then we introduce the four competing models and compare them against these properties.

3.1. Some dimensions of good enough data governance

There is to date no generally accepted comprehensive list of requirements for good enough data governance, but an emerging body of literature that emphasises certain goals and practices that speak to the quality of data governance regimes (Daly et al., 2019; Hardinges et al., 2019; Hardjono, Shrier, and Pentland, 2019; Langford, 2000; Mozilla Insights et al., 2020). These include:

- **Safeguards of normative interests.** Good data governance must ensure the adequate protection of fundamental rights (privacy, non-discrimination, freedom of speech, right to an effective remedy access to a court, etc.) (Trenham and Steer, 2019), other public interest objectives, and safeguard equitable benefits from the use of data.
- **Minimise negative and maximise positive externalities to individuals, communities, and society as a whole.** Data governance should contribute to a just distribution of the power and benefits generated from the use of the data. According to Lovett et al. (2019), this includes that data governance is respectful of particular cultural, social sensitivities, especially when data can be linked to well-defined groups and communities based on ethnicity, language, religious beliefs, or other elements of shared identity. We would add that these considerations are readily applicable to many other,

western forms of community and social organisation.

- **Scalability and interoperability**. Data governance must be able to scale according to the number of data subjects, data users, and the amount of data (Mozilla Insights et al., 2020). If the model does not scale well, the cost of shifting between different governance models must not be prohibitive. In general, different data governance models need to be interoperable and must not limit the choice and mobility of various stakeholders.
- **Context-sensitivity and sectoral fit.** Data governance models should reflect the specific limitations, concerns, sensitivities of the context as defined by data subjects, the data in question, or the potential data uses. Non-personal machine generated data in the energy sector may require different data governance regimes than, say, the learning analytics data of children from vulnerable groups.
- **Proportional and transparent trade-offs between risks and benefits.** Every choice between different governance models, and every decision taken within one may lead to unforeseen harm and uncertainties regarding benefits. Risk impact assessment must establish transparency of how potential harms and benefits are distributed across stakeholders, define standards of acceptable/unacceptable risks. Effective and proportional mitigating measures need to be in place and address the negative effects and preserve the trust in the governance model.
- **Transnational capacity.** The issue of transnational data flows and jurisdictional data sovereignty are contentious economic, political issues. While transnational capacity should also preclude practices of data extractions, it should not stand in the way of global interconnectivity and international participation in value creation from the data. For example, data governance should achieve that data can be queried and used so that it contributes to value creation, however, without that, the data itself is transferred to, sold to or shared with third parties (Hardjono, Shrier and Pentland, 2019).

These data governance specific considerations must be provided for by the institutional design of governance itself. Even if the data collection and use is taking place within the walled gardens of a corporate data controller, similar, internal data governance mechanisms must be in place to comply with, if nothing more, that controller's internal rules, GDPR—and other rights. For data intermediaries, and open technical infrastructures, the question of governance is equally and maybe even more directly relevant, either at the data, or at the technology level.

3.2. Competing logics of data governance

Having identified a set of requirements for good enough data governance, we now compare and evaluate the competing governance models. The meso-level data

governance models have been grouped following their main logic: (1) business and platform logics to data governance; (2) Public sector information logics; (3) technological and legal mechanisms that seek to empower individuals; and (4) community-based data logics.

3.2.1. Business and platform logics to data governance

Most of the successful (in terms of business performance) data practices evolved in the US context (Varian and Shapiro, 1999). The already powerful credit rating and marketing industries provided the templates for the monetisation of the newly discovered forms of digital data (Lauer, 2017). Emanating from the US, a particular data-driven business logic that treats personal data as an asset or resource that serves to maximise extraction of profitable value, could take a foothold. This developed out of a *res nullius* perspective, where societal and individual normative interests and safeguards, context sensitivity relating to societal sectors seem non-existent. Businesses largely prefer governance models that help maximise these, to optimise accuracy, to enhance the speed of processing, and to enlarge computational resources that enable them to use (potentially rights-invasive) techniques such as automated decision-making or AI. These governance models are designed to deliver services in a highly competitive market (Baumer, 2014), and are supported by legitimised business secrets that help secure and further strengthen the market and information position of businesses *vis-à-vis* individual stakeholders in the data market (Janssen, 2020b). This business model has greatly contributed to a nearly unlimited growth of economically successful data-driven business and platforms in the US and across the globe.

EU-based businesses and platforms are largely driven by the same incentives, interests and logics as their US counterparts, but they had to internalise the EU's data protection framework. The GDPR framework forces them to comply with rights and interests of individuals which are external to their own logics. However, despite EU-wide applicable uniform legal mechanisms to secure equitable data governance across the EU, platform and business logics have largely dominated present data governance models at meso-levels during the last decade—also within the EU. Several different causes have led to the creation of conditions for the dominance of business and platform logics; here, we mention the most important ones.

EU law, particularly when poured into a Regulation, generally aims at unifying its application to secure an equal level playing field across the Union. For instance, the GDPR and the EU Charter of Fundamental Rights and the case law pertaining to these rights apply uniformly in all member states. However, given that the GDPR

entered into force in 2018, today's practices have largely manifested under its predecessor, the 1995 Data Protection Directive (DPD) and attendant enforcement structures by national data protection authorities in the member states. That is, not all national regulators were stringent on DPD compliance and enforcement, which led platforms and businesses to settle where the least strict compliance and enforcement were implemented.

While the uniform GDPR's norms gradually take hold, the legacy of national oversight mechanisms—as the GDPR tasks national bodies with oversight again—still carries on. Data protection authorities in the member states may lack the means—in terms of expertise, manpower, and access to an organisation's intentions, motivations and behaviours, or lack of insight in an organisation's complex technical systems—to properly fulfil their oversight task. Notably, (foreign) businesses and platforms have calculated and settled in the member state with the 'weakest' or 'more favourable' regulator—permitting them to enlarge opportunities to create their own data governance models, as chances that the regulator strictly enforces are minimal (Venkataramakrishnan, 2021).

The accomplishment of the now dominant business and platform logics towards meso-level data governance, which are not bound by EU rules (unless they act under EU law), has caused concerns among EU businesses, in that the EU rights and values driven governance frameworks are too restrictive, thereby putting them into a competitive disadvantage compared to their US-based and Chinese competitors.

Where novel space of data governance at meso-level occurs—much under the pressure of opening-up data markets and public organisation-held data sets—the current platform and business logics might likely continue shaping and moulding the meso-level data governance approaches. However, regulators, at least those in the EU, are more wary about platform and business logics at meso-level that underpin proprietary data concentration. The European Commission has recently tabled three bills (the Data Governance Act, the Digital Markets Act and the Digital Services Act), which aim for setting new rules for digital and data-driven businesses.

3.2.2. Public sector information logics

Governments and the public sector are important producers of data and it is in line with international best practices to release public sector information (PSI) for reuse. In its 2008 Recommendation the Organisation for Economic Coordination and Development (OECD) enshrines "openness as the default rule to facilitate access and re-use" of PSI (OECD, 2008). The rationale for setting PSI free is simple

and compelling: "to increase returns on public investments in public sector information and increase economic and social benefits from better access and wider use and re-use, in particular through more efficient distribution, enhanced innovation and development of new uses" (ibid.).

Next to considerations that the public has a right to access information and that public sector data is an important resource that can benefit society, another argument for opening up public sector data is that such data are generated with public funds, meaning that they should not be kept exclusive or that no new charges should be levied for its re-use. The Open Data Directive, which stimulates the re-use of open data for commercial or non-commercial purposes, is aligned with the European fundamental rights framework. As is customary, the Open Data Directive is without prejudice to the GDPR which protects individuals' personal data. A similar logic, by extension, has been applied to publicly funded scientific research data for which the Open Data Directive requires member states to adopt open access policies. A related European initiative is the European Open Science Cloud (EOSC) which is currently developed with the help of EU funds in order to create an environment for hosting and processing research data pursuant to the FAIR principles (Findable, Accessible, Interoperable, Reusable) (European Commission 2020b). The EOSC, which is still under construction, has been designated as one of the nine European Data Spaces envisioned by the European Data Strategy (European Commission, 2020a). Once fully operational, also the EOSC will be opened-up beyond the research community and connect with the wider public and private sector (European Commission, 2020a).

Considerations of scalability and interoperability are incorporated into the legal framework. The Open Data Directive seeks to enable access and re-use of open data for all interested actors in the market, thereby giving recognition to the non-rival property of data. With this in mind, the Directive significantly limits the use of exclusive arrangements between public sector bodies or public undertakings over access to data with third parties. Also, the principle of 'open by design and by default' seeks to reverse the mechanism of access to publicly held data away from having to make a request to proactive release of such data. How this gets translated into practice depends on member states' public sector and public undertakings to live by the principle 'open by design and by default'. The Directive gives due prominence to access "by electronic means, in formats that are open, machine-readable, accessible, findable and re-usable, together with their metadata" (European Parliament and the Council, 2019).

The Open Data Directive is premised on the overwhelmingly positive feedback

loop open data has in a data-driven economy and society. Following a critique, however, open data policies disproportionately benefit those private actors that command the necessary capabilities to extract value from 'big data' and that this—similar to a critique of public data—promotes inequality (Spiekermann et al., 2019). Kitchin (2013) in his 'Four critiques of open data initiatives' argues that "the real agenda of business interested in open data is to get access to expensively produced data for no cost, whilst [...] weakening [governments] position as the producer of such data". Collington (2019, p. 8) argues that the costs of producing open data "fall largely on the public sector and society, but the surplus value so often comes to be realised by large digital platform companies and the financial services industry". There is also a geopolitical argument to be made that EU open data are released to the world and not only to European taxpayers whereby beneficiaries in third countries are not contributing to European societies. Currently there is very little research available about the value creation from open data and how it benefits European societies.

Moreover, while publicly funded data has to be open and released, private sector data is conventionally treated as an exclusive resource that is constitutionally protected under the freedom to conduct a business (Article 16, EU Charter of Fundamental Rights). However, there is a nascent school of thought highlighting that also business-to-government data sharing should be better enabled (High-Level Expert Group, 2020). Moreover, what has become known as reverse PSI (Poullet, 2020) is the idea to introduce mandatory data sharing obligations on private sector actors for data that is of high interest for the public sector and society. The French Digital Republic Bill is a case in point, as it contains a list of privately held data which have to be shared with the public sector and disclosed as a public record.

3.2.3 Technology-based data governance logics

The technological toolbox, another approach shaping data governance at meso-level, aims at facilitating individual data autonomy (Pohle and Thiel, 2020; Summa, 2020) and is rapidly expanding. The objective and consistent claim of these approaches is to empower individuals, by giving them tools to manage their data, and—ultimately—to achieve informational self-determination. In particular decentralised technical tools, such as personal data stores (PDSs) and distributed ledgers, are gaining momentum, positioning themselves as novel meso-level socio-technical alternatives for new data governance strategies.

Stemming from private companies with commercial interests, from public actors

and government initiatives, or from bottom-up community projects, distributed ledgers and related decentralised design approaches are getting more established in the global data governance space. Similarly, technological solutions such as PDSs, or technical architecture offered by private platforms that seek to assist individuals in managing their data, are emerging in the data marketplace. Overall, their objectives are similar: to empower individual users with more transparency and control over the processing of their personal data.

Many of the technological intermediaries seek to tackle the growing information and power asymmetries between big platforms and individual users, thereby bringing the data processing close to individuals. Rather than bringing the data for the processing to big platforms, the compute is brought to the data—hence the decentralisation aspect. Decentralised data processing and 'self-sovereign identity' solutions are progressively receiving institutional, social, and regulatory attention for their potential to reshape current data governance (European Commission, 2020a). Coupled with the decentralised architecture on which they are based, blockchains also present tamper-proof and record keeping abilities. This positions the technology in the data marketplace, potentially supporting the objective of individual empowerment over data capture, data analytic and data sharing.

Self-sovereign identity technologies. Popularised by the German Constitutional Court Population Census case (1984) the right of informational self-determination is formally defined as "the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others" (Gutwirth, 2009, p. 45). It ensures that restrictions on this right by the state have to be based in law, while any restriction must be necessary and proportionate to the aim pursued by that restriction. The latest European Commission document on the creation of a European strategy for data highlights the need "to give individuals the tools and means to decide at a granular level what is done with their data" (European Commission, 2020a, p. 10). In particular, it highlights the promises that decentralised tools such as distributed ledgers, personal data stores and other technical architectural design might help individuals "manage data flows and usage, based on individual free choice and self-determination" (p. 11).

Within the technological realm of tools for individual empowerment self-sovereign identity is gaining popularity. The term "self- sovereign authority" was first used in the blog *The Moxy Tongue* in 2012 in order to contest the dependent relationship between individual identity and the state, and proposing the decoupling of the existence of individual identities from this act of identity registration by/through

state actors (The Moxy Tongue, 2012, n.p.). The concept was recaptured by Christopher Allen (2016), who used it to describe a principle-based framework that would create a decentralised system of user-centric, self-administered, interoperable digital identities. This system is driven by ten foundational principles, following Kim Cameron's Laws of Identity (2005): 1) Existence, 2) Control, 3) Access, 4) Transparency, 5) Persistence, 6) Portability, 7) Interoperability, 8) Consent, 9) Minimalisation, and 10) Protection. It constitutes the latest evolution of digital identity representations, further separating it from centralised and federated models, and aiming to decouple identity issuance by the state in order to bring it under full control of the citizen (Giannopoulou and Wang, 2021, p. 3). Ultimately, self-sovereign identity "makes the citizen entirely responsible for the management, exploitation and protection of one's data" (Herian, 2018, p.115). While the implementations of the principles vary substantially, it can be said that self-sovereign identity aims to "enable a model of identity management that puts individuals at the centre of their identity-related transactions, allowing them to manage a host of identifiers and personal information without relying upon any traditional kind of centralized authority" (Fry and Renieris, 2020, n.p.).

Self-sovereign identity is "an identity management system created to operate independently of third-party public or private actors, based on decentralised technological architectures, and designed to prioritise user security, privacy, individual autonomy and self-empowerment" (Giannopoulou and Wang, 2021, p. 2). Its aim is to transcribe autonomy and individual control in technological design terms. Thus, technological *user-centric design* over the storage and access controls to personal identity data, appears to be the essence of any self-sovereign identity solution. Naturally, the degree to which these design choices manifest, varies depending on the objective in question. The objective of this architecture would be to create the conditions for data empowerment by design, giving data subjects the ability to both physically store their encrypted keys that unlock their identity features, and have access/use control over the whole or parts of their identity. The purported benefit from this design is that these features also prioritise security, encryption, and data minimisation by design.

Multiple projects promise to deliver individual 'data sovereignty' in a technological solution; one that embodies individual autonomy over one's personal data and individual control over their processing lifecycle. These solutions aim to achieve a network of interoperable identities, by redesigning the way authorisations in data flows currently operate. In practice, there is a considerable number of actors in this field, which has been recognised to fall under the—now general—denomination of

'self-sovereign identity'. While recognising that these projects are "still in their infancy", the Commission highlights the field's potential and examines what the appropriate regulatory environment that would manage to moderate these projects and accompany them towards their purported goal would be.

Personal data store technologies. Personal data store platforms provide an individual a technical device (the personal data store, or PDS) that allows individuals themselves to manage and take decisions over data capture, and over who can access and undertake data analytics over their data in that device (Janssen et al., 2020a). Individuals can also manage the transfer (the actual data sharing) of their data to an organisation. This can be raw data, or data from aggregate. Through the device, the data processing happens close to the individual (hence the 'decentralisation aspect'), rather than within the walled gardens of large, data driven internet companies, out of sight of the individual. In addition to the technical component, PDSs often entail terms of services that govern the PDS system, operating as means to ensure that an organisation's behaviour is compliant with an individual's preferences, and PDS platform requirements.

A PDS' empowerment aspirations are generally compliant with GDPR's guiding principles, and aim to improve transparency and an individual's management and control over the processing of their personal data (Janssen et al., 2020a). Yet, the effectiveness of PDSs, in their quest to empower individuals and to tackle the current information and power asymmetries, has recently been questioned (Janssen et al., 2020b). Once personal data moves beyond the device, control over how data is processed by data recipients is largely reduced. While decentralised data management might offer helpful user-oriented data management tools, PDSs remain grounded in the mistaken idea that with sufficient information presented in the right way, individuals will be able to overcome systemic asymmetries of information and power that were largely created by business logics at the same meso-level where PDSs operate. That is, PDSs do not alter the business logic created unequal distribution of understanding, knowledge, prediction, or risk assessment over a business' data processing. In all, decentralising data governance doesn't necessarily imply decentralisation of control (Janssen et al., 2020b).

Decentralised non-personal data exchange technologies. The European Commission's focus on facilitating the sharing of private sector data (e.g. of SMEs) underlines the need for developing new data governance for technological projects, which would be able to provide new architectural ideas for creating reliable data exchanges. Against this backdrop, decentralised data exchanges have recently emerged as a technological infrastructure solution, with the objective to ensure

data traceability, transparency and trust between data sharing parties. These exchanges are created using a decentralised architecture, which, with the help of a distributed network of participating nodes, avoids the storage and processing of data in centralised intermediaries. Decentralised data sharing ecosystems are designed to facilitate all types of data flows (such as machine generated data) on a large scale, without risking trust between transacting parties or trust in the quality of the data. This is supported by technological safeguards and by design encryption techniques, as well as governance choices, which aim to diffuse asymmetric power dynamics among transacting parties.

There is a wide variety in projects and companies that attempt to attest to these considerations and expectations. For example, private companies such as the Ocean Protocol promise to deliver a data ordering blockchain-based framework that would support distributed data marketplaces according to—sector specific or general—data needs. Sector-specific data marketplaces for automobile data, health data, or more broadly research data are also being developed.

The variety of tools facilitating efficient data exchanges promise to deliver on the recognised market and innovation potential of organised sector-specific or general-purpose data marketplaces. When the legal shortcomings in facilitating non-personal data exchanges between businesses or between businesses and institutions cannot be amended through effective legal reforms—as it has been consistently shown, attention shifts to technological infrastructures. Blockchain data exchanges provide a stellar example of these infrastructures.

3.2.4 Community based logics: bottom-up data intermediaries

The idea of data commons, data cooperatives, or data trusts (see a detailed taxonomy, and the analysis of the legal consequences of the terms below), termed by the Open Data Institute (ODI) as “data institutions”, is gaining traction in policy and practice. Notable is the initiative of the European Commission (2020c) to introduce and regulate “data intermediaries” in its proposal for a Regulation on European Data Governance (the “Data Governance Act”). In essence, data intermediaries aim to institute an intermediating governance layer between data subjects on the one hand, and data recipients (natural or legal persons who seek to use that data for commercial or non-commercial purposes) on the other. This data intermediary has a number of roles and responsibilities, which it exercises on behalf of, among other beneficiaries, data subjects and data users, via its own agency:

- It collects data from individual data subjects/sources;
- It stores/processes data of individual data subjects, or facilitates data

sharing and access arrangements, both legal, and technical, with data users and/or third parties;
- It enters into agreements with third parties and authorises/licences the use of the data aggregates and derivatives;
- It monitors, prevents unauthorised uses, and enforces agreements; and
- It captures value from data use and redistributes value to data subjects.

There are multiple domains in which similar arrangements exist. For example, in scientific research, scientists have long been aware of the need to define the conditions, and infrastructures of data sharing arrangements, and designed bespoke systems to fit their needs (Wilbanks and Friend, 2016). One of the key features of these arrangements is that they reflect the very specific situations in which the sharing of often highly sensitive data, such as health data, must be facilitated among a defined group of stakeholders, such as medical professionals, researchers, commercial companies, public health bodies, etc.

In the current EU regulatory landscape, individuals face similar limitations as intellectual property (IP) rights holders which arise from the comparable nature of the two information markets. Both legal frameworks create and allocate legal entitlements in the information with the data producer, that is the individuals, and the IP rightsholder. In both cases the meaningful exercise of those rights is limited by the transaction costs. The same way it is costly and difficult for an individual IP rights holder to monitor the use of their creations, negotiate use terms with IP users, and enforce their rights *vis-à-vis* unlicensed users (Landes and Posner, 2003), individuals' right to personal data protection is difficult to monitor (Giannopoulou, 2020). Solove (2013) argues that individuals cannot possibly keep up with privacy self-management given the sheer size of this task, information and power asymmetries. Despite the substantial differences between the nature, substance, purpose and destiny of the two fields of law (copyright and personal data protection), the nature of market failures in the two information markets are surprisingly similar.

Within the copyright domain, the solution to the transaction cost problem was to aggregate individual rights into Collective Rights Management Organizations (CRMOs) (Handke, 2014). To facilitate the licencing of copyrighted works where it was not always possible, feasible, or efficient, rights holders formed collective entities, which created pools of copyrighted works under a collective agency. CRMOs license the pooled works first on behalf of their members, or through extended collective licensing, on behalf of all rights holders. CMROs are legally empowered to license the pooled intellectual properties, monitor, and enforce copyrights, collect and distribute among their members remuneration. CRMOs also address the issue of imbalances in negotiation power between often powerful IP user organisations

(such as broadcasters, or digital platforms), and individual creators. This raises the question as to whether collective rights management intermediary institutions would address the problems of power imbalances, and the practical erosion of data subject rights in the data domain? Would such an approach be legally (or technically) possible?

Several exemplar data intermediaries have already been identified; the Open Data Institute, in its report on data trusts (Hardinges et al., 2019) lists various expressions of collective data agency of individual data subjects. *Data trusts* are modelled after legal trusts. Trustees of a data trust will take on responsibility (with some liabilities) to steward data for an agreed purpose. *Data cooperatives* are mutual organisations owned and democratically controlled by members, who delegate control over data about them. *Data commons* follow the institutional models around common pool resources, such as forests and fisheries. *Research partnerships* provide access to data to universities and other research organisations. The umbrella term of *data collaboratives* refers to such intermediaries that describes the collaborations between private data companies and the public sector (B2G) with the goal of engaging in data sharing activities in order to "generate public value".

All these different approaches establish a "middleman" with its own agency to remove some of the friction and transaction costs from data use, by establishing legal and/or technological vehicles of data stewardship. Unlike traditional data controllers who collect and use data from individuals (often) largely for their own benefit, and which tend to capture most of the value from such data use, data intermediaries are supposed to be independent from the prospective data users. Data intermediaries might, depending on their purpose, the parties involved, and the data held, be controlled by the stakeholders (e.g. data cooperatives) involved in the data intermediary. The data intermediary's obligations and responsibilities over decisions taken regarding the data processing, are supposed to be directed towards the beneficiaries.

These governance approaches are thought to have various benefits, such as the ability to balance conflicting views, and incentives about under what terms and conditions data can be shared and accessed. Collective data governance arrangements in data intermediaries may have a legally binding responsibility to address the interests of individuals, citizens and other beneficiaries. The decisions over data use and sharing can be more open, participatory and deliberative, so people have a say that they would otherwise not have, and the benefits of data use and sharing can be more widely, ethically and equitably distributed. One of the significant purported benefits of such intermediaries is that they might create entities

with comparable size, clout, and negotiating power as the giants in the digital economy may also seek to receive raw data or data aggregate that is produced and held by the intermediary. In this way, data intermediaries could balance out the information and power asymmetries currently tipped in favour of digital businesses (Delacroix and Lawrence, 2019). In that way, the concept of informational self-determination would be brought under a new light, that of empowerment through the collective.

However, issues remain with the various expressions of data intermediaries. It seems that we lack a legal formulation which would best circumscribe the purpose of data intermediaries. The UK common law based legal trust might be appealing, but as a common law concept, it is not as such immediately applicable in continental legal systems. Other legal forms, such as cooperatives, or associations, have their own limitations, which in similar cases, such as collective rights management in the copyright domain, have been overcome with special legal mandates that apply to the particularities of the necessary intermediation. Endowing these new data intermediaries with data, and rights to exercise powers and rights on behalf of their members might however be difficult, as not every right assigned to natural persons can be mandated or transmitted to a legal entity. Where data intermediaries might not be effective, or where imperfections occur in their management of the processing of data of their members, substantial technical and legal opportunities may largely remain for prospective data users to bypass the data intermediaries when acquiring the data. A data intermediary's benefits for commercial purposes have not yet been regulated. The draft Digital Governance Act (Chapter III, Data Governance Act) and the German legislative proposal regulating approved consent management services and end-user settings both propose a restrictive approach at this point (*§26, Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien of 2021*).

Also, and this seems to be the most consequential issue, all these arrangements assume that it is not only possible, but desirable to clearly define the group of data subjects, the scope of individual or personal data, and the purposes which could make up the collective arrangement. But such hard boundaries are rare, and more porous community, or stakeholder boundaries are prevalent. Extended collective licensing arrangements, common in the copyright domain, successfully developed to address similar challenges. It may be necessary that if the intermediary layer idea gathers momentum, similar extended powers should also be considered in the data space.

4. Conclusion

Digital data practices are in rapid flux and development. The same applies to the efforts which try to create some order in the creation, extraction, use, and trade in data. From a technical and business perspective, the data space is unified and global, with intense competition over unclaimed data resources. The legal landscape, meanwhile, is inconsistent and fragmented, while enforcement is often struggling to keep up with the latest developments. States are torn between conflicting objectives: on the one hand, opening up their data wealth for relatively unregulated reuse, and on the other, defining data as a basis of sovereignty, and competitive advantage. Individuals are consistently victims of extractive and also abusive data practices, even if they enjoy strong data protection rights. Technologists seek to offer tools of self-protection. Communities try to organise coordinated collective action at a scale.

As we have noted earlier, the interaction between meso- and macro-level frameworks, is bidirectional: macro-frameworks can shape all and favour certain meso-level governance logics, while local stakeholders—and increasingly also globally operating technology corporations—influence the macro-structures through political participation, economic activity, and various counter-practices.

The biggest tension in this relationship today is the apparent mismatch between the success criteria for companies competing in the global data economy at meso-level, and the semi-open fundamental rights approach of the EU's macro-level framework. There are many signs that point to this tension: the success of US firms which could accumulate clout before being subjected to EU rules, EU businesses voicing their concerns that the EU frameworks are too restrictive, thus putting them into a competitive disadvantage *vis-à-vis* US and Chinese competition; the political declarations of EU institutions which pay lip service to European values while continuously seeking to expand data access and sharing arrangements for economic ends in order to compete with the rest of the world. This comes to the fore in the language used in EU policy documents emphasising the need to balance competitiveness and fundamental rights considerations in the data space (e.g. European Commission, 2020a).

The meso-level governance logics are under dual pressure. On the one hand they need to comply with not one, but multiple macro-regimes, if they want to do business in those jurisdictions. On the other, meso-regimes also compete with each other for adoption by citizens, public and private stakeholders in the face of a still pervasive business logic of data accumulation and concentration. Under these con-

ditions, we see a real danger that the winning meso-logic will be the one which is the most successful within the global economic competition framework. Such an outcome would increase the pressure on the European macro-framework and slowly compromise its human rights and values-based attributes so that at some point, it starts to emulate its macro-competitors, such as the US and China. Given that Europe's macro-level framework is still much better aligned with good data governance practices aspired to at the meso-level, such an outcome would be dramatic for their ability to persevere and succeed. Yet, the Commission's proposal for a Data Governance Act that gives some legal recognition to "data intermediaries" could be a step in the right direction.

The plethora of new data governance logics, especially data intermediaries, certain technological frameworks, and their hybrids, might offer an alternative path, where the fundamental rights-based EU framework can deliver and empower meso-level data governance institutions, which carry these values in their DNA. The EU is the world's major economic and political power, distinguished by its values-based approach, grounded in the Enlightenment values. As there are signs of the EU macro-approach to personal data protection being cautiously copied by her global competitors, all the conditions are there for it to become the largest exporter of value-sensitive meso-level governance logics as well. For that, it is necessary to better define and delineate the properties of good meso-level data governance within the EU context. This paper has taken the first steps to do that.

References

Aaronson, S. A., & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law*, *21*(2), 245–272. https://doi.org/10.1093/jiel/jgy019

Allen, C. (2016, April 25). The path to self-sovereign identity [Blog post]. *Life With Alacrity*. https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html#dfref-1212

Andrejevic, M. (2011). The work that affective economics does. *Cultural Studies*, *5*, 604–620. https://doi.org/10.1080/09502386.2011.600551

Backer, L. C. (2019). China's Social Credit System: Data-Driven Governance for a 'New Era.' *Current History*, *118*(809), 209–214. https://doi.org/10.1525/curh.2019.118.809.209

Bamberger, K. A., & Mulligan, D. K. (2011). Privacy on the Books and on the Ground. *Stanford Law Review*, *63*, 247–316. https://www.stanfordlawreview.org/print/article/privacy-on-the-books-and-on-the-ground/

Baumer, E. P. S. (2014). Toward Human-Centred algorithm design. *Big Data & Society*, *4*(2). https://doi.org/10.1177/2053951717718854

Bradford, A. (2012). The Brussels effect. *Northwestern University Law Review*, *107*(1), 1–68. https://scholarlycommons.law.northwestern.edu/nulr/vol107/iss1/1/

Cameron, K. (2005, May). The laws of identity [Blog post]. *Kim Cameron's Identity Weblog*. https://www.identityblog.com/?p=352

Chander, A. (2014). How Law Made Silicon Valley. *Emory Law Journal*, *63*(3), 639–694. https://scholarlycommons.law.emory.edu/elj/vol63/iss3/3/

Chander, A., Kaminski, M., & McGeveran, W. (2021). Catalyzing Privacy Law. *Minnesota Law Review*, *105*, 1732–1802. https://minnesotalawreview.org/wp-content/uploads/2021/04/3-CKM_MLR.pdf

Collington, R. (2019). *Digital Public Assets: Rethinking Value and Ownership of Public Sector Data in the Platform Age* [Discussion Paper]. Common Wealth. https://uploads-ssl.webflow.com/5e2191f00f868d778b89ff85/5e3bfa10722cc53f4c3cd817_Digital-Public-Assets-Common-Wealth.pdf

Daly, A., Devitt, S. K., & Mann, M. (Eds.). (2019). *Good Data*. Institute of Network Cultures. https://networkcultures.org/wp-content/uploads/2019/01/Good_Data.pdf

Decision of the 1. Senate, 1 BvR 209/83-NJW 1984 (Bundesverfassungsgericht 15 December 1983).

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

Drexl, J. (2019). Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy. In A. Di Franceschi & R. Schulze (Eds.), *Digital Revolution—New Challenges for Law: Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies* (pp. 19–41). C.H. Beck; Nomos.

Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien of 2021, German Bundestag (2021). https://dsgvo-gesetz.de/ttdsg/

European Commission. (2017). *Communication from the Commission to the European parliament and the Council: Exchanging and protecting Personal Data in a Globalised World (COM(2017)7 final)*.

European Commission. (2020a). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data (COM(2020)66)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066

European Commission. (2020b). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A new ERA for Research and Innovation (COM/2020/628 final)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:628:FIN

European Commission. (2020c). *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

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, OJ L 345 90 (2003). http://data.europa.eu/eli/dir/2003/98/oj

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172 56 (2019). http://data.europa.eu/eli/dir/2

019/1024/oj

European Union. (2020). *Declaration Building the next generation cloud for businesses and the public sector in the EU*. https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe

Finck, M., & Pallas, F. (2020). They who must not be identified—Distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11–36. https://doi.org/10.1093/idpl/ipz026

Fry, E., & Renieris, E. (2020, March 31). SSI? What we really need is full data portability [Blog post]. *Women in Identity*. https://womeninidentity.org/2020/03/31/data-portability/

Fuchs, C. (2011). New Media, Web 2.0 and Surveillance. *Sociology Compass*, *5*(2), 134–147. https://doi.org/10.1111/j.1751-9020.2010.00354.x

Gady, F.-S. (2014). EU/U.S. Approaches to Data Privacy and the "Brussels Effect": A Comparative Analysis. In *International Engagement on Cyber IV: A Post-Snowden Cyberspace*.

Gao, H. (2021). Data Regulation with Chinese Characteristics. In M. Burri (Ed.), *Big Data and Global Trade Law* (pp. 245–267). Cambridge University Press. https://doi.org/10.1017/9781108919234.017

Giannopoulou, A. (2020). Algorithmic systems: The consent is in the detail? *Internet Policy Review*, *9*(1). https://doi.org/10.14763/2020.1.1452

Giannopoulou, A., & Wang, F. (2021). Self-sovereign identity. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1550

Goldfarb, A., & Trefler, D. (2018). *How Artificial Intelligence impacts labour and management. In World Trade Report: : The future of world trade* (World Trade Report 2018, p. 140) [Opinion Piece]. World Trade Organization. https://www.wto.org/english/res_e/publications_e/opinionpiece_by_avi_goldfarb_and_dan_trefler_e.pdf

Google Spain, Case C-131/12 (European Court of Justice 13 May 2014).

Granger, M.-P., & Irion, K. (2018). The right to protection of personal data: The new posterchild of European Union citizenship? In H. de W. Vries & M.-P. Granger (Eds.), *Civil Rights and EU Citizenship* (pp. 279–302). Edward Elgar Publishing. https://doi.org/10.4337/9781788113441.00019

Greenleaf, G. (2012). The Influence of European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108. *International Data Privacy Law*, *2*(2), 68–92. https://doi.org/10.1093/idpl/ips006

Gutwirth, S., Poullet, Y., Hert, P., Terwangne, C., & Nouwt, S. (Eds.). (2009). *Reinventing data protection*. Springer. https://doi.org/10.1007/978-1-4020-9498-9

Handke, C. (2014). Collective administration. In *Handbook on the Economics of Copyright*. Edward Elgar Publishing.

Hardinges, J., Wells, P., Blandford, A., Tennison, J., & Scott, A. (2019). *Data Trusts: Lessons from Three Pilots* [Report]. Open Data Institute. https://theodi.org/article/odi-data-trusts-report/

Hardjono, T., Shrier, D., & Pentland, A. (Eds.). (2019). *Trusted Data* (Revised And Expanded). MIT Press.

Herian, R. (2018). *Regulating Blockchain. Critical perspectives in law and technology*. Routledge. https://doi.org/10.4324/9780429489815

Hess, C., & Ostrom, E. (2003). Ideas, artifacts, and facilities: Information as a common-pool resource. *Law and Contemporary Problems*, *66*(1/2), 111–145. https://scholarship.law.duke.edu/lcp/vol66/iss1/5/

High-Level Expert Group on Business-to-Government Data Sharing. (2020). *Towards a European strategy on business-to-government data sharing for the public interest* [Final report]. European Union. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954

Insights, M., Geuns, J., & Brandusescu, A. (2020). *Shifting Power Through Data Governance*. https://drive.google.com/file/d/1XLlGWRbm2bu48GgTFjG2aU4DSCL0U1s9/view

Irion, K. (2012). Government Cloud Computing and National Data Sovereignty. *Policy & Internet*, *4*(3), 40–71. https://doi.org/10.1002/poi3.10

Irion, K. (2016). A special regard: The Court of Justice and the fundamental rights to privacy and data protection. In U. Faber, K. Feldhoff, K. Nebe, K. Schmidt, & U. Waßer (Eds.), *Gesellschaftliche Bewegungen—Recht unter Beobachtung und in Aktion: Festschrift für Wolfhard Kohte* (pp. 873–890). Nomos.

Irion, K. (2021). Panta Rhei: A European Perspective on Ensuring a High Level of Protection of Human Rights in a World in Which Everything Flows. In M. Burri (Ed.), *Big Data and Global Trade Law* (pp. 231–242). CUP.

Janssen, H., Cobbe, j, Norval, J., & Singh, J. (2020). Decentralised data processing: Personal Data Stores and the GDPR. *International Data Privacy Law*, *10*(4), 356–384. https://doi.org/10.1093/idpl/ipaa016

Janssen, H., Cobbe, J., & Singh, J. (2020). Personal information management systems: A user-centric privacy utopia? *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1536

Kitchin, R. (2013, November 27). Four critiques of open data initiatives [Blog post]. *London School of Economics Impact of Social Sciences*. https://blogs.lse.ac.uk/impactofsocialsciences/2013/11/27/four-critiques-of-open-data-initiatives/

Landes, W. M., & Posner, R. A. (2003). *The economic structure of intellectual property law*. Harvard University Press.

Langford, J., Poikola, A., Janssen, W., & Lähteenoja, V. (2020). *Understanding MyData Operators* [Paper]. MyData Global. https://mydata.org/wp-content/uploads/sites/5/2020/04/Understanding-Mydata-Operators-pages.pdf

Lauer, J. (2017). *Creditworthy. A History of Consumer Surveillance and Financial Identity in America*. Columbia University Press.

Lovett, R., Lee, V., Kukutai, T., Cormack, D., Rainie, S. C., & Walker, J. (2019). Good data practices for Indigenous data sovereignty and governance. In A. Daly, S. K. Devitt, & M. Mann (Eds.), *Good Data* (pp. 26–36). Institute of Network Cultures. https://networkcultures.org/wp-content/uploads/2019/01/Good_Data.pdf#page=28

Mac Sıthigh, D., & Siems, M. (2019). The chinese social credit system: A model for other countries? *Modern Law Review*, *82*(6), 1034–1071. https://doi.org/10.1111/1468-2230.12462

Madiega, T. (2020). Digital sovereignty for Europe Digital sovereignty: State of play (EPRS Ideas Paper No. *PE*, *651*(992)). https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

Mann, M., Devitt, S. K., & Daly, A. (2019). What Is (in) Good Data? In A. Daly, S. K. Devitt, & M. Mann (Eds.), *Good Data* (pp. 8–23). Institute of Network Cultures. https://networkcultures.org/wp-content/uploads/2019/01/Good_Data.pdf#page=10

Micheli, M., Ponti, M., Craglia, M., & Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, *7*(2). https://doi.org/10.1177/2053951720948087

O.E.C.D. (2008). *OECD Recommendation of the Council for Enhanced Access and More Effective Use of Public sector Information*. https://www.oecd.org/sti/44384673.pdf

O'Hara, K., & Hall, W. (2018). *Four internets: The geopolitics of digital governance* (No. 206; CIGI Papers). https://www.cigionline.org/sites/default/files/documents/Paper%20no.206web.pdf

Ostrom, E. (1990). *Governing the Commons: The Evolution of Institutions for Collective Action* (p. 280). Cambridge University Press. https://doi.org/10.1017/CBO9780511807763

Ostrom, E. (1994). *Neither market nor state: Governance of common-pool resources in the twenty-first century* [Lecture]. Lecture Series No. 2, International Food Policy Research Institute.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Poullet, Y. (2020). *From open data to reverse PSI – A new European policy facing GDPR* (No. 11; European Public Mosaic). Public Administraiton School of Catalonia. http://www.crid.be/pdf/public/8586.pdf

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. https://doi.org/10.1080/17579961.2018.1452176

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. *Internet Policy Review*, *10*(3).

Solove, D. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, *126*, 1888–1903. https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/

Spiekermann, K., Slavny, A., Axelsen, D., & Lawford-Smith, H. (2019). Big Data Justice: A Case for Regulating the Global Information Commons. *Journal of Politics*, *83*(2), 1–38. https://doi.org/10.1086/709862

Summa, H. A. (2020, March). 'Building your own internet': How GAIA-X is Paving the Way to European Data Sovereignty. *Dotmagazine*. https://www.dotmagazine.online/issues/cloud-and-orientation/build-your-own-internet-gaia-x

The Moxy Tongue. (2012, February 15). What is 'sovereign source authority'? [BLog post]. *The Moxy Tongue*. https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html

Trenham, C., & Steer, A. (2019). The Good Data Manifesto. In A. Daly, S. K. Devitt, & M. Mann (Eds.), *Good Data* (pp. 37–53). Institute of Network Cultures. https://networkcultures.org/wp-content/uploads/2019/01/Good_Data.pdf#page=39

Varian, H. R., & Shapiro, C. (1999). *Information Rules. A Strategic Guide to the Network Economy*.

Harvard Business School Press.

Venkataramakrishnan, S. (2021, February 9). Irish data regulator under fire over dated software. *Financial Times*. https://www.ft.com/content/9484b8fe-ccca-4707-8ea5-87e883b7490f

Wagner, B., & Janssen, H. (2021, January 4). A first impression of regulatory powers in the Digital Services Act [Blog post]. *Verfassungsblog*. https://verfassungsblog.de/regulatory-powers-dsa/

Wilbanks, J., & Friend, S. (2016). First, design for data sharing. *Nature Biotechnology*, *34*, 377–379. https://doi.org/10.1038/nbt.3516

Willis, D., & Kane, P. (2018, November 5). How Congress stopped working. *ProPublica; The Washington Post*. https://www.propublica.org/article/how-congress-stopped-working

Wong, J., Henderson, T., & Ball, K. (2020, July 29). Data Protection for the Common Good: Developing a framework for a data protection-focused data commons. *Data for Policy Conference*. https://doi.org/10.5281/zenodo.3965670

Yin, K., & Zhang, G. (2020, October 26). A Look at China's Draft of Personal Data Protection Law [Blog post]. *The International Association of Privacy Professionals*. https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law/

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*, 75–89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

Published by

in cooperation with