From Data Spaces to Data Governance

vol. 24 I n°3 I 2022

« au service de l'analyse » — since 1998

network industries quarterly

contents

Network Industries Quarterly, Vol. 24, issue 3, 2022 (September)

"From Data Spaces to Data Governance"

In February 2020, the European Commission (EC) presented its European Data Strategy, whose main objectives are to set up European Data Spaces, to create a single market for data and to develop an attractive, secure and dynamic data economy. Common European data spaces in the sectors of health, environment, energy, agriculture, mobility, finance, manufacturing, public administration, and skills, will ensure that more data becomes available for use in the economy and society, while keeping the companies and individuals who generate the data in control. The Data Governance Act published by the EC in November 2020, constitutes the first of the legislative proposals presented in the EU Data Strategy and applies to both personal and non-personal data. Its main objectives are to strengthen the availability of data for use by increasing trust in data intermediaries and to stimulate data sharing mechanisms across the EU.

This special issue of the Network Industries Quarterly is dedicated to some of the best papers that were presented at the 11th FSR Annual Conference on the Regulation of Infrastructures "From Data Spaces to Data Governance". The conference offered a timely occasion to take stock of the progress made in the various network industries towards the objectives outlined in the EU Data Strategy and the Data Governance Act.

The first contribution by **Donne** examines the impact of data sharing in the electricity sector from the perspectives first of companies and then of public authorities.

Tombal analyses whether two horizontal legislative initiatives supporting business-to-government (B2G) data sharing can contribute to environmental protection. More specifically, his paper looks at the *voluntary* 'data altruism' mechanism provided in the Data Governance Act and at the *compulsory* B2G data sharing obligation for 'exceptional needs' provided in the Data Act proposal.

Mannan, Wong and **Bietti** present research on the impact of data governance legislation on 'data cooperatives.' In particular, their paper explores the opportunities and challenges presented by new legislative developments and argues for a shift in how public institutions engage with existing data cooperatives to both cater for their needs and enable bolder forms of collective data management.

Catanzariti explores the tension between the use of extraterritorial claims for data and the opposite response of data nationalism. Arguing that both are forms of territory-based control, her paper proposes applying a functional approach to data sharing – as an alternative to data location – to the project for an EU cloud.

Teodora Serafimova

Research Associate, Transport Area – Florence School of Regulation, EUI

dossier

Network Industries Quarterly | Published four times a year, contains information about postal, telecommunications, energy, water, transportation and network industries in general. It provides original analysis, information and opinions on current issues. Opinions are the sole responsibility of the author(s).

Subscription | The subscription is free. Please do register at fsr.transport@eui.eu or info@ic4r.net to be alerted upon publication.

Letters | We do publish letters from readers. Please include a full postal address and a reference to the article under discussion. The letter will be published along with the name of the author and country of residence. Send your letter (maximum 450 words) to the editor-in-chief. Letters may be edited.

Publication director | Matthias Finger

Managing editor | Teodora Serafimova

Publishing editor | Ozan Barış Süt

Founding editor | Matthias Finger

Publishers | Florence School of Regulation, Transport Area, Via Giovanni Boccaccio 121, 50133, Florence, Italy, phone: +39 055 4685 795, email: FSR.Transport@eui.eu and Istanbul Center for Regulation, Istanbul Technical University, Taşkışla, 34367 Istanbul, Turkey, email: info@ic4r.net

Websites: https://fsr.eui.eu/transport/, https://ic4r.net/, https://www.network-industries.org/

Non-Personal Data in the Electricity Sector: a Key Asset for Companies and Public Authorities

Antoine Donne[1]

For companies in the electricity sector, data are now a legal requirement to be able to operate. This justifies rules governing business-to-business (B2B) data sharing. Data are also coveted by public authorities to perform their monitoring tasks (the state as a regulator) and provide market facilitation services (the state as a platform). This justifies the regulation of business-to-government (B2G) data sharing.

Introduction

Digitalisation is a major driver of change in the electricity sector (IEA 2017; Rossetto & Reif 2021). However, the legal framework that governs data and digitalisation is fragmented. This results in a puzzle with many pieces of legislation – existing and upcoming, sectoral and horizontal – that need to fit together. Several energy-sector pieces of legislation are already in force and have an impact in terms of data sharing (e.g. the Electricity Directive 2019/944, the CACM Regulation 2015/1222 and the REMIT Regulation 1227/2011). In addition, the European Data Strategy, COM(2020) 66 final of 19 February 2020, an EU policy oriented toward data sharing, is central in the implementation of new horizontal legislation. It covers a wide array of initiatives (including cloud services and data spaces). However, this article only discusses proposals related to B2B data sharing and B2G data sharing under the Data Governance Act 2022/868 (DGA) and the Data Act Proposal, COM(2022) 68 final of 23 February 2022. This fragmentation entails a risk of conflict of rules between the different texts. Against the background of these various legislative texts, this article focuses on the impact of data sharing in the electricity sector from the perspectives first of companies and then of public authorities.

Data, an asset coveted by companies

Data are a key asset for companies. Beyond business or technical needs, data are increasingly a legal requirement to be able to operate in the energy sector. In this context, existing B2B data sharing obligations are reinforced while new rules are proposed to regulate the concrete means that allow the sharing of data to take place (i.e. data intermediation services).

Data, a legal requirement to operate

Starting in the 1990s, liberalisation and digitalisation of the electricity sector paved the way for the central role that data play in today's energy system for companies. While one may think that liberalisation means deregulation, on the contrary liberalisation was concomitant with implementation of a new extensive legal framework regulating the energy sector (Jones 2020). Under this framework, operation of a business in the electricity sector is often subject to authorisation, and communication of data by companies to public authorities is a prior requirement imposed by law in order to obtain the right to operate.

Taking the example of nominated electricity market operators (NEMOs) in charge of operating cross-border electricity markets pursuant to the CACM Regulation, a wide array of information ranging from technical to business data is required to be disclosed to public authorities by the NEMO. Focusing specifically on technical data, NEMOs are under an obligation to provide public authorities with access to the source codes of their algorithms. This constitutes a far-reaching obligation as companies traditionally considered this information a business secret.

In conclusion, data are a key asset for companies to comply with their legal obligations throughout the lifecycle of a project. These obligations result from energy sector regulations. In addition, data are also necessary for third-party businesses to run their own activities along the energy value chain. This justifies strengthening the sharing of data between businesses.

Data for all businesses alike, which justifies rules on B2B data sharing

Data are key not only for data holders but also for all other businesses. In this context, regulation of data sharing becomes prevalent, although it is not new, unlike regulation of the means that allow the sharing of data to take

1 Senior Legal Counsel at EPEX SPOT, PhD candidate at Université Paris Dauphine PSL, a.donne@epexspot.com

place, such as data intermediation services. These new rules are enacted in horizontal rather than sectoral legislation.

Regulation of B2B data sharing is not new. In fact, sectoral and horizontal legislation are already in force. An example of sectoral legislation in the energy sector is the Electricity Directive, which provides a framework for sharing individuals and companies' metering data. An example of horizontal regulation is the Database Directive 96/9, which – despite this not being its main aim – can be considered to have introduced an earlier data sharing obligation for the benefit of users of a database to extract and/or re-utilise insubstantial parts of its contents, evaluated qualitatively and/or quantitatively and for any purposes whatsoever. However, following the European Data Strategy, what is new is that data sharing is now at the cornerstone of EU (digital) policy. The Data Act Proposal establishes, in particular, an obligation for holders of data that have been generated by users of a product to share them with that user or third parties designated by that user. Therefore, a general B2B data sharing obligation is established. However, this shall be done with due regard to the protection of the rights of the data holders and of protected third parties (ALI & ELI 2021). In practice, only trade secrets of the data holder and third parties are protected. There is no mention of other rights such as intellectual property rights.

Regulations requiring the sharing of data are associated with regulation of the channels of communication that ultimately enable the data sharing. One of the means enabling data sharing is data intermediaries. Data intermediation services are the subject of novel regulation. Pursuant to the DGA, data intermediation services "should offer a novel, 'European' way of data governance, by providing a separation in the data economy between data provision, intermediation and use." Data intermediation services are defined as services establishing commercial relationships for the purpose of data sharing between an undetermined number of data holders on the one hand and data users on the other hand (many to many), using technical, legal or other means. A key criterion in the DGA is the establishment of a business, legal or technical relation between data holders and data users with the aim of mediating the relationship (Baloup et al. 2021). Examples of data intermediation services include data marketplaces (e.g Dawex). In contrast, this would exclude services that obtain data from data holders but without establishing a commercial relationship between data holders and data users (e.g. Bloomberg). This would also exclude services that are exclusively used by one data holder in order to enable the use of its data (one to many) (e.g. the EEX and EPEX SPOT data webshop).

In conclusion, data is key for all companies operating in the energy sector. For this reason, new rules mandating general data sharing have been proposed. Data intermediation services, which concretely enable the sharing of data to take place, are also subject to new rules. These new rules stem from horizontal regulation. This somewhat departs from the previous approach that saw the enactment of sector-specific rules. Therefore, the new rules stemming from horizontal regulations will need to be carefully combined with past rules stemming mostly from sectoral regulations that may remain in force to avoid conflict of rules.

Data, an asset coveted by public authorities

Data are an asset coveted by public authorities too. Public authorities seek to access data held by businesses. Traditionally, data are used by public authorities as a mean of control over companies that carry out regulated activities (the state as a regulator). However, data are also increasingly used by public authorities as a means of intervening in the economy (the state as a platform).

The state as a regulator, a limited version of B2G data sharing

Public authorities used to be the biggest data holders. In contrast, today datasets are primarily held by private actors (Thomas 2021). In this new context, public authorities are granted a right of access and use of data held by companies (High-Level Expert Group on Business-to-Government (B2G) Data Sharing 2020). In their capacity as state as a regulator, public authorities use the data collected from businesses for their own internal needs.

The first objective of B2G data sharing is primarily to supervise companies acting in the energy market. Communication of data to public authorities by companies, as required by law, serves the purpose of monitoring the regulated activities carried out by businesses. Taking the example of NEMOs, beside the CACM Regulation mentioned above, another means of supervision available to public authorities is the REMIT Regulation, which requires NEMOs to transmit market data to public authorities.

A second objective is to be able to react to unforeseen events. In this regard, the Data Act Proposal introduces an obligation on data holders to make their data available to

public sector bodies in the case of public emergencies or in situations in which public sector bodies have an exceptional need to use certain data but the data cannot be obtained on the market, in a timely manner through enacting new legislation or by means of existing reporting obligations.

In conclusion, the law grants public authorities a wide right of access and use of data held by private companies. However, in their capacity as state as a regulator, the right of use afforded to public authorities is purpose-based. It is somewhat limited compared to public authorities' right to reuse data in their role as state as a platform where their relationship with businesses is based on open data principles.

The state as a platform, a full version of B2G data sharing

In their capacity as state as a platform (Chevallier 2018), public authorities seek to make available to the rest of society the data they hold, including those originating from companies in the first place. In these circumstances, the right of use afforded to such data users is likely to interfere with the business interests of the initial data holder, whether it is done for transparency purposes or for open data purposes.

First, communication of data can serve the purpose of market transparency. To illustrate this, climate-change disclosure obligations help companies to achieve 'net zero' carbon emissions. Reaching net zero will in turn involve a reallocation of capital. However, investors need information to reallocate their capital in order to reach net zero. However, the situation currently lacks transparency when it comes to the information available to investors. This calls for mandatory climate-change disclosure in order to improve the transparency of the information available to investors (Armour et al 2021). For example, in France under article L533-22-1 of the *Code monétaire et financier* (French financial act) and articles L225-102-1, R225-104 and R225-105 of the *Code de commerce* (French commercial act) financial institutions and some companies are required to disclose climate-related information in relation to their portfolio and activities (climate risk exposure, mitigation measures taken for all emissions that occur in a company's value chain, both upstream and downstream).

Second, while the transparency measures described above merely ensure information for all stakeholders, a step beyond this is the communication of data held by a company for the purpose of reuse by another company. Open public sector data is a long-established principle under the Open Data Directive 2019/1024. Under the DGA Proposal, the objective is to further expand the reuse of data held by public authorities but that are the subject of third-party rights and therefore not covered by the Open Data Directive. However, there is a major shift in the approach to the reuse of data between the Open Data Directive and the DGA Proposal. The former is based on open data principles, meaning that the data can be reused for any purpose, while the latter establishes purpose-based reuse, meaning that the data can only be used for a specific purpose (Baloup et al. 2021).

In conclusion, public authorities in their capacity as state as a platform are able to ensure broad diffusion and reuse of data originating from companies.

Conclusion

Data are increasingly a requirement to comply with companies' legal obligations. This justifies new rules on B2B data sharing. Data are also needed by public authorities to carry out monitoring of the market in their role as state as a regulator and external tasks in their capacity as state as a platform. This justifies the regulation of B2G data sharing.

As a result of all the new legislation currently proposed, the legal framework that governs data sharing appears more and more fragmented. This creates risks of overlaps and even of conflicts of rules between the different pieces of legislation. Stakeholders in the energy sector will need to familiarise themselves with provisions stemming from both energy-sector regulations and horizontal regulations. In addition, this article has highlighted some conflicts of rules that should be addressed by upcoming horizontal legislation.

References

American Law Institute (ALI), European Law Institute (ELI) (2021), *ALI-ELI Principles for a Data Economy: Data Rights and Data Transactions.*

Armour, J., Enriques, L. and Wetzer, T. (2021), 'Mandatory Corporate Climate Disclosures: Now, but How?,' *ECGI Working Paper Series in Law*, 614/2021.

Baloup, J. et al. (2021), 'White Paper on the Data Governance Act,' *CiTiP Working Paper Series*.

Chevallier, J. (2018), 'Vers l'État-plateforme?' *Revue française d'administration publique*, 167: 627-637.

High-Level Expert Group on Business-to-Government (B2G) Data-Sharing (2020), *Towards a European Strategy on Business-to-Government Data Sharing for the Public Interest*.

International Energy Agency (IEA) (2017), *Digitalization & Energy*.

Jones, C., ed. (2020)., *EU Energy Law, Volume I, the Internal Energy Market* (Claeys & Casteels).

Rossetto, N. and Reif, V. (2021), 'Digitalization of the Electricity Infrastructure: a Key Enabler for the Decarbonization and Decentralization of the Power Sector.' *EUI Working Paper Florence School of Regulation*, RSC 2021/47.

Thomas, J., Wendehorst, C., Duller, Y. and Schwamberger, S. (2021), *Response of the European Law Institute: Public Consultation on the Data Act* (European Law Institute (ELI)).

Business-to-government data sharing for environmental purposes

Thomas Tombal[1]

In this paper, I analyse whether two horizontal legislative initiatives supporting business-to-government (B2G) data sharing can contribute to environmental protection. More specifically, I look at the voluntary 'data altruism' mechanism provided in the Data Governance Act and at the compulsory B2G data sharing obligation for 'exceptional needs' provided in the Data Act proposal.

Introduction

While data are sometimes presented as the new oil in the European data economy, it would be reductive to solely consider the potential economic value of data without reflecting on their societal value. Indeed, as the European Commission's *Strategy for data* outlines, "making more data available and improving the way in which data is used is essential for tackling societal, climate and environment-related challenges, contributing to healthier, more prosperous and more sustainable societies" (European Commission 2020a: 3).

Importantly, not only public sector data but also private sector data can make a significant contribution to the common good (European Commission 2020a: 6). This implies that a lack of data sharing by private actors will not only create economic challenges but also societal challenges. Indeed, as the societal value of the data held (exclusively) by some actors is enormous, allowing public actors to use these data could generate immense scientific and environmental benefits for our society (Shkabatur 2019: 383).

Therefore, I argue that data sharing between private and public actors can significantly contribute to the realisation of environmental objectives. More specifically, I pinpoint two interesting European legislative initiatives that can support this. While sector-specific legislation has the advantage of being much more targeted and adapted to a sector's needs, this must be balanced with the non-rivalrous and general-purpose nature of data, which implies that they can be re-used for completely different purposes in another sector (European Commission 2020b: 15). In fact, such a sectoral limitation seems particularly unwarranted if the data sharing legislation pursues broader societal objectives.

Consequently, I focus on business-to-government (B2G) horizontal data sharing initiatives which can contribute to environmental protection. More specifically, I look at the *voluntary* 'data altruism' mechanism provided in the Data Governance Act (DGA 2022) and at the *compulsory* B2G data sharing obligation for 'exceptional needs' provided in the Data Act proposal (DAP 2022).

Voluntary B2G data sharing and 'data altruism'

Clearly, private actors can *voluntarily* decide to share data with public actors for environmental purposes. For instance, phone operators increasing their B2G sharing of location data with a regional authority can allow the latter to optimise its public transport system in order to reduce CO2 emissions from personal vehicles. In practice, such *voluntary* data sharing mainly relies on contracts. Private actors are therefore free to draft such contracts as they please, although they can rely on European Commission guidelines (European Commission 2018a: 13-4).

However, recently the Commission has started to promote voluntary sharing for societal purposes through the development of a series of 'Common European data spaces,' which should lead to large pools of data becoming available in domains of public interest such as environmental protection (European Commission 2020a: 22-3). A key legislative instrument to support the establishment of these European data spaces is the DGA (2022).

More specifically, Articles 16 to 25 of the DGA contain measures aiming to facilitate voluntary data sharing for the

1 Post-doctoral researcher at the Tilburg Institute for Law, Technology and Society (TILT) and the Tilburg Law and Economics Center (TILEC) of Tilburg University; Lecturer at the Université de Namur; t.j.a.tombal@tilburguniversity.edu;

This work was undertaken in the context of the 'Digital Legal Studies research initiative' which is funded through the Law Sector Plan of the Dutch Ministry of Education, Culture and Science (OCW).

common good at the EU level. In the DGA this is referred to as "data altruism," which can be defined as a voluntary mechanism through which data subjects (individuals – see General Data Protection Regulation, Art. 4.1) can decide to share their personal data and data holders (private actors – see DGA, Art. 2.8) can decide to share their non-personal data for objectives of general interest without seeking or receiving a reward (Art. 2(16)). This can contribute to achieving environmental objectives such as combating climate change.

This "data altruism" mechanism (DAM) is in fact quite particular as it does not organise direct voluntary data sharing between private actors and public entities that will make use of the data for a specific environmental objective. Instead, the mechanism aims to create data pools that are managed by an intermediary called a "data altruism organisation" (DAO) (Art. 18). Data are therefore only indirectly shared between private actors and public entities as the latter only obtain the data from the pool and not directly from the former. For instance, using this DAM private actors can provide data about air quality and releases of polluting materials around their worksites to an environmental data pool managed by a DAO, from which a public actor can extract data in order to develop a service advising against certain leisure activities for more fragile people in certain specific areas.

Importantly, the private actor can only share non-personal data on its own initiative with these data pools and cannot decide to provide personal data that it holds unless the individuals to which the data pertain have consented to it. In this regard, the DGA provides that in order to facilitate data altruism, the Commission may develop a standardised "European data altruism consent form" (Art. 25).

A third particularity of this DAM is that the conditions for being recognised as a DAO are quite strict. Indeed, only public and private non-for-profit entities that pursue objectives of general interest and have a legally independent functionally separate structure can be recognised as DAOs (Art. 18). Therefore, a for-profit private actor that decides to share data extracted from its commercial activity in order to promote environmental protection as a 'side-activity' cannot be recognised as a DAO. It will therefore have to fall back on classic contracts.

To conclude, it must be underlined that this DAM is only one option to engage in voluntary data sharing for environmental objectives, and that private actors are not compelled to use this mechanism. Indeed, other mechanisms, such as "open collaborative knowledge sharing platforms, open access scientific and academic repositories, open source software development platforms and open access content aggregation platforms" can also be used for the common good (DGA: Recital 49). In the next section I turn to situations in which a private actor might be compelled to share some of its data with public actors.

Imposing compulsory B2G data sharing for 'exceptional needs'

The underlying logic of imposing B2G data sharing is that if it were fully up to private actors to decide whether they want to engage in such sharing it might limit the possibility of societal benefits in fact being achieved. Accordingly, discussions on B2G compulsory data sharing emerged in 2017 during the public consultation pertaining to the latest recast of the Public Sector Information Directive (PSI Directive 2019). At the time, the European Commission was considering including a new provision in the Directive according to which data held by private companies but deemed to be of public interest should be shared with public sector bodies.

While numerous respondents to the public consultation supported this proposition, such a provision was finally not included in the recast of the Directive (European Commission 2018b: 8). The reason was that many stakeholders responding to the public consultation had indicated that the Commission had failed to provide a sufficiently clear definition of these 'public interests' and that the objectives and scope of such a proposition also lacked clarity (European Commission 2018b: 8). According to them, further discussion was needed on compulsory B2G data sharing initiatives.

Therefore, the European Commission appointed a High-Level Expert Group (HLEG) on B2G Data Sharing. Its mandate was to evaluate the key principles involved in the supply of private sector data to public sector bodies under preferential conditions for re-use which were contained in the European Commission's abovementioned data sharing guidelines (European Commission 2018a). The HLEG suggested a series of principles for "scalable, responsible and sustainable B2G data sharing for the public interest" (HLEG on B2G Data Sharing 2020: 7). In substance, the HLEG identified four core principles, namely proportionality, data-use limitation, risk mitigation and safeguards, and compensation, which aim to balance the interests of private data holders on the one hand and pub-

lic re-users on the other hand (HLEG on Business-to-Government Data Sharing 2020: 80-3).

In the wake of the HLEG's seminal report, discussion pertaining to the possibility of imposing *compulsory* B2G data sharing for societal purposes has reappeared in the European Commission's inception impact assessment on the Data Act (European Commission 2021: 5). This eventually led to the inclusion in Articles 14 to 22 of the DAP (2022) of *compulsory* B2G data sharing provisions in cases of 'exceptional needs'.

The DAP provides that "upon request, a data holder [Art. 2(6)] shall make data available to a public sector body [Art. 2(9)] or to a Union institution, agency or body demonstrating an exceptional need to use the data requested" (Art. 14.1). Importantly, however, this obligation does not apply to small and micro-enterprises (Art. 14.2).

The key criterion to determine when private actors might be compelled to share data with a public sector body is therefore that of 'exceptional needs'. While the policy option to request B2G data sharing "for any duly justified purpose" was considered (European Commission 2022: 37), this option was eventually rejected because it would entail higher administrative and compliance costs for private actors without necessarily compensating them with greater benefits, and because such a broad scope would be too unpredictable for private actors and could lead to a lack of harmonisation across the EU (European Commission 2022: 49-50). The DAP therefore only applies in specific *ad hoc* B2G sharing scenarios, and complements "existing reporting or compliance obligations in sectoral legislation that establish ongoing or recurring data exchange mechanism[s] between public institutions and the private sector" (European Commission 2022: 158; Drexl et al. 2022: 52-3).

According to the DAP, an 'exceptional need' will exist in specific circumstances such as when there is a need to respond to, prevent or assist recovery from a public emergency (Arts. 15.a) and b)) or when a lack of available data prevents a public sector body from carrying out a specific task in the public interest and the body is unable to obtain such data by timely alternative means (Art. 15.c)).

In the light of this relatively narrow definition of 'exceptional needs' one might wonder whether data sharing for environmental purposes might be considered an instance of data sharing for 'exceptional needs'. One could argue that global warming and degradation of our environment are public emergencies that we need to respond to or to prevent (Arts. 15.a) and b)). Such a view could be supported by the alarming reports of the Intergovernmental Panel on Climate Change (IPCC 2021; IPCC 2022) on the impact of human activity on global warming and on the catastrophic consequences that this can lead to – especially for more vulnerable populations – if our societies do not evolve in the coming years towards more sustainable ways of living that preserve our environment.

Furthermore, a public emergency is defined in the DAP as an "exceptional situation negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, or the substantial degradation of economic assets in the Union or the relevant Member State(s)" (Art. 2(10)). One could argue that the current state of our environment and climate could be considered to represent an exceptional situation that risks leading to serious and lasting repercussions on living conditions or economic stability. In this regard, the Impact Assessment accompanying the DAP indicates that "access to and use by public sector bodies of direct economic loss data, including the costs of emergency response and recovery, could improve the accuracy of the risk assessments that inform climate adaptation actions" (European Commission 2022: 61).

On the other hand, one could argue that while global warming and the degradation of our environment could have disastrous consequences they have not yet fully materialised and are somewhat mid- to long-term concerns so that these concerns might not yet be qualified as public emergencies, at least if addressed from a general perspective. This view seems to be supported by Recital 57 of the DAP, which seems to focus on specific identifiable public emergencies such as "emergencies resulting from environmental degradation and major natural disasters including those aggravated by climate change, as well as human-induced major disasters." In other words, while B2G data sharing could be imposed to address a (or prevent an imminent) specific public emergency that is a consequence of global warming (e.g. a flood, a hurricane, a drought or a fire), it might not be imposed to address more general concerns pertaining to global warming and the degradation of the environment, because one might consider that we are not "in circumstances that are reasonably proximate to the public emergency in question" (DAP: Recital 58). This interpretation seems to be supported by the Commission stating that "it is the exceptional character of the situation that will be the main criterion" (European Commission 2022: 158).

Similarly, the fact that global warming and the degradation of our environment could be perceived as mid- to long-term concerns rather than imminent concerns could also prevent the possibility of relying on Article 15.c) of the DAP to impose B2G data sharing. Indeed, one could argue that as the issue is not imminent the potential lack of available data preventing public sector bodies from carrying out their environmental protection tasks could still be timely addressed through alternative means such as by adopting dedicated legislative measures (DAP: Art. 15.c).1; Drexl et al. 2022: 51).

Nevertheless, if the risk of serious and lasting repercussions on living conditions or economic stability deriving from environmental degradation were to become more significant and imminent as time passes, data sharing for environmental purposes could be explicitly added as a new 'exceptional need' in a subsequent review of the Data Act (DAP: Art. 41.c)).

Conclusion

In conclusion, while the DGA's 'data altruism' mechanism might foster increased B2G data sharing for general environmental purposes, one must not overlook that it is purely *voluntary*. However, if it were fully up to private actors to decide whether they want to engage in such sharing it might limit the possibility of societal benefits in fact being achieved.

Data sharing for general environmental objectives might also not be considered data sharing for 'exceptional needs' in the light of the current phrasing of Article 15 of the DAP. Due to the fundamental environmental and climate adaptation challenge that our societies must address, one could question whether we can afford to wait any longer or whether we should act now and already include B2G data sharing to tackle environmental and climate issues in the final version of the Data Act. What is certain is that further research on data sharing by private actors as an avenue to foster societal benefits will need to be conducted, as I attempt to do in Thomas Tombal (2022).

References

Legislation

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), *OJ L 152/1*, 3 June 2022.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119/1*, 4 May 2016.

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*, 26 June 2019.

Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 23 February 2022, COM(2022) 68 final.

Secondary sources

Drexl, J. et al. (2022) *Position Statement of the Max Planck Institute for Innovation and Competition on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act)*, 25 May 2022 (Munich), <https://www.ip.mpg.de/en/research/research-news/position-statement-on-the-eu-data-act.html>, accessed 20 August 2022.

European Commission (2018a) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a common European data space,"* COM(2018) 232 final, 25 April 2018 (Brussels).

European Commission (2018b) *Consultation on PSI Directive review – Synopsis report*, 25 April 2018 (Brussels), <https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-revision-directive-re-use-public-sector-information>, accessed 20 August 2022.

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, 19 February 2020 (Brussels).

European Commission (2020b) *Commission Staff Working Document, Impact assessment report accompanying the document "Proposal for a Regulation of the European Parliament and of the Council on European data governance: An enabling framework for common European data spaces (Data Governance Act)*," SWD(2020) 295 final, 25 November 2020 (Brussels).

European Commission (2021) *Inception Impact Assessment "Data Act (including the review of the Directive 96/9/EC on the legal protection of databases)*," Ares (2021)3527151, May 2021 (Brussels).

European Commission (2022) *Commission Staff Working Document,* "*Impact assessment report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)*," SWD(2022) 34 final, 23 February 2022 (Brussels).

High-Level Expert Group on Business-to-Government Data Sharing (2020) *Towards a European strategy on business-to-government data sharing for public interests: Final report*, 2020 (Brussels), https://op.europa.eu/en/publication-detail/-/publication/d96edc29-70fd-11eb-9ac9-01aa75ed71a1, accessed 20 August 2022.

Intergovernmental Panel on Climate Change (2021) *Climate Change 2021: The Physical Science Basis* (Cambridge: Cambridge University Press).

Intergovernmental Panel on Climate Change (2022) *Climate Change 2022: Impacts, Adaptation and Vulnerability* (Cambridge: Cambridge University Press).

Shkabatur, J. (2019) 'The Global Commons of Data,' *Stanford Technology Law Review*, 22: 354-411.

Tombal, T. (2022) 'Data sharing by private actors as an avenue for more sustainability' in H. Jacquemin (ed.), *Sustainability and IT* (Bruxelles: Larcier) [forthcoming].

Data Cooperatives in Europe: A Preliminary Investigation

Morshed Mannan[1], Janis Wong[2] and Elettra Bietti[3]

This paper presents research on the impact of data governance legislation on 'data cooperatives.' It explores the opportunities and challenges presented by new legislative developments and argues for a shift in how public institutions engage with existing data cooperatives to both cater for their needs and enable bolder forms of collective data management.

Introduction

In spite of significant developments in the European Union's digital and data policies in the last five years, not least the entry into force of the General Data Protection Regulation (GDPR) in 2018, there continue to be lingering concerns surrounding our increasingly datafied society. The concept of 'data stewardship' has arisen partially as a critique of how corporations (and in some cases governments) manage personal data and also to highlight alternative methods for acquiring, storing, aggregating and de-identifying personal data and setting procedures for their use. This means that stewards should seek to protect the interests of those whose data is managed by these systems and not just those of the entities they work for. The emergence of data cooperatives can be seen as one approach to data stewardship, as will be discussed further in this paper.

Data cooperatives are structures that enable the creation of open data and personal data stores for mutual benefit,[4] rebalancing what many perceive as an asymmetric relationship between data subjects and data processing entities.[5] While data cooperatives show promise in creating more inclusive, equitable and empowering ways of managing data, and have generated some interest at the policy level, these cooperatives are still rare. The potential and success of these novel and radically different organisations, many of which operate within the EU, therefore depend on the evolution of EU legal and policy frameworks, alongside a rise in citizens' awareness and the adoption of data cooperative solutions.

This paper presents the preliminary results of an ongoing investigation into data cooperatives in Europe. The paper is centrally concerned with the relationship between data cooperatives and EU frameworks for data governance. Our contribution aims to both support data cooperatives in navigating legal constraints and opportunities in Europe, and to inform policy discussions on the construction of a sustainable democratic digital economy.

We draw attention to the possible impacts, benefits and limitations of the GDPR and the new Data Governance Act (DGA) for the growing ecosystem of data cooperatives in Europe. It is important for data cooperatives established in the EU and beyond to monitor landmark EU legislation such as the GDPR and DGA as it will no doubt affect their trajectories, growth and potential to thrive. It deserves close scrutiny and requires EU legislators to involve cooperatives more closely in policymaking.

The paper is structured as follows. In Part I we map the data cooperative landscape in Europe and outline some of the legal developments relevant to the data cooperative ecosystem. In Part II we describe some key takeaways from interviews carried out with cooperatives in Europe and lay out a vision for future collaboration between cooperatives and EU institutions.

Data cooperatives in Europe: Landscape, typologies & relevant law

Data cooperatives aim to give more control to members over their data and, in some cases, to use these data in the interest of a wider user community or the general public. EU regulatory regimes such as data protection law impact the existence of these cooperatives, shaping and potential-

1 Max Weber Fellow, European University Institute, morshed.mannan@eui.eu; Morshed Mannan's research is funded by the European Research Council under the European Union's Horizon 2020 Research and Innovation Programme (Grant Agreement No. 865856).

2 Research Associate, The Alan Turing Institute, jwong@turing.ac.uk

3 Joint Postdoctoral Fellow at the NYU School of Law and the Digital Life Initiative at Cornell Tech in New York, elettra.bietti@nyu.edu

4 J. Tait, 'Open Data Cooperation – Building a Data Cooperative', available online at: <https://www.opendatamanchester.org.uk/947/>.

5 S. Delacroix and N. Lawrence, 'Bottom-up data Trusts: disturbing the one-size-fits-all approach to data governance', 9(4) International Data Privacy Law (2019), 236-252.

ly constraining their purposes, goals, business structures and technical features.

There are a number of data cooperatives in Europe. However, they tend to be small scale and relatively young. Some cooperatives are registered as cooperatives while others describe themselves as data cooperatives without being registered as such. In surveying the cooperative landscape, we identified two ways in which they can be categorised. One is according to the *motivation* or *purpose* for collecting and processing data. The data cooperatives we studied focus on the fields of health (Salus), personal data (polypoly), remote work (dOrg), transport in the gig economy (Drivers' Seat) and agriculture (SAOS). The second way is according to *how* the data are *technically gathered and used*. We identified some data cooperatives that do not want to access their members' data (Salus, polypoly) and others that work directly with these data (Drivers' Seat, SAOS). There are various reasons for this, including legal issues and ideological conceptions of data.

Data collection and processing carries with it certain legal obligations and restrictions. EU legislation such as the GDPR affects data cooperatives registered or operating in the European Economic Area (EEA). Privacy and personal data protection are indeed fundamental rights in the EU.[6] This means that in Europe, there are significant restrictions on what private and public actors can do with personal data and information that relates to an identified or identifiable living individual. This is not only significant for cooperatives operating in the EEA but potentially also for cooperatives operating outside the EEA that handle the personal data of EU data subjects.

European data protection law, including the GDPR, is based on the foundational principle that any processing of personal data is unlawful unless it can be justified as fair and lawful processing. The GDPR introduced inalienable data subject rights that allow individuals to access information about their personal data and how they are processed,[7] to rectify and erase personal data[8] and to port data.[9] Data subjects must exercise these rights individually and cannot delegate them. They can only delegate their rights to lodge complaints and request remedies against data protection authorities, controllers and processors.[10]

Several data cooperatives are involved in the healthcare sector, so it is pertinent that the GDPR's default rule is a prohibition of processing of health, genetic and biometric data that can be used to identify an individual.[11] The GDPR itself provides several exceptions too, however. It is possible to give explicit consent to processing of these data for certain specific purposes.[12] A foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim can carry out processing if the processing has a legitimate aim and appropriate safeguards are in place as long as the processing concerns members, former members or persons who have contact with the entity in connection with its purposes. These personal data cannot be shared with third parties without the consent of the relevant data subjects.[13]

New EU legislative initiatives will promote the exercise of personal data rights in the Union. The Data Governance Act (DGA), which will become directly applicable after a grace period on 24 September 2023, enables greater access to and use of data for novel, commercial and altruistic ends. The DGA presents a framework for data access and use by setting out the conditions for re-using and accessing these data. Data intermediation services, including data cooperatives, must comply with a number of requirements to provide services across the Union.[14] These include notifying a designated authority in the Member State where they have their main establishments (or in which the legal representatives of non-EEA organisations have their establishments) and meeting a host of conditions, such as limiting the use of the data collected with respect to any activity of a natural or legal person. Significantly, the DGA clarifies that data intermediation service providers have 'fiduciary duties' to data subjects if they intermediate exchanges of data between data subjects and legal persons.[15] All these requirements have consequences for the operations of data cooperatives.

In addition to new procedural requirements for data cooperatives, the DGA advances a specific, and arguably muddled, conception of what data cooperatives are and does not reflect the diversity of the data cooperatives in existence. The DGA explicitly includes services provided by data cooperatives within the types of data intermediation

6 Charter of Fundamental Rights of the European Union, arts. 7-8.

7 GDPR, art 15.

8 GDPR, art 16.

9 GDPR, art 20.

10 GDPR, art 77-80.

11 GDPR, art 9(1).

12 GDPR, art 9(2)(a).

13 GDPR, art 9(2)(d).

14 DGA, arts 11(4)-(5), 12.

15 DGA, recital 33.

services in its remit,[16] with data cooperatives expected to help user-members make informed choices prior to consenting to data use and to negotiate terms and conditions with data users prior to individual consent being given. This includes the activities of data cooperatives like polypoly. However, this conception of data cooperative fails to acknowledge the *not-for-profit* data cooperatives that exist both in the EU (e.g., Salus) and beyond (e.g., MIDATA), which aim to establish commercial relationships between data subjects and data holders on the one hand and data users on the other. It also ignores data cooperatives that collectively pool members' data (e.g., Drivers' Seat). This raises questions about whether existing data cooperatives will be able to continue describing themselves as such. Instead, it is possible that data cooperatives that serve 'general interests' – which include healthcare data cooperatives that pool data[17] – may be expected to register as 'Data Altruism Organisations,' a new creation of the regulation that can collect and process personal and non-personal data so as to make these data available for general interest purposes.

These laws and requirements not only entail new costs for cooperatives but they also require a transformation in how these organisations operate.

Key takeaways from our interviews

As part of our research, we conducted interviews with the leaders of Salus.coop, polypoly and dOrg. We were interested in understanding their organisational structures and purposes, the legal issues they face – particularly in relation to data governance – and their interactions with public institutions. We also communicated with organisations such as SAOS and Driver's Coop for general comments regarding our work but did not conduct interviews with them. We supplemented this with desk-based research on these organisations.

a) Data cooperative models tend to be under-resourced and would benefit from help and coordination at the EU level.

We noted that data cooperatives and their members have little understanding of the regulatory environment beyond incorporation and registration as cooperatives, which is often due to a lack of resources. With respect to data governance, cooperatives like Salus.coop mentioned that they rely on data subject access under Articles 77-80 of the GDPR as a basis for their business model but there was limited awareness about the opportunities and challenges afforded by new legislation like the DGA. Some data cooperatives are unaware of the extent to which their work is connected to and impacted by existing EU legislation. Others want to engage in the development of laws and policies but do not know how to do so. As a result, data cooperatives in general tend to be *law-takers* as opposed to *law-makers* when it comes to regulatory developments regarding data cooperative models.

b) Data cooperatives have a keen interest in collaborating with public institutions

These cooperatives have appetite for working with public institutions and want the data cooperative model to thrive within local communities across the continent. For example, Salus works closely with public institutions to generate value in the healthcare sector. In order to better develop infrastructure for cooperatives and other alternative models of data governance in Europe, policymakers should more actively speak to data cooperatives within and outside the EU to understand how these organisations can adapt to legislative developments while also ensuring that these developments respond to their needs. This could, for instance, include acknowledging the existence of not-for-profit data cooperatives. This is supported by our interactions with data cooperatives, who suggested a more proactive approach by public institutions as a way to help them grow faster and generate greater social impact.

c) Data cooperatives tend to be driven by individualist technical and ideological models, including blockchain and multi-party computation.

Development and deployment of distributed ledger technologies are common in the data cooperative space. This is due to broadly shared beliefs regarding the potential of these technologies to redistribute power away from centralised infrastructure and towards a dispersed network of people and software programmes (e.g., smart contracts). However, the risks in using these technologies are that they contribute to an excessively *individual-centric* approach to (personal) data management. Use of these technologies attempts to make individual users responsible for how their data is accessed and used, thus (purportedly) shielding data cooperatives from responsibilities under data protection and other laws. The use of these technologies therefore raises questions about whether current data cooperatives, while providing data intermediation services, are able to

16 DGA, arts 2(15) and 10(c).

17 DGA, recital 45.

effectively bear the fiduciary duty of acting in the best interest of data subjects as required under the DGA.

d) There is a lack of initiatives in Europe that focus on co-managed collective pools of data, which may be a result of the stringent requirements in EU data protection law. In order to increase the socio-economic and relational value of collective data, data cooperatives could serve as carve-outs from data protection law.

Sitting uneasily within the requirements imposed by the GDPR and the possibilities created by the DGA, data cooperatives remain a promising yet so far missed opportunity to create social value through data. For example, the DGA explicitly seeks to enhance the agency and control of individuals over their data,[18] with the rights under the GDPR continuing to be personal and non-delegable beyond certain limited exceptions. In other words, the DGA still continues to strengthen an *individualistic* model of data governance, precluding more ambitious *collectivist* models of data governance where, for instance, the collective interests of data subjects would be recognised and cooperatives would be allowed to pool and process aggregated data, as do Drivers' Seat in the US and PescaData, which pools the data of fishing cooperatives in Mexico. We found a relative lack of collective data pools in the EU cooperative ecosystem.

Legal changes are needed to promote a bolder and more capacious data cooperative movement. It seems necessary, for example, to extend the DGA beyond its current scope and encourage exploration of more ambitious collaborative attempts to support data pools beyond the limited scope of 'data altruism.' In addition to reforming the DGA, bodies created by this regulation such as the European Data Innovation Board could more proactively include representatives of the cooperative movement. It also seems necessary to envisage certain exceptions to the GDPR requirements regarding the processing of personal data for collective and public-interest purposes.

Conclusion

Data cooperatives present an innovative and radical approach to the governance of collective data while preserving data subjects' agency over their personal data. They therefore merit the urgent attention and support of EU policymakers. Legal frameworks such as the GDPR and the DGA affect data cooperatives, yet these entities have no say on the laws themselves. Greater collaboration is needed between data cooperatives, legislators, policymakers and public institutions. Cooperatives should not be passive witnesses to legal changes but become active stakeholders in their making.

Collaboration between various stakeholders and data cooperatives can bring about data sovereignty for citizens as well as significant social value. However, current data protection law and other proposed data laws continue to promote a more individualistic conception of data, even by some existing data cooperatives. Given the benefits of collective data approaches, we suggest that policymakers should more boldly pursue a collective conception of data and of data cooperative models. They must go beyond current conceptions of 'data altruism' and embed the socio-relational value of aggregated data in the law.

18 DGA, recital 30.

Data sharing in search of sovereignty: the case of the European cloud

Mariavittoria Catanzariti[1]

This paper explores the tension between the use of extraterritorial claims for data and the opposite response of data nationalism. Arguing that both are forms of territory-based control, it proposes applying a functional approach to data sharing – as an alternative to data location – to the project for an EU cloud.

Introduction

Jurisdictional claims for data are underpinned by two opposing regulatory models. The first claims an extraterritorial digital reach. Examples include access to data located abroad by domestic law enforcement authorities, global injunctions and claims of territorial extension of domestic law. The second, often in reaction, relies on data nationalism. Examples include data localisation requirements by national governments and the establishment of national clouds for various types of data. This paper challenges the presumed territoriality/extraterritoriality dichotomy and claims that 1) this apparent dichotomy leads to converging territorial solutions; and 2) territorial overuse undermines the geopolitical and legal order. Based on these assumptions, the paper argues that, when it is applied to data, territoriality needs to be profoundly rethought so that inter-state frictions and extraterritorial jurisdictional claims can be avoided. This implies moving beyond the territoriality/extraterritoriality dichotomy and using functional factors that do not necessarily depend on the territorial location of data to regulate data flows. Such an approach proves to be useful in order to frame the project for an EU cloud in the broader debate on EU digital sovereignty (Pohle 2020; Moerel-Timmes 2021).

The territoriality/extraterritoriality dichotomy

All over the world regulators have sought to: a) enlarge the territorial scope of their sovereign powers over data; and b) re-territorialise data-enabling territories with digital capabilities. These two options appear to be opposites but in fact they converge in many ways because they are both forms of territory-based control (Christakis 2020). The first option allows regulators to gain regulatory traction over apparently borderless data through linkages with data infrastructure located in state territories or with activities associated with data infrastructure outside those territories (for example, local storage and processing requirements and geo-blocking). This includes adjudicating rights by granting the public and private sectors access to data worldwide or enabling courts to issue extraterritorial injunctions (Woods 2018). The second option means grounding data governance in the physical location of data infrastructure and building the idea of digital sovereignty in two possible ways: by laying down legal norms, e.g. requiring companies to store, process and copy data exclusively on servers located within the national borders; or by ensuring compliance with them such as with extraterritorial orders and global injunctions based on the location of corporations (Chander and Lê 2014, 2015).

This paper contends that the legal status of data is not inherently dependent on connecting territorial factors to the physical infrastructure of data cables because of their non-territorial and ubiquitous nature (Daskal 2013). Data are non-territorial in the sense that their physical location does not really matter in terms of what data represent and neither does it matter for the underlying relevant interests at stake. Data are also ubiquitous in the sense that they can be used by multiple actors while being accessed everywhere irrespective of where they are located. Where data are originated, located or accessed presents a challenge to traditional regulatory models based on territorial jurisdiction as the basic principle of jurisdictional order. It is extremely hard to precisely describe the geographical route of data in movement, as data live in many copies and places.

A lack of technological autonomy in the EU has generated extraterritorial claims over data in reaction to extraterritorial violations by third countries of individual rights protected by EU law. This has been possible because of

1 Research Associate, European University Institute (Centre for Judicial Cooperation – RSCAS), Mariavittoria.catanzariti@eui.eu

a 'loss of data' due to data storage in foreign clouds, as was the case of the NSA scandal. Failure to recognise this, in terms of regulatory responses, creates a chain reaction: states with more technological and economic power exercise the strongest extraterritorial claims, as is exemplified by the adoption of the US CLOUD Act, which has allowed an overreaching extraterritorial use of sovereign powers (police orders) all over the world, or the strongest territorial traction for digital investments, as is exemplified by the Chinese Security Law. Conversely, EU law has tried to reappropriate territorial shares with different degrees of extraterritorial reach: enlargement of the territorial scope of application (Cremona and Scott 2019); strengthening the requirements for data transfers to third countries (*Schrems I* and *II*); or a defensive approach to standard setting against extraterritorial interferences. Often the justification that is used is that the extraterritorial reach of EU law better preserves individuals' data, substantially legitimising a global reach of EU fundamental rights such as privacy and data protection (Schwartz and Peifer 2017) and positioning EU law in the global market as a standard setter (Bradford 2020). A result of this trend is that there is currently an alignment between the academic literature and EU policy and regulation on the EU's data strategy. The landmark concept, even if is not spelled out, is the expansion of the legal notion of territory (Scott 2014) throughout European data spaces – industry, green deal, health, mobility, finance, energy, agriculture and public administration – where data can flow freely within the EU across sectors. These data spaces basically overlap with a sectoral scope of application of EU law across subject matters that is territorially based.

However, many legal phenomena in sectoral areas of EU data governance show how the nature of data is disruptive with respect to physical territory. In the field of data protection, the right to dereferencing (e.g. removing links related to personal information) has sometimes only been imposed for data located within the EU (CJEU, *CNIL* case) but it has also been granted to individuals vis-à-vis companies established outside the EU, to which EU data protection law has been applied (CJEU, *Google Spain* case). In disputes related to electronic commerce, requirements for intermediaries to remove illegal content have operated worldwide (SCC *Equusteek* and CJEU *Facebook* cases). In the field of access to data by law enforcement, public authorities have issued some warrants to service providers to release data irrespective of the location of their storage (*U.S. v. Microsoft* case). In intellectual property law, orders from national courts to operators of online marketplaces that advertise and offer goods for sale on their websites targeting consumers outside the EU aim to also prevent infringements of intellectual property rights in third countries (CJEU, *L'Oréal SA* case). As for the global protection of human rights, transatlantic mass-surveillance of individuals programmes violate the right to respect for private life under the European Convention of Human Rights (ECtHR, *Big Brother Watch v. UK* case). As for the global reach of the European Charter of Fundamental Rights, the Safe Harbour Agreement and the Privacy Shield were declared invalid under EU law for violating Mr. Schrems's fundamental right to data protection after his data were transferred and physically relocated in the United States (CJEU, *Schrems I and II* cases).

Towards a functional approach to an EU cloud

Our aim is to reflect whether the ongoing strategy to establish a model of EU cloud computing may overcome the territoriality/extraterritoriality dichotomy. The function of a European cloud would primarily be to store, share and reuse personal and non-personal data in the European data infrastructure in order to achieve technological autonomy. Based on the institutional French-German Gaia-X Initiative (Federated Data Infrastructure for Europe), which was based on previous national projects,[2] the European trend toward a model of digital sovereignty has great potential if it is based on the technical interoperability of adequacy standards instead of on a model of digital borders. Being digitally sovereign means Europe being independent from other countries and from technological solutions imposed by the private sector. The Digital Summit Focus Group defines digital sovereignty as the "possibility of independent self-determination by the state and by organisations with regard to the use and structuring of digital systems themselves, the data produced and stored in them, and the process depicted as a result" in order to gain "complete control over stored and processed data and also the independent decision on who is permitted to have access to it."[3]

Overcoming territoriality in cloud computing implies using functional criteria for the EU cloud that make control over data possible through interoperable standards. I rely in particular on a novel functional perspective that considers what data stands for: underlying interests at stake in sharing data as jurisdictional connecting factors. Functional criteria promise to better address the non-territorial

2 Andromède, Bundescloud, Cloudwatt and Numergy were the first examples of European clouds designed to compete with US clouds, but they were insufficiently competitive and failed.

3 Project Gaya-X, 2019, https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/project-gaia-x.pdf?__blob=publicationFile&v=5, p. 7.

nature of data according to a) a substantial connection between data access and use and the protection of underlying interests; b) the interest in sharing data in case of conflicts of law; c) the compatibility of purposes of data sharing with multiple jurisdictional claims; and d) high standards of protection for data users (Svantesson 2015).

The functional perspective recognises jurisdiction over physical space trying to balance state interests with other equal sovereign powers when data flow beyond territorial borders. This has important practical implications for regulating data sharing in a European cloud. From a legal point of view, this may be done by means of regulation or contracts. From a technological point of view, a model of digital sovereignty is only sustainable if it constructed on a voluntary basis with common security standards and trustworthy interoperable mechanisms rather than on the basis of unilateral territorial action. Creating a theoretical regulatory model for data sharing in the EU cloud has the advantage of focusing on the interaction between specific jurisdictional powers and operational technological solutions. Based on a theoretical functional reframing of territoriality as applied to data, this paper maintains an operational solution that rejects data localisation is a possible way to build a European data cloud infrastructure. This could be a way toward a model of digital sovereignty and it only has great potential if it is based on the technical interoperability of adequacy standards instead of on a model of digital borders based on data localisation requirements. My point is that moving away from location-based approaches to data will reduce the tension caused by the global overreach of many data regulation schemes adopted by countries. So far, the EU's extraterritorial claims have been determined by the increasing dependence of state-critical digital infrastructure on a limited number of foreign market players. Conversely, functional criteria can better address the ubiquitous and non-physical nature of data than territorial connection factors can. In particular, functional criteria can attribute jurisdictional powers over data to states based on: 1) the relevant interests in data sharing; and 2) the prevalence of the advantages of data sharing and agreed common rules in potential conflicts of law. Data localisation is assumed as the functional equivalent of the territoriality principle for an EU cloud. The functional perspective questions the territorial connection as a relevant factor in data disputes and investigates how other factors better address what data stand for and what the underlying interests at stake behind data flows are.

The whole architecture for an EU cloud requires a legal analysis in which functional criteria for data sharing rather than data location act as jurisdictional triggers. This reconceptualisation is not merely theoretical. It has immediate consequences both in terms of the limits of extraterritorial claims in digital matters and the legal architecture for the establishment of an EU cloud infrastructure. Deterritorialising data aims to provide a legal alternative to the territoriality principle for an EU cloud. It focuses on the relevant factors in this model: a) openness to actors, including foreign cloud-hosting providers from third countries; and b) the inapplicability of foreign laws to EU cloud capacities. These two requirements can be used differently depending on the degree to which users share data and the choice of legal basis for the application of foreign laws to clouds. The technological autonomy of cloud infrastructure allows the use and exchange of data among EU and non-EU actors on the basis of shared security protocols and common legal standards.

There are different models for building clouds: 1) a model that imposes local data storage by European companies and public actors limiting data movement; 2) data sharing in an EU cloud among European and non-European companies based upon dedicated protocols (enhancement of the encryption measures and data security); 3) a transparent system of notifications of use and measures taken with data. A functional model of an EU cloud can be based on the feasibility of compatible interests in data sharing among different actors. In a case in which cloud providers are subject to the jurisdiction of foreign countries – countries the laws of which conflict with EU law in relation to some specific piece of sensitive data – they should make it clear in such a way that it allows other interoperable actors to avoid the risk or adopt technical measures to prevent themselves from violating EU law. Cloud providers should otherwise state that there is a conflict and verify whether any access, request for data or re-use of data by foreign countries violates EU law.

A European cloud might compete with major cloud computing services such as Alibaba, Microsoft and Amazon. A cloud that combines public cloud services with locally managed infrastructure would allow sensitive data to be located in specific jurisdictions while being linked to public cloud services. Cloud providers have much influence on data governance not only in terms of intellectual property rights regarding data and the operational functioning of physical infrastructure but also in terms of their impact on the marketplace where they deploy their technology. Besides the practical effect that data localisation may produce on market isolation and a rise in market protectionism, data localisation in fact represents the territorial metaphor for an obsolete model of data governance. There are many reasons to reject data localisation for the EU cloud:

data localisation undermines the free flow of personal and non-personal data and hampers competitiveness among markets. It also produces excessive costs for users and companies that want the flexibility to use different cloud providers and access the most advanced technological solutions. Data localisation also reduces the incentive to invest more in updating products and offering services. Additionally, data localisation would make it impossible to differentiate between personal and non-personal data in the sense that it should be applicable to all data or none in the cloud.

In terms of data security concerns, if governments mandate local storage of data, in practice what they are doing is requiring companies to split the data they possess and store it in multiple versions in order to comply with the local requirements in different jurisdictions.

From a technological point of view, data localisation implies making web services technically non-viable because of technical obstacles to providing online services. In a situation in which companies are subject to several data localisation regimes, they cannot fully ensure data localisation in many jurisdictions. Data might be stored in edge caches across borders and replicated to respect the restrictions of data location; it might be 'sharded' across multiple machines in multiple data centres; and it might be backed up in multiple locations in case there is a failure and made accessible in many places for maintenance and de-bugging.

Conclusions

Untying the operational functioning of digital jurisdiction from the geographical location of data has a fundamental impact on the model of digital sovereignty for Europe (Floridi 2020). First, storing data on EU servers requires a huge investment in infrastructure but it can only be done on a voluntary basis. This entails offering users and private actors incentives to choose to locate data on EU servers rather than with other services. Second, ensuring Europe and the Member States maintain jurisdictional power on the basis of operational functional criteria that are alternative to data location creates a valuable network of partners which voluntarily decide to share data on a cloud that guarantees better standards. These standards can be, for example, interoperability adequacy standards, technological security standards and/or rights protection standards. The operational functioning of the EU cloud strongly depends on the type of data that are shared: if they are user data (the data stored in the cloud), derived data (data learned by cloud providers about behaviours on the cloud) or system data (data learned by cloud providers about system functioning). My idea favours the integration of all these data through a transparent mechanism notifying users that would allow full control of data that are processed through decentralised edge mechanisms that are independent of localisation requirements. This implies the possibility of enlarging: the number of actors who can operate on the cloud; the purposes of data sharing among the users of the cloud; and the capacity to exert jurisdictional claims based on compliance with interoperability adequacy standards and not based on the territorial connecting factors of data and infrastructure.

In conclusion, this paper has shown that the principle of territoriality if applied to data needs to be rethought and revised (Hörnle 2021) taking into account the advantages offered by a functional approach. Choosing the EU cloud as a case study is illustrative of the relevant effects that territorially based and functional approaches to jurisdictional claims over data may have. In practice it can show the sterility of the alternative between digital sovereignty – in other words, digital territoriality – and digital extraterritoriality and opens functional data sharing as an opportunity for Europe.

References

Bradford, Anu (2020), The Brussels Effect: How the European Union Rules the World (Oxford: Oxford University Press).

Chander, A. and Lê, U (2015), 'Data Nationalism,', Emory L. J. 64: 677.

Christakis, T. (2020), 'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy (7 December 7, 2020). Available at SSRN: https://ssrn.com/abstract=3748098 or http://dx.doi.org/10.2139/ssrn.3748098

Cremona, M. and Scott, J. (2019), *EU law beyond EU borders: the extraterritorial reach of EU Law*, (Oxford: Oxford University Press).

Daskal, J. (2013) 'The Unterritoriality of Data,', Yale Law Journal, 25(2): 326.

Desai, D. (2013), 'Beyond Location: Data Security in the 21st Century,', Communications of the ACM, 56.

Floridi, L. (2020), 'The Fight for Digital Sovereignty: What it is, and Why it Matters, Especially for the EU,', Philosophy & Technology, 33: 369–378.

Hörnle, J. (2021), *Internet Jurisdiction: Law and Practice*, (Oxford: Oxford University).

Moerel, L. and Timmers, P. (2021), 'Reflections on Digital Sovereignty,', Available at SSRN: https://ssrn.com/abstract=3772777.

Pohle, J. and Thorsten, T. (2020) 'Digital Sovereignty'. Internet Policy Review, 9(4) https://doi.org/10.14763/202.4.1532.

Schwartz, P. and Peifer, K. N. (2017), 'Transatlantic Data Privacy Law,', The Georgetown Law Journal, 106: 115.

Scott, J. (2014), 'Extraterritoriality and territorial extension in EU law', The American Journal of Comparative Law 62: 87.

Svantesson, D. (2015), *New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft*, AJIL Unbound, 115: 69-74.

Woods, A. (2018), *Litigating Data Sovereignty*, Yale Law Journal, 128: 328.

networkindustries quarterly

Open Call For Papers

The liberalisation and more recently the digitalisation of the network industries have brought various challenges to incumbent firms operating in sectors such as air transport, telecommunications, energy, postal services, water and railways, as well as to new entrants, to regulators and to the public authorities. Therefore, Network Industries Quarterly is aimed at covering research findings regarding these challenges, to monitor the emerging trends, as well as to analyse the strategic implications of these changes in terms of regulation, risks management, governance and innovation in all, but also across, the different regulated sectors.

Published four times a year, the Network Industries Quarterly features short (2000-2500 words) analytical articles about these topics in both the industrialised and the emerging countries. It provides original analysis, information and opinions on current issues. Articles address a broad readership made up of university researchers, policy makers, infrastructure operators and infrastructures services providers. Opinions are the sole responsibility of the author(s). Contact info@ic4r.net or fsr.transport@eui.eu to subscribe. Subscription is free.

Network Industries Quarterly is jointly published by the Transport Area of the Florence School of Regulation (European University Institute) and the Istanbul Center for Regulation (Istanbul Technical University). It is an open access journal funded in 1998 and merged with Network Industries Quarterly Turkey in 2022. Prof Matthias Finger is its foundational and current director.

Article Preparation

Network Industries Quarterly is a multidisciplinary international publication. Each issue is coordinated by a guest editor, who chooses four to six articles related to the topic chosen. Articles must be high-quality, written in clear, plain language. They should be original papers that will contribute to furthering the knowledge base of network industries policy matters. Articles can refer to theories and, when appropriate, deduce practical applications. Additionally, they can make policy recommendations and deduce management implications.

Detailed guidelines on how to submit the articles and coordinate the issue will be provided to the selected guest editor.

Additional Information

More Information

- *network-industries.org*
- *fsr.eui.eu*
- *ic4r.net*

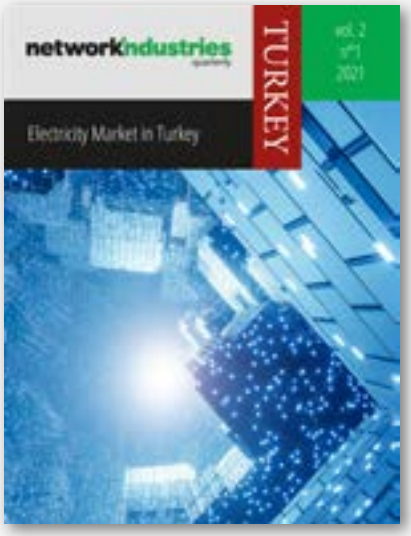
Questions / Comments?

Teodora Serafimova, Managing Editor:
Teodora.Serafimova@eui.eu
Ozan Barış Süt, Designer:
ozanbarissut@gmail.com

Past Issue

Vol 24 - No. 2 (2022)
Digital platforms: The new network industries?

For more issues, please click



Past Issue

Vol 2 - No. 2 (2022)
Regulation of Digital Platforms in Turkey

For more issues, please click