

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

Mariavittoria Catanzariti<sup>1</sup>

*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 trac-

tion 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

<sup>1</sup> Research Associate, European University Institute (Centre for Judicial Cooperation – RSCAS), [Mariavittoria.catanzariti@eui.eu](mailto: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,<sup>2</sup> 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.”<sup>3</sup>

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/GAIA-X/Redaktion/EN/Publications/project-gaia-x.pdf?\\_\\_blob=publicationFile&v=5](https://www.data-infrastructure.eu/GAIA-X/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 recon-

ceptualisation 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.