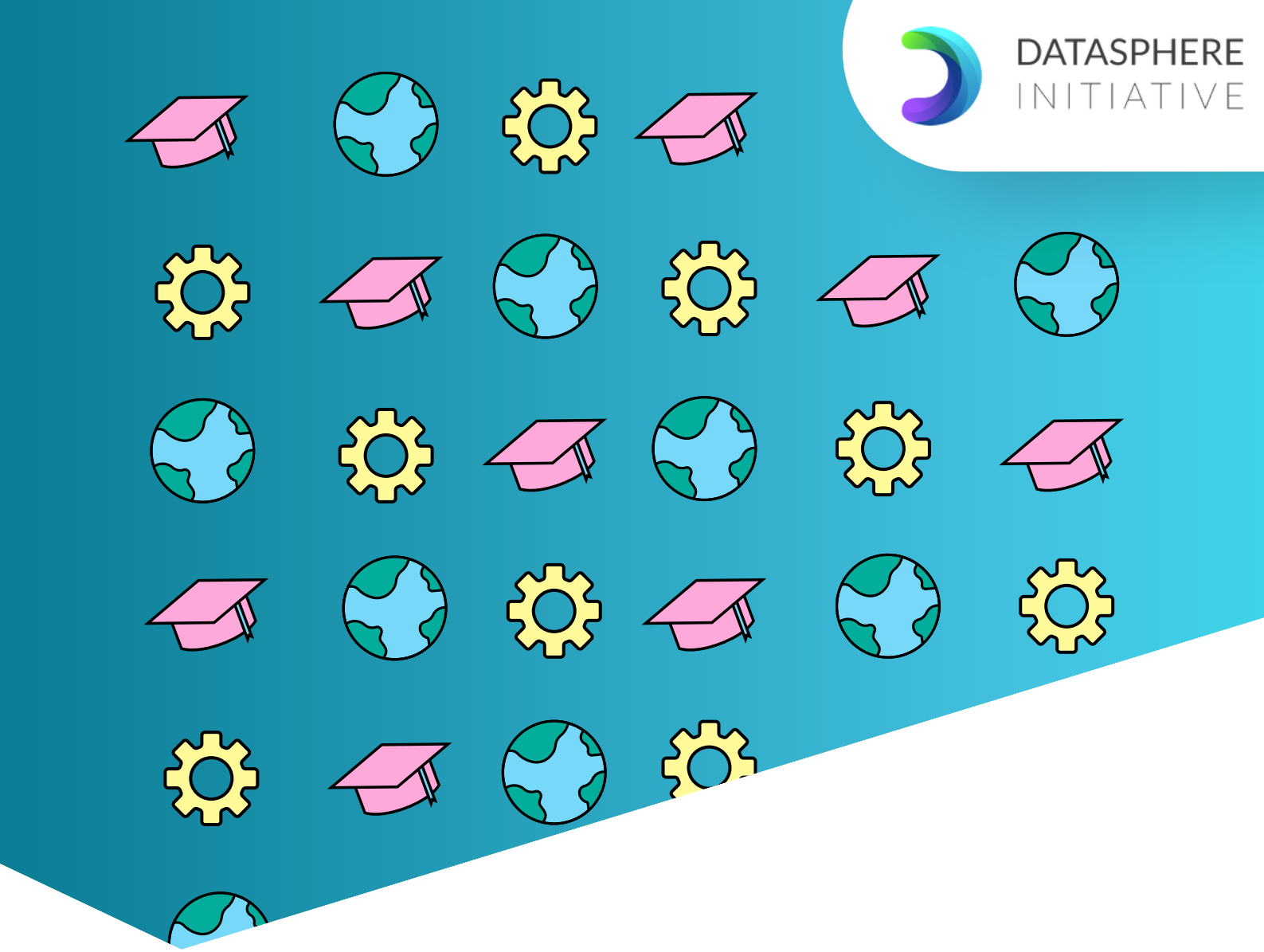


DATASPHERE INITIATIVE

THE RISE OF EUROPEAN DATA

A KANTIAN IMPERATIVE FOR GLOBAL DATA GOVERNANCE

FRANCESCO VOGELEZANG

FELLOWSHIP
2021-2022

ABOUT THE DATASPHERE INITIATIVE

The Datasphere Initiative is a global network of stakeholders fostering a holistic and innovative approach to data governance. By cultivating dialogue and connecting communities, the Datasphere Initiative connects sectoral silos and people to build a collaboratively governed datasphere and responsibly unlock the value of data for all.

For more information, visit www.thedatasphere.org or contact info@thedatasphere.org.

REPORT CITATION AND COPYRIGHT

Vogelezang, F. (2022) The rise of European Data. A Kantian Imperative for Global Data Governance. Datasphere Initiative.

ACKNOWLEDGEMENTS

The Paper was authored by **Francesco Vogelezang** as an output of the Datasphere Initiative Fellowship Program 2021-2022.

Francesco is thankful to **Bertrand de La Chapelle**, Chief Vision Officer, **Carolina Rossini**, Director of Policy and Research, and **Sophie Tomlinson**, Director of Partnerships and Communications at the Datasphere Initiative for their review and input.

The paper has been designed by **Natalia Loungou.**

ABOUT THE AUTHOR

The Data Governance Act introduces new standards aimed at combating unlawful cross-border transfer and government access to non-personal data held by public sector authorities, data intermediation services, and data altruism organizations.

Francesco Vogelezang

Francesco Vogelezang is a policy analyst at the Open Future Foundation – a think tank for the open movement – where he conducts policy research on European data governance files, with a focus on the Data Commons.

He holds a Bachelor in European Studies from Maastricht University, with a minor in European and International Law. He graduated from SciencesPo Paris – with the Student of Honor award – where he obtained a Master's degree in European Affairs, with a specialization in Digital, New Technology & Public Policy.

In addition, Francesco has previous experience in project leadership as he worked as a Topic Manager for Student Forum Maastricht, where he guided the drafting process of a policy proposal to the European Commission on public sector digitization. Similarly, he was the co-lead of the Digital Democracy cycle of the Institute for Internet & the Just Society where he managed pro-bono research projects on issues related to internet governance.

Francesco is currently based in Amsterdam, the Netherlands. In his free time, he enjoys reading, running, playing golf, and (trying to) reconnect with his Dutch language heritage.

This paper is an outcome of his Fellowship at the Datasphere Initiative 2021/2022. Francesco's research focused on the impact of legislative developments at the European level on the concept of the datasphere with a particular focus on the European Union Data Governance Act and its extraterritorial impact on the emergence of global data governance regimes.

TABLE OF CONTENTS

ABSTRACT

Data localization measures are on the rise. Data is increasingly seen by state actors as a means to secure geopolitical objectives while increasing domestic economic competitiveness. The European Union, under the von der Leyen Commission, has made digital sovereignty one of its key policy priorities to safeguard Europe's interests and values in global debates around tech regulation. In this field, the most recent legislative activity has taken place around data governance, with the adoption of the Data Governance Act (DGA) and the publication of the Data Act (DA) proposal. Among many objectives, both Regulations aim to combat illegal transfers of non-personal data to the rest of the world by ensuring that Europeans' data travels with appropriate safeguards in cross-border exchanges. This essay assesses the impact on global data flows of the cross-border provisions introduced by these two Regulations. It emerges that the rules introduced by the DGA and DA underpin a renewed geopolitical ambition of the European Commission in global data governance discussions. Not only that, the two measures foster the emergence of a new geographic conceptualization of data – i.e. "European data" – that transcends individual approaches to data regulation where data can be seen as a "strategic national asset" to consolidate economic and political objectives (Solano et al., 2022, p. 18). Based on this concept, this paper assesses whether a geographical approach to data governance can contribute to the emergence of transnational open standards or whether it can further exacerbate ongoing fragmentation of global data flows.

INTRODUCTION

The EU-US Trade and Technology Council (TTC) is a transatlantic forum set up in June 2021 which aims to foster cooperation on digital trade and technology-related issues between the European Union (EU) and the United States (US). The TTC comprises ten working groups operating on issues related, but not limited to, climate and clean tech, investment screening cooperation, global trade challenges, and data governance. The last category arguably constitutes the most contentious topic given the long standing tradition on both sides of the Atlantic of failing to secure lawful personal data sharing agreements. Already in 2014, with the first Schrems judgment, the Court of Justice of the European Union (CJEU) invalidated the 2000 US-EU Safe Harbor Agreement on the grounds that, in the context of cross-border transfers of EU citizens' personal data, the US legal framework did not provide an adequate level of protection to that offered by the EU law. Then, in 2017, with the second Schrems ruling, the CJEU equally invalidated the newly negotiated Privacy Shield. As a result, transatlantic data flows for personal data now rest on an intricate ramification of adequacy decisions, appropriate safeguards, and derogations that have the ultimate effect of disrupting data exchanges (Jurcys et al., 2022). Christakis (2020) describes the current status-quo as a "gray zone compliance" in cross-border situations. The recently announced EU-US Trans-Atlantic Privacy Framework (2022) on March 25, 2022 should provide a long-awaited and much needed legal framework.

Despite these difficulties in securing a comprehensive cross-border data sharing framework, legislative activity has not halted. In particular, the EU has worked on two main initiatives as part of its European strategy for data: the Data Governance Act (DGA) – approved in April – and the Data Act (DA) – proposed in February. Among many provisions, the two Regulations introduce new standards aimed at combating unlawful cross-border transfer and government access to non-personal data held in Europe, with the objective of preventing conflicts with Union law. Arguably, the new rules for non-personal data resemble those for personal data protection as both the DGA and DA make sure that data originating from Europe travels with appropriate safeguards across borders. As such, there seems to be greater alignment between the European personal and non-personal data sharing regimes in cross-border situations, which seems to give rise to a geographical approach to data.

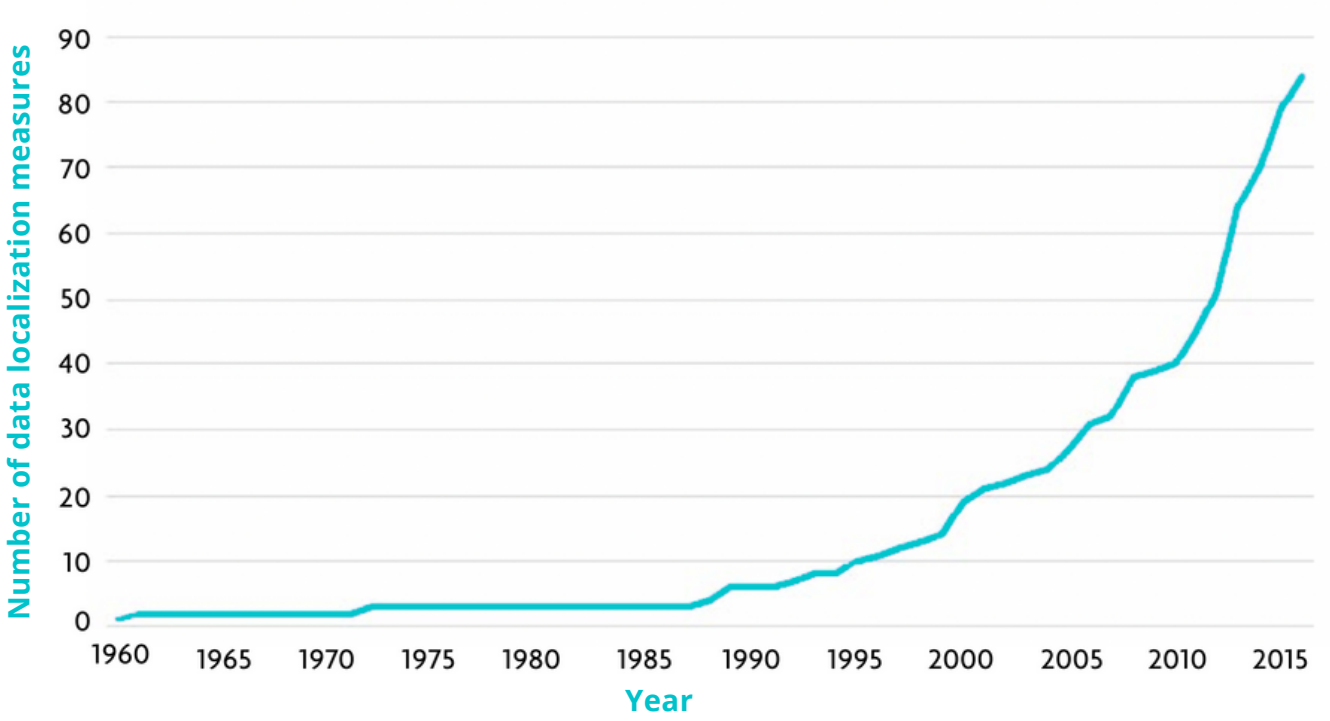
This essay explores the impacts of both the DGA and DA on cross-border exchanges by investigating the emergence of a geographical approach to data by the EU. It does not aim to provide a policy framework to solve disputes surrounding global dataflows, but to contribute to the academic and policy discussions on cross-border data exchanges. It emerges that both the DGA and DA constitute a true normative shift from the EU's traditional approach of digital regulation as they aim at maximizing internal non-personal data sharing while preventing situations where foreign access requests might collide with EU law. In turn, this approach can contribute to ongoing fragmentation of global data flows if no corresponding standards of protection are developed in third countries (Perarnaud, Rossi, and Musiani, 2022). Yet, at the same time, a geographical approach to data can also be conducive to multilateralism if data can sufficiently be leveraged as a "transnational strategic asset" across national jurisdictions.

First, this essay provides a brief conceptual overview of global data flows, data sovereignty, and data localization measures. Second, it takes a closer look at the European data governance ecosystem by analyzing the new rules for cross-border data transfers introduced by the DGA and DA. Third, based on the analysis, it discusses the emergence of a geographical approach to European data. Finally, the conclusion wraps up the research findings and proposes venues for further research.

AN EMERGING TREND: DATA FRAGMENTATION

Manyika et al. (2016) estimate that cross-border data flows contributed in 2014 with US$2.8 trillion to world GDP, exceeding the impact of the global physical goods trade. In 2019, the UK Trade Policy Observatory estimated that international e-commerce represented a total of US$148 with US$2 more trillion arising from digitally delivered services (Borchert, I. et al. (2021). In total, digital trade was worth between US$5.5 and US$6 trillion, which corresponds to almost 25% of total world exports.

Yet, data localization measures are on the rise as a means for countries worldwide to assert economic influence. Given the increasing digital shift of trade and economic power, it is no surprise that protecting data has become a synonym for local value creation and increased geopolitical competitiveness. Since access to data constitutes a source of power legitimization, controlling who has access to the means of power corresponds to being able to project global influence in the digital economy. As figure 1 shows, countries have resorted to increasing localization requirements to dilute fears of losing control over data.



"Increase in data localization measures globally" (1960-2015). (Wu, 2021, p. 10)

Data localization measures can be defined as “non-trade barriers, for they explicitly aim to limit flows across borders by requiring companies to store and process data within national borders” (Treverton and Esfandiari, 2020, p. 12). They have the objective of storing data within national jurisdictions, with the goal of making it subject to its specific domestic laws. For this reason, data localization measures are often interchanged with the concept of “data sovereignty”, which can be understood as “the right to control the collection, ownership and application of citizens’ data'' (Aaronson, 2021, p. 3). However, data sovereignty can also be seen as one of the many operationalizations underpinning the broader concept of digital sovereignty where localization requirements are the means to assert power globally over data.

Wu (2021) delineates three categories of data localization measures. First, with “local-only storing, transmission and processing”, countries prohibit international data transfers by locally managing data to establish control over their citizens. This is the typical approach underpinning Chinese and Russian ecosystems. Second, companies can also be required to maintain a local copy of data in local servers and data centers. This approach, typical of India, makes it easier for law enforcement authorities to access data in case of criminal investigations. Third, with “narrower conditional restrictions”, transfers of data outside the country are only permitted if certain conditions are met by the recipient country. This is the EU approach which falls within the scope of this essay.

Data localization measures are applied not only in domestic laws stipulating conditions for data to leave national borders, but also in international trade agreements. Aaronson (2021) identifies three mechanisms where state actors enjoy considerable leeway to petrify localization measures in international trade agreements. First, while agreements aim to liberalize data flows, wide exceptions apply in cases where signatories can restrict data flows on grounds of national security, social stability, public health, and privacy. Second, while signatories tend to ban practices where data must be stored and analyzed locally or be subject to performance requirements – for example, “mandating a business to build a factory or invest in a firm to operate in a country” (p. 14) – they have not addressed practices which have a broader effect on market access, such as Internet shutdowns or the spread of disinformation. Third, almost every digital trade agreement contains rules on personal data protection and consumer protection. However, to be made enforceable, they require a corresponding level of alignment across various legal regimes that can simultaneously apply rules to big data firms in cross-border settings. On the contrary, diverging national standards targeting tech giants have an opposing effect in creating new barriers to digital trade.

These caveats reinforce a regulatory tendency where national jurisdictions can carve out significant exceptions to restrict global data flows based on domestic interests. Ultimately, these loopholes make cross-border flows conditional on the alignment between various countries’ domestic rules on data. If not, cross-border legal divergences between State-actors foster the emergence of what could be seen as “national data fortresses”, where data is hoarded within a national jurisdiction due to the lack of legal interoperability with third countries. In the case of personal data protection, it has long been argued that privacy and trade are two mutually conflicting concepts given the need of balancing individuals’ protection against liberalized data flows (Chander and Schwartz, 2022). However, this relationship between protection and trade is replicating itself on non-personal data too. Current developments in the European context of data governance suggest a similar approach where global non-personal data flows can be restricted by protection imperatives. This is the object of analysis in the next section.

THE EUROPEAN DATA GOVERNANCE ECOSYSTEM: FROM DATA PROTECTION TO DATA PROTECTIONISM?

In digital regulation debates, the EU has long been perceived as a normative values-based actor concerned with the protection of its citizens' data and the establishment of a competitive digital market through harmonized rules (see Akcali Gur, 2020; O'Hare and Hall, 2021). It is no surprise that, regarding cross-border transfers of personal data, the EU imposes explicit requirements regulating access and transfer to third countries, with the goal of providing equitable protection. In this light, O'Hare and Hall (2021) have conceptualized this approach as the "Brussels' Bourgeois vision of the Internet" that can be summed up around the protection of individual liberty and civility through the anticipation and neutralization of harm. Accordingly, Brussels' Internet tries to preserve openness while making it conditional on the preservation of its core values.

That being said, the EU's approach to Internet regulation has at the same been interpreted as conducive to increasing its global influence. Anu Bradford (2020) has coined the famous term of the "Brussels Effect" to describe the EU's ability to influence markets' and states' conducts worldwide by means of internal market regulation. In regulating its domestic affairs, the EU manages to create a global standard of regulation not only applicable to non-EU actors wanting to serve its large market, but also eventually becoming the object of emulation by third countries. Here, a classic example is the General Data Protection Regulation which has arguably become the global gold standard in personal data protection law (Lam, 2017). Cervi (2022) finds that the EU's success in exerting global influence in data protection can be ascribed to three main factors: "its internal market appeal, its credibility as a regulator and enforcer, and the timing of its regulatory actions in line with evolving policy needs" (p. 17).

As such, internal drives for market regulation contribute to an external "globalizing role" of the EU, where its laws become the object of imitation by third countries. And while this has long been the case for personal data protection rules, recent regulatory interventions reveal a similar drive for non-personal data too. This was particularly clear in the European strategy for data (2020) where the Commission emphasized its ambition to invest in industrial data to become a successful player in the data-agile economy. On this point, the Commission acknowledges that the "winners of today will not necessarily be the winners of tomorrow" (p. 3) as new opportunities for technological leadership will arise from "industrial and professional applications, areas of public interest or Internet-of-things applications in everyday life, areas where the EU is strong" (p. 3). The European strategy for data describes this as the "third way" in digital policy where the EU can provide an effective alternative to the State-led Chinese system and the US market-based approach. This third way would safeguard the protection of European principles, values, and fundamental rights while boosting economic competitiveness and value creation in Europe. With data, Brussels aims to take part in the race to technological regulation as a true competitor to the Chinese and US approaches. On these issues, the EU Commissioner for the internal market Thierry Breton released two emblematic statements early in 2020:

"Europe may have lost the battle to create digital champions capable of taking on US and Chinese companies harvesting personal data, but it can win the war of industrial data".

"My ambition is that European data will be used for European companies in priority, for us to create value in Europe".

This ambition to become a leading player in the global regulatory ecosystem for digital technologies also finds its application in the 2020 State of the Union address by Commission president Von der Leyen. One of the main objectives in the first 100 days of office was indeed to become "the geopolitical Commission" (p. 8) to advance global multilateral cooperation while protecting European strategic interests. As Renda (2022) claims, this can be ascribed to Brussels' self-perceived "role of global regulator" in the field of data governance (p. 4) and as a form of "regulatory bullying" (Aaronson, 2021, p. 12). In this light, regulatory activity in the European data governance ecosystem becomes an important tool to project external geopolitical ambitions in relation to access to and use of industrial data.

External influence on private and public players can also be linked to the concept of "European digital sovereignty", one of the most used terms in digital regulatory discussions at the EU level. The European strategy for data (2020) already anticipated that "in order to release Europe's potential we have to find our European way, balancing the flow and wide use of data, while preserving high privacy, security, safety and ethical standards" (p. 3). Although there is no official definition of digital sovereignty and consistent applications by EU institutions, agencies, and bodies, digital sovereignty can be generally understood as "a form of legitimate, controlling authority over —in the digital context—data, software, standards, services, and other digital infrastructure, amongst other things" (Floridi, 2020, p. 370). Here, Roberts et al. (2021) find that data governance is the field where references to digital sovereignty are most recurrent.

This finding does not come as a surprise in light of legislative initiatives which have recently underpinned the Commission's activity in data governance. Both the DGA and DA constitute a true normative shift from the EU's traditional approach to digital regulation as they aim to maximize internal non-personal data sharing while preventing situations where foreign access requests might collide with EU law. On this point, Renda (2022) even claims that the EU has effectively betrayed its core values as it has shifted from supporting the development of open standards to the adoption of a "quasi-autarchic" approach to technology policy (p. 14). Likewise, Komaitis (2022) has recently stated that the EU has fallen into a so-called "China-trap" as it has shifted its regulatory activity from the preservation of open standards to control how power is distributed in the online environment. Data is no stranger in these discussions as access and control to data sharing is a requisite for greater self-sufficiency in the online sphere. Thus, by analyzing 13 different free trade agreements as well as the EU's position in the World Trade Organization, Scassera and Elebi (2021) find that the "EU has adopted a colonialist strategy, going out to hunt for data from the global South, in order to position its own companies in the new global cybernetic value chains" (p. 1). These objectives are pursued with the premise of generating greater value in Europe and, therefore, increase competitively against the rest of the world.

Range and Mayer (2020) have previously argued that if there was an official EU religion, it would definitely be privacy – given its almost obsessive focus on personal data protection. Yet, the recent geopolitical shift of the Von der Leyen Commission may arguably be changing the regulatory narrative underpinning data governance from "data protection" to almost "data protectionism". As the next two subsections illustrate, this trend is particularly evident with the cross-border rules transfer introduced by the DGA and DA.

DATA GOVERNANCE ACT RULES

The new rules for cross-border transfers introduced by the DGA stipulate new standards aimed at combating unlawful cross-border transfer and government access to non-personal data held by public sector authorities, data intermediation services, data reusers, and data altruism organizations. Among the main actors introduced by the DGA, there are so-called "data intermediation services" which will be central in the European data economy to neutrally and independently intermediate transactions amongst data users, data holders and data reusers. Article 2(11) this defines a data intermediation service as:

> *"a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data".*

The second new type of actor introduced by the DGA are so-called "recognized data altruism organizations" which aim to leverage voluntary data sharing instances in the common good, such as for objectives linked to health care, climate change, mobility, the compilation of official statistics, public services, public policy making, and scientific research. These new organizations will take the shape of data repositories – i.e data pools – administered by entities of not-for-profit nature and will be subject to transparency and structural separation requirements akin to those developed on data intermediation services.

The DGA mentions that the new rules for cross-border transfers will apply to IP-protected data, trade secrets, and commercially sensitive data. Article 31 obliges public sector bodies, data intermediation services, and recognized data altruism organizations to take "all reasonable technical, legal and organizational measures, including contractual arrangements, to prevent the international transfer to non-personal data held in the Union where such transfer would create a conflict with Union law". The Regulation does not elaborate on what "all reasonable technical, legal and organizational measures" are. Yet, it specifies that any decision or judgment by a court or tribunal of a third country to transfer or give access to non-personal data held by data intermediation services, recognized data altruism organizations, public sector bodies, and data reusers must be declared invalid, unless it is based on an international agreement, such as a mutual legal assistance treaty. If there is no international agreement, transfer to a third country can only take place if there are sufficient rule of law safeguards. If these are met, data intermediation services, data altruism organizations, public sector bodies, and data reusers must then "provide the minimum amount of data permissible in response to a request, based on a reasonable interpretation of the request".

In addition, the DGA introduces in its article 5 specific rules for public sector bodies when granting the right to reuse certain categories of protected public sector information to data reusers that intend to transfer non-personal data to a third country.[1]

[1]Article 3(1) specifies that certain categories of protected public sector information include data protected by commercial confidentiality, statistical confidentiality, IP-data, and personal data.

It stipulates that, in these circumstances, public sector bodies can only transfer non-personal confidential data and data protected by IP rights if a number of conditions are met: first, the reuser must contractually comply with EU law on intellectual property rights; second, it must not disclose confidential data when transferring the data; finally, it must accept the jurisdiction of the courts or tribunals of the Member State of the transmitting public sector body. When transferring data, the public sector body must provide assistance and guidance to data reusers in complying with these obligations. To this end, the Commission can adopt implementing acts establishing model contractual clauses for complying with the obligations of article 5. Likewise, when justified by a substantial amount of requests concerning the reuse of non-personal data in third countries, the Commission may adopt implementing acts declaring the legal, supervisory and enforcement arrangements of a third country.

Finally, when certain categories of non-personal data held by public bodies are deemed too sensitive and may therefore put at risk Union policy objectives, the Commission can adopt delegated acts to lay down special conditions applicable to the transfers of such data to third countries. Such conditions must be non-discriminatory and limited to what is necessary to achieve the Union public policy objectives, and may include "terms applicable for the transfer or technical arrangements, limitations with regard to the re-use of data in third countries or categories of persons entitled to transfer such data to third countries or, in exceptional cases, restrictions with regard to transfers to third countries".

DATA ACT RULES

In parallel to the rules introduced by the DGA, the current DA proposal contains provisions which target non-personal data flows where the data transmitter is a cloud service provider.

Article 27 compels cloud service providers to take "all reasonable technical, legal and organizational measures, including contractual arrangements to prevent international transfer or governmental access to non-personal data held in the Union where such a transfer or access would create a conflict with Union law (...)". In addition (Art. 27.2), requests by public authorities or upon court orders can only be recognized or enforced if based on international agreements, such as mutual legal assistance treaties. Recital 77 specifically mentions in that regard that, in the absence of such agreements, situations may arise where a request to transfer or provide access to non-personal data arising from a third country law would conflict with an obligation to protect such data under Union law or national law, in particular as regards the protection of fundamental rights of the individual, such as the right to security and the right to an effective remedy, or the fundamental interests of a Member State relating to national security or defense, as well as the protection of commercially sensitive data. This also includes the protection of trade secrets, intellectual property rights, and contractual undertakings regarding confidentiality in accordance with such law. Hence, the proposed rules for international data transfers have important implications for cloud computing service providers as the Commission aims to prevent conflicts with EU law when third countries' access requests to non-personal data stored in Europe are not based on international agreements.

In the absence of international agreements, the DA (Art. 27.3) would allow for the transfer of EU data on the basis of administrative decision or court order by third countries if three conditions are met. First, the third country's legal system needs to outline the reasons and proportionality of the decision/order to be set out and for the decision/order to be specific in character. Second, the reasoned objection of the addressee must be subject to a review by a competent court in the third country. Third, the reviewing court must be empowered to take duly into account the relevant legal interests of the provider of such data.

This approach is in line with the data transfer regimes stipulated in the DGA for non-personal data, but with a minor addition. Article 27(3) sets that a service provider may ask a relevant EU or member state authority to assist in determining whether it may positively respond to a foreign access request relating to commercially sensitive data or implicating national security interests. The Commission is expected to develop guidelines for the assessment of whether the above conditions are met, with assistance from the European Data Innovation Board, a new EU body established by the DGA.

If the conditions of article 27(3) are met, and the transfer does not create a conflict with union law, the minimum amount of data permissible in response to a request is based on a reasonable interpretation of the request.

A LOGICAL CONSEQUENCE? THE RISE OF EUROPEAN DATA

The rules introduced by the DGA and DA not only provide greater convergence between the EU's personal and non-personal data sharing requirements for cross-border data transfers, but also cause two intended consequences and an unintended one.

First, by strictly regulating non-personal data flows to third countries – as spelled out in the European strategy for data – the EU is crystallizing its ambition on industrial data by making sure that non-EU countries face higher barriers to accessing non-personal data. Brussels is trying to consolidate preferential access to its non-personal data as a means to derive value creation in Europe and increase its competitiveness vis-a-vis the US and Chinese systems. A so-called third way to data regulation aims, externally, to make sure that Europeans' data can travel with adequate safeguards while, internally, ensuring that a data-rich environment can flourish across the 27 Member States. In turn, this has the intended effect of erasing barriers to data sharing between European companies, individuals, and public sector bodies while posing additional restrictions to the cross-border exchange of non-personal data with the rest of the world.

Second, the EU aims to impact global data governance discussions, hoping that third countries will emulate its approach for non-personal data protection, akin to the previous experience with the GDPR. The EU is thus trying to establish itself as a global regulator by making sure that its trendsetting role is visible in third countries' legal regimes. That being said, some question the effectiveness of the globalizing role of the Brussels effect. For instance, Renda (2022) has recently argued that the role of the Brussels effect will be limited in this regard because "Europe's inability to exercise legal empathy – ie, respect for and dialogue with other legal systems – may hamper its ambition to lead the world on digital regulation" (p. 12).

Equally, regarding the recent Artificial Intelligence Act, Gstrein (2022) doubts whether the Brussels effect will set a global precedent while Siegmann and Anderljung (2022) are more optimistic about the potential diffusion of the European model in third countries, especially in fostering a trustworthy and human-centered regulatory regime for artificial intelligence. Overall, the biggest take-away is that the Von der Leyen Commission has reignited a new geoeconomic role of the European Commission to influence global markets and third countries alike. A Bourgeois approach to Internet regulation also encompasses pragmatic considerations on the EU's role in setting global standards of emulation by means of internal market regulation, which smartly camouflage its geopolitical ambitions in the field.

Finally, the unintended consequence stemming from the introduction of the DGA and DA is the rise of what could be seen as "European data": a new conceptualization that transcends individual approaches to data regulation by embedding a collective approach to data governance on the basis of geographical provenance. This is done by leveraging an understanding of data as a "strategic national asset" (Solano et al., 2022, p. 18) to consolidate economic and political goals via increased control, ownership and application irrespective of the nature of data, except for its geographical origin. As such, a geographical approach to data ensures that personal and non-personal data travel across borders with equitable protection to that offered by national standards. In this sense, a geographical approach to data governance exists where, on the one hand, data accumulation and access benefit the originating geographical region while, on the other hand, transfers to a third country only occur if appropriate safeguards are adopted. In the EU, this development can be ascribed to the objective of making sure that data originating from Europe, whether it is personal and non-personal data, is adequately protected when traveling across borders.

A KANTIAN CATEGORICAL IMPERATIVE IN DATA GOVERNANCE?

The new EU rules for non-personal data protection add an extra layer of complexity to the negotiations taking place as part of the Trade and Technology Council. Although the newly expected Trans-Atlantic Privacy Framework revolves around personal data exchanges, the DGA and DA further exacerbate ongoing legal tensions between the two regimes as new conflicts might arise on non-personal data protection. Future success at the negotiating table in the field of data governance will inevitably depend on the legal interoperability between the European third way and the US market-based approach.

This difficulty in finding common ground between historically close allies is not only due to different dogmatic differences to data protection, but also to a dilemma that has long affected global data governance (de La Chapelle and Porciuncula, 2021). On the one hand, it seems that State-actors do not have sufficient incentives to engage in unconditional data sharing because of their fear of facing a competitive disadvantage by opening up data flows. On the other hand, they also want to gain access to data which is held by other countries, as a means to establish more control over precious information.

Accordingly, if replicated in all countries around the world, a geographical approach to data can be a double-edged sword: it can exacerbate cross-border legal tensions by further fostering a restrictive territorial approach to data, for which the initiator ultimately finds itself on the receiving end of other countries' restrictions.

A geographical approach to data can increase distance between national jurisdictions if local competitive advantage is prioritized at the expense of cooperation. The set of envisaged protections and safeguards introduced by a geographical approach would thus have the final result of restricting data flows if standards do not converge in third countries. Data would ultimately be stored in the originating region as a means to increase domestic value creation and consolidate competitive edges against the rest of the world. For instance, a nascent geographical approach in Europe can further away the emergence of a potential deal with the US if the rules for personal and non-personal data protection do not trigger a sufficient degree of external emulation. In this light, the Brussels effect would further contribute to ongoing fragmentation of global data flows by fostering the proliferation of national data fortresses. Bilateral trade treaties would still constitute the main basis of agreement for cross-border trade and would therefore allow State-actors to invoke localization requirements to achieve specific data sovereignty goals. As previously discussed, these could either take the shape of economic data protectionism to accumulate as much data capital as possible (Sadowsi, 2019) or they could be justified by privacy considerations and other public interest objectives. The unintended consequence would thus lead to a paradoxical situation where States wanting to maximize access to data without participating in global data flows, simply end up localizing data in their national jurisdictions and lose access to data from other regions.

However, a geographical approach to data can constitute a promising avenue for multilateralism if transnational legal differences are actively bridged and legal convergence is sought. An understanding of data as a strategic national asset (Solano et al., 2022, p. 18) could further be leveraged into a "strategic transnational asset", provided that sufficient legal convergence exists between countries. This is because it could ensure that data travels across borders with commonly agreed safeguards while, at the same time, benefitting the economies of both sending and receiving States. Hence, the Brussels effect could positively contribute to legal convergence across borders if it can be decoupled from its territorial focus and instead embraces an extraterritorial one.

That being said, reconciliation via a geographical approach to data seems to be feasible only within clearly defined regions, and between like-minded countries. Recent proposals, such as a "Bretton Woods for Data" by Denham (2021), a "Global Data Compact" (MacFeely et al., 2022), and a "New Global Data Deal" (MacFeely, 2020), try to maximize openness via the delineation of commonly agreed standards. This is also what the Trade and Technology Council is trying to achieve despite clear operational difficulties in reconciling different approaches to data governance, even among like-minded democracies. Yet, they are "local" by definition as they require legal interoperability between participating jurisdictions. Likewise, the previous EU-US Safe Harbor Agreement and Privacy Shield were clear attempts to foster a transnational data governance regime based on shared privacy and data protection rules. The recently proposed Trans-Atlantic Privacy Framework is based on the same logic. As such, even if the Brussels effect would effectively leverage its extraterritorial component, it would fall short in fostering the emergence of a truly global data sharing compact.

Thus, global regulatory activity in the field of data governance has the side-effect of making the preservation of a global open Internet ever-difficult, if not impossible, in light of varying standards of protection. A "network of networks" – initially rooted in the idea of access to information as a precondition for cyberspace's existence – is increasingly resembling a "network of national networks" – where normative considerations around the meaning and value of access to information are increasingly shied away by pragmatic considerations around control, access, and ownership of data. Therefore, any development aimed at opening up data flows between national jurisdictions will only be "glocal" in its focus as it will be possible between similar, or at least converging, national legal traditions. As a result, a truly global and open Internet is in peril, if not already surpassed as a concept by more local considerations on how to govern data. State actors are becoming more sovereign on their data to the detriment of global openness and decentralization. The world is becoming more and more pragmatic in its approach to data.

This regional blocks' model constitutes a possible avenue to maintain open networks, at least between comparable jurisdictions, but still contributes to an emerging multipolar world order. In this light, a fragmented data governance landscape would consolidate ongoing tendencies around the control of power distribution in the online sphere. And it is in this context that we will likely see geographical approaches to data taking place based on shared norms, rules, values, and visions.

To understand this phenomenon better, further research should take a closer look at the European data governance ecosystem to understand how this approach will be replicated in other parts of the world. After all, the EU has long been depicted as a trendsetter in digital regulation and might once again set the bar high for geographical approaches to data governance. The final question is whether the EU approach to data regulation will be giving rise to a Brussels effect that is either territorial in its scope and will therefore increase regulatory distance with third countries; or whether it will lead to adoption of comparable regulations in other parts of the world, maintaining the vision of a global, interoperable internet.

A fundamental question for all regulators is actually a form of Kantian categorical imperative: does their legal framework lead to a positive outcome if it is copied by all other actors? In other terms: when adopting its legislation, would a country want all other countries to replicate it? If the regulation is too self-serving, the self-defeating ultimate result might be a fragmented environment detrimental to everyone. Scalable regulations on the other hand might contribute, through their replication, to a convergence on a higher standard, benefiting everyone. This can become a litmus test for evaluating the European Strategy for Data and EU efforts to leverage its normative power to foster international convergence on higher standards.

REFERENCE LIST

Aaronson, S. A. (2021) Data is disruptive: How data sovereignty is challenging data governance. Available at: https://www.hinrichfoundation.com/research/article/digital/data-is-disruptive-how-data-sovereignty-is-challenging-data-governance/ (Accessed: 13 July 2022).

Akcali Gur, B. (2020) 'The normative power of the EU: a case study of data protection laws of Turkey', International Data Privacy Law, 10(4), pp. 314–329. Available at: https://doi.org/10.1093/idpl/ipaa013.

Borchert, I. et al. (2021) 'G7 Leaders should discuss international trade (seriously) « UK Trade Policy Observatory'. Available at: https://blogs.sussex.ac.uk/uktpo/publications/g7-leaders-should-discuss-international-trade-seriously/ (Accessed: 24 September 2022).

Bradford, A. (2020) The Brussels Effect: How the European Union Rules the World. New York: Oxford University Press. Available at: https://doi.org/10.1093/oso/9780190088583.001.0001.

Cervi, G.V. (2022) 'Why and How Does the EU Rule Global Digital Policy: an Empirical Analysis of EU Regulatory Influence in Data Protection Laws', *Digital Society*, 1(2), p. 18. Available at: https://doi.org/10.1007/s44206-022-00005-3.

Chander, A. and Schwartz, P.M. (2022) Privacy and/or Trade. SSRN Scholarly Paper 4038531. Rochester, NY: Social Science Research Network. Available at: https://doi.org/10.2139/ssrn.4038531.

Christakis, T. (2020) '"Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 3)', European Law Blog, 17 November. Available at: https://europeanlawblog.eu/2020/11/17/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3/ (Accessed: 11 July 2022).

Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (2020). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311 (Accessed: 11 July 2022).

De La Chapelle, B. and L. Porciuncula. (2021) We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty. Internet and Jurisdiction Policy Network. Available at: https://www.internetjurisdiction.net/uploads/pdfs/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf (Accessed: 30 September 2022).

Denham, E. (2021) 'A new Bretton Woods for Data - YouTube'. Available at: https://www.youtube.com/ (Accessed: 14 July 2022).

European Commission (2020) European Strategy for Data. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066 (Accessed: 11 July 2022).

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Philosophy & Technology, 33(3), 369–378. https://doi.org/10.1007/s13347- 020-00423-6.

Gstrein, O.J. (2022) European AI Regulation: Brussels Effect versus Human Dignity? SSRN Scholarly Paper 4214358. Rochester, NY: Social Science Research Network. Available at: https://papers.ssrn.com/abstract=4214358 (Accessed: 15 September 2022).

Jurcys, P., Corrales Compagnucci, M. and Fenwick, M. (2022) The future of international data transfers: managing legal risk with a 'user-held' data model. SSRN Scholarly Paper 4010356. Rochester, NY: Social Science Research Network. Available at: https://doi.org/10.2139/ssrn.4010356.

Komaitis, K. (2022) 'EU Internet regulations are falling into the "China trap"', POLITICO, 28 June. Available at: https://www.politico.eu/article/eu-internet-regulation-falling-into-china-trap/ (Accessed: 13 July 2022).

Lam, C. (2017) 'Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in Schrems v. Irish Data Protection Commissioner', Boston College International and Comparative Law Review, 40(3), p. E. Supp. 1.

MacFeely, S. (2020) 'In search of the data revolution: Has the official statistics paradigm shifted?', Statistical Journal of the IAOS, 36, pp. 1075–1094. Available at: https://doi.org/10.3233/SJI-200662.
MacFeely, S. et al. (2022) 'Towards an international data governance framework', Statistical Journal of the IAOS, 38(3), pp. 703–710. Available at: https://doi.org/10.3233/SJI-220038.

Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov, K., and Dhingra, D. (2016) Digital globalization: The new era of global data flows. Available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows (Accessed: 13 July 2022).

Maximillian Schrems v Data Protection Commissioner (2015). Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362 (Accessed: 11 July 2022).

O'Hara, K., Hall, W. and Cerf, V. (2021) Four Internets: Data, Geopolitics, and the Governance of Cyberspace. New York: Oxford University Press. Available at: https://doi.org/10.1093/oso/9780197523681.001.0001.

Perarnaud, C., Rossi, J. and Musiani, F. (2022) 'Splinternets': Addressing the renewed debate on internet fragmentation. European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/thinktafrk/en/document/EPRS_STU(2022)729530 (Accessed: 15 August 2022).

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act) (2020). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767 (Accessed: 11 July 2022).

Ramge, T. and Mayer-Schoenberger, V. (2021) Fuori i dati!: Rompere i monopoli sulle informazioni per rilanciare il progresso. Egea.

Renda, A. (2022) Beyond the Brussels Effect. Leveraging Digital Regulation for Strategic Autonomy. Available at: https://feps-europe.eu/wp-content/uploads/downloads/publications/220301%20beyond%20the%20brussels%20effect.pdf.

Roberts, H. et al. (2021) Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies. SSRN Scholarly Paper 3937345. Rochester, NY: Social Science Research Network. Available at: https://doi.org/10.2139/ssrn.3937345.

Sadowski, J. (2019) 'When data is capital: Datafication, accumulation, and extraction', Big Data & Society, 6(1), p. 2053951718820549. Available at: https://doi.org/10.1177/2053951718820549.

Scassera, S. and Elebi, C. M. (2021) Digital colonialism. Analysis of Europe's trade agenda. Transnational Institute. Available at: https://www.tni.org/en/publication/digital-colonialism (Accessed: 16 September 2022).

Siegmann, C. and Andrljung, M. (2022) The Brussels Effect and Artificial Intelligence. Center for the Governance of AI. Available at: https://www.governance.ai/research-paper/brussels-effect-ai (Accessed: 23 September 2022).

Solano, J. L., Martin, A., de Souza, S. and Taylor, L. (2022) Governing data and artificial intelligence for all. Models for sustainable and just data governance. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)729533 (Accessed: 14 July 2022).

Trans-Atlantic Privacy Framework (2022) European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087 (Accessed: 30 September 2022).

Treverton, G. F. and Esfandiari, P. (2020) Data: Governance and Geopolitics. Available at: https://technopolitics.org/wp-content/uploads/2021/Data-Governance.pdf (Accessed: 13 July 2022).

Von der Leyen. (2020) State of the Union 2020. The Von der Leyen Commission: One year on. Available at: https://ec.europa.eu/info/sites/default/files/von-der-leyen-commission-one-year-on_en.pdf (Accessed: 11 July 2022).

Wu, E. (2021) Sovereignty and Data Localization. Available at: https://www.belfercenter.org/sites/default/files/2021-07/SovereigntyLocalization.pdf (Accessed: 13 July 2022).

thedatasphere.org