4 July 2023

Geopolitical aspects of the EU's Data Strategy

Raquel Jorge-Ricart

Geopolitical aspects of the EU's Data Strategy

Raquel Jorge-Ricart | Analyst, Elcano Royal Institute | @RaquelJorgeR

Index

(*) This paper was originally published as a chapter of the PromethEUs' Joint Publication on the EU Data Strategy 'The EU's Data Strategy from a multifaceted perspective. Views from Southern Europe', https://www.i-com.it/2023/06/08/prometheus-publication-eu-data-strategy-a-multifaceted-perspective-from-southern-european-countries/.

1. Why data is a major geopolitical factor

Data is one of the most valuable resources in today's global competition – but it is not yet seen as a global common that leads to collaboration. So far, global data flows are still governed through a maze of multilateral, bilateral, unilateral, and *ad hoc* rules, principles, and voluntary frameworks that are not always accepted or applied by all actors. Cross-border international collaboration on this issue is far limited, with ups and downs in the success of a common global agenda on data governance. Also, data governance is getting balkanized in blocs that propose different, if not contrasting, data models. Doing so is as important as strategic for the maintenance of an international security and peace order which growingly relies on the power over data and has strong impacts on three layers: security, economic, and rights.

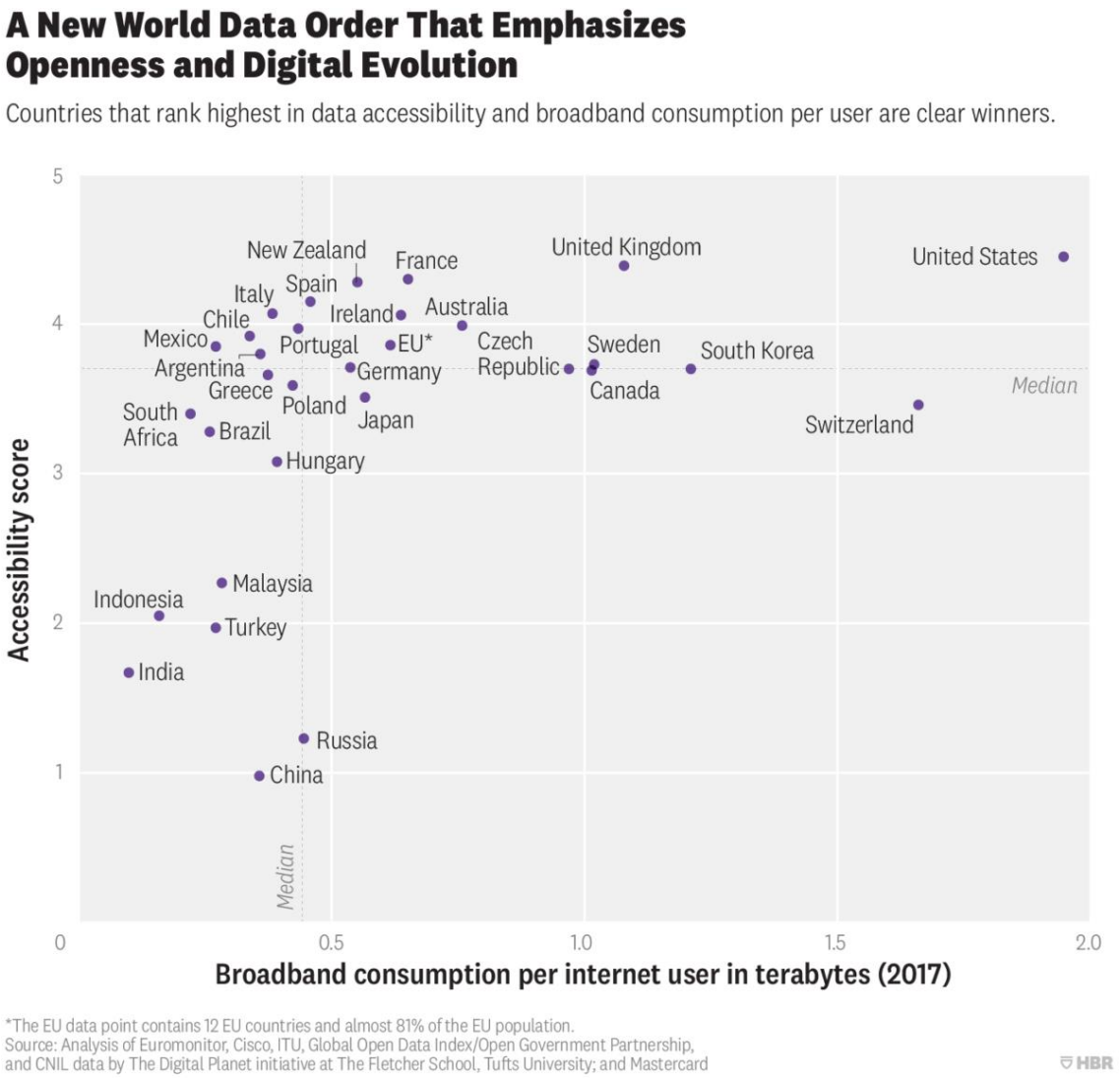
The European Union's Data Strategy aims to make the EU a leader in a data-driven society[1]. The goal of creating a single market for data is to allow data to flow freely within the EU and across sectors for the benefit of businesses, researchers, and public administrations. However, the Data Strategy has much to do with the current debate over strategic autonomy -or digital sovereignty- and the way the EU needs to promote its global vision on technology through three lens: security, economy, and rights and values. According to Harvard Business Review,[2] the countries that are leading the data economy worldwide are the United States, the United Kingdom, China, Switzerland, and South Korea. To estimate this, authors create a new metrics that may measure the wealth and power of nations based on a new version of the "GDP": **the Gross Data Product**. To identify the world's top "grow data product" producers, they consider four criteria[3]: the volume, usage, accessibility and complexity.

[1] European Commission (2023). The European Data Strategy. Accessible at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

[2] Chakravorti, B., Bhalla, A., Shankar Chaturvedi, R. (2019), "Which Countries Are Leading the Data Economy?", Harvard Business Review, 2019. Accessible at https://hbr.org/2019/01/which-countries-are-leading-the-data-economy.

[3] - Volume: Absolute amount of broadband consumed by a country, as a proxy for the raw data generated.
- Usage: Number of users active on the internet, as a proxy for the breadth of usage behaviors, needs and contexts.
- Accessibility: Institutional openness to data flows as a way to assess whether the data generated in a country permits wider usability and accessibility by multiple AI researchers, innovators, and applications.
- Complexity: Volume of broadband consumption per capita, as a proxy for the sophistication and complexity of digital activity.

Figure 1. Position per countries based on accessibility score and broadband consumption per Internet user



Source: Chakravorti, B., Bhalla, A., Shankar Chaturvedi, R. (2019), "Which Countries Are Leading the Data Economy?", Harvard Business Review, 2019. Accessible at https://hbr.org/2019/01/which-countries-are-leading-the-data-economy

Still, it remains complex to establish a ranking of "new" data leaders, as global leadership over data power cannot be only weighed in terms of who provides further accessibility. The current international system is witnessing an increasing authoritarian overhaul of data capture, storage, use and processing. According to the *Freedom on the Net* 2022 report, which assesses 89% of the world's Internet user population, 37% of the population lives in countries with no Internet freedom, 34% live in partly free countries, and only 18% of user population lives in territories where Internet freedom is fully granted[4].

[4] Freedom House (2022). *Freedom on the Net* report. Accessible at https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf.

Global Internet freedom has declined for the 12th consecutive year, and countries have applied several strategies to **access, block, disrupt, and control data**. An increasing number of national governments have blocked websites, access to data, imposed new national laws on threats to the free flow of information, have centralized technical data infrastructure, have applied regulations with stricter data localization policies which centralize the governmental control over user data, or impose companies to comply with national requirements -making them store data within the country, change their operations in a way that facilitate government censorship or requests to sensitive data, or prohibiting data users to bypass the "national digital walls" and access third countries' information. Also, restrictions and blocks on foreign websites have increased (in 2022, 37 countries did so) and 11 countries have approved new laws restricting these foreign websites and content.

These nationally driven data policies are having a major impact on how countries relate to each other, and how the global Internet is built. Censorship, filtering, market access restrictions, strict licensing regulations, joint-venture requirements, maximum foreign equity shares, nationality requirements and stricter obligations for foreign companies have led to increasing barriers to the cross-border flow of data, a topic that has become geopolitically sensitive, due to its impact on security, economic competitiveness, and fundamental rights.

The geopolitical competition has been placed at two levels: the race over the harvesting of data, and the race over the usage of data. Both have implications on how countries collaborate internationally, the political willingness to enter into international agreements on data flows (either personal or non-personal), and the much-needed role of "trust" to bundle a massive package of information and maintain international security and peace.

1. The EU's role in the geopolitics of data

It is by no chance that the EU has been addressing how their goods, services, assets, and personal data relate to third countries through several ways. The first approach is **regulation**, which has been closely followed by the majority of stakeholders. However, two other approaches are as important as strategic: the role of multilateral initiatives, "coalitions of the willing" and international meetings; and the importance of technology diplomacy as a policy area to institutionalize the geopolitics of data, alongside other technological challenges.

1.1. Through regulation

1.1.1. The General Data Protection Regulation (GDPR)

The EU's General Data Protection Regulation (GDPR) -the backbone of the EU Data Strategy- only permits the transfer of personal data to those jurisdictions that comply with a sufficient level of data protection. Article 45 gives the European Commission the power to determine whether a country outside the EU offers an adequate level of data

protection[5]. The effect of such a decision is that personal data can flow from the EU -and three Associated Countries: Iceland, Liechtenstein, and Norway- to the third country without any further safeguard being necessary.

So far, the so-called "data adequacy decisions" have been recognized in Andorra, Argentina, Canada (for commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay. All data adequacy decisions exclude data exchanges in the law enforcement sector, except for the United Kingdom.

Data adequacy provisions have as admirers as critics. On the one hand, it is perceived as a guardrail that ensures the protection of fundamental rights, the influence over third countries to develop norms which respect democratic values, and as a geopolitical tool to gain leadership over the global agenda on cross-border data flows. The GDPR is widely considered a blueprint for data privacy, often referred to as the "gold standard"[6] for international data usage, as an increasing number of countries tend to mimic the principles and structure of this regulation[7]. This would follow the Brussels Effect[8] approach, which explains how EU regulatory power is externalized, influences the behaviors of foreign governments and companies, and induces the framing of certain global norms.

On the other hand, data adequacy provisions have also received criticism because their standards may lead certain governments to "mandate domestic data storage, feature blanket exceptions for national security or state actors without safeguards, or delegate increased decision-making power to politicized regulators—all of which renders users vulnerable to government abuse despite improvements pertaining to the use of personal data for commercial purposes"[9].

1.1.2. Data Services Act (DSA) and Digital Markets Act (DMA)

The final texts of both the DSA and the DMA were a thermometer of how the EU aimed to tackle its relationship with actors from third countries. While the major impact of these rules is on the internal single market, the reality is that it addresses many aspects of digital sovereignty -capabilities of states, respect to human rights, and economic leadership.

[5] European Commission, Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
[6] Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law 6*(2), 77-78. https://doi.org/10.1093/idpl/ipw006.
[7] Luisi, M. (2022). GDPR as a Global Standards? Brussels' Instrument of Policy Diffusion. Accessible at https://www.e-ir.info/2022/04/09/gdpr-as-a-global-standards-brussels-instrument-of-policy-diffusion/.
[8] Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press, USA.
[9] Freedom House (2022). *Freedom on the Net* report. Accessible at https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf.

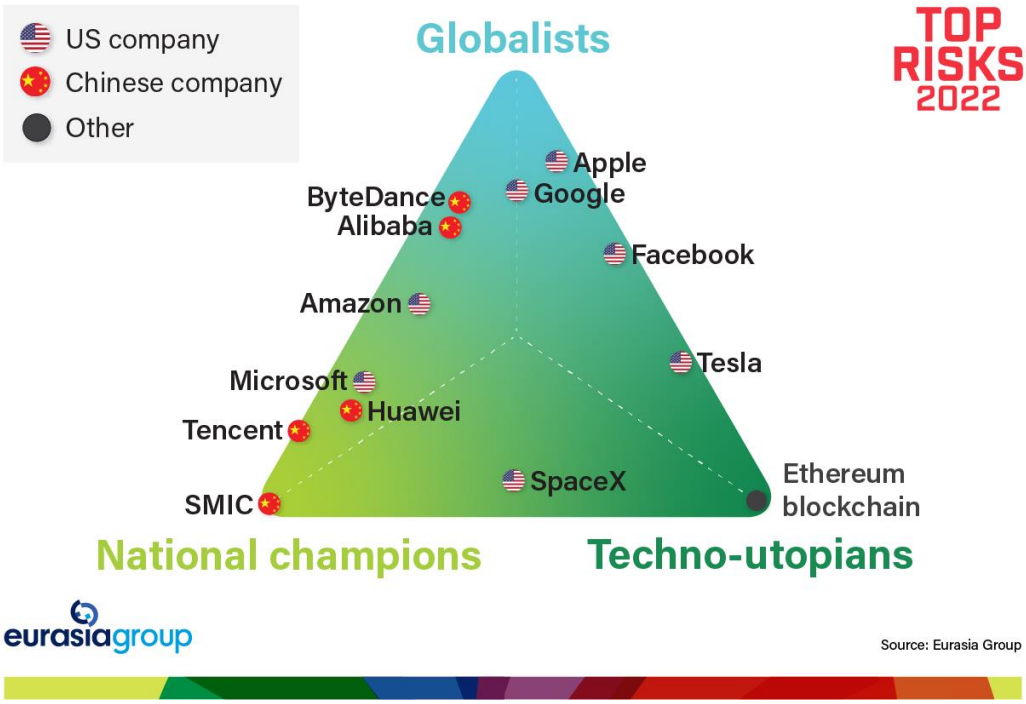
With regards to the DSA, the imposition of measures over Very Large Online Platforms[10] features how the EU is touching the behavior of these companies, which mostly come from China and U.S. jurisdictions[11]. The goal is three-fold: protect rights (citizens' rights from increased risks and harms), guarantee security (through content moderation to avoid harmful messages, or to cause damages), and foster a competitive economy (removing barriers for trade in digital services and protecting SMEs, which are the bulk of companies at the EU). As for the DMA, the main aspect on digital sovereignty was how to reduce market concentration and ensure fairness in business practices.

However, the main challenge for the EU to deploy this regulatory tool as a geopolitical asset relies on whether the EU will get to influence other countries to follow the same approach. It is not only about imposing certain rules to those that already do interact with the EU, but about encouraging others to do the same with their owns. This might explain why the EU launched in 2022 a new Tech Office in San Francisco with a Senior EU Envoy for Digital to the U.S., whose portfolio aims to create public acceptance of this regulation as a positive tool for international collaboration.

Similarly, another challenge for the geopolitical instrumentalization of these regulations is to understand that **geopolitical strategies should vary depending on the country and type of technology company**, as firms may have different geopolitical approaches.

[10] European Commission (2023). *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*. Accessible at https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413.
[11] Freihse, C., Overdiek, M. (2022). Digital Services Act and Digital Markets Act: Towards European Digital Sovereignty? *GED*. Accessible at https://globaleurope.eu/europes-future/digital-services-act-and-digital-markets-act-towards-european-digital-sovereignty/.

Figure 2. Three types of global technology companies, by attitude



Source: Eurasia Group (2022)[12]. Top Risks 2022.

The way of addressing the geopolitics of technology in general, and of data in particular, is not only about the governmental rivalry between China and the United States. It is also about each technology company, as companies coming from the U.S. see the world through different lens. This is why the Eurasia Group divides firms in three main types:

- **Globalists**. Firms that built their power by operating on an international scale, settling down across countries and competing intensively. This is the case of Apple, Facebook, and Google, whose services go beyond national borders and outside from physical territory. They aimed to dominate a specific market niche and to extend it globally. Alibaba, ByteDance, and Tencent followed the same pattern, first dominating the Chinese market, second expanding it worldwide.

- **National champions**. Some globalists were -and are- national champions that first grew at the national level. What differs is that the category of "national champions" refer to those companies that are more willing to align themselves explicitly with the priorities of their home governments. These firms are partnering with governments in various important critical technology domains. Main cases come from China, such as Huawei and SMIC. In the U.S., globalist companies emerged after being national champions, such as Amazon and Microsoft, which compete to provide cloud-computing infrastructure to the U.S. government.

[12] Eurasia Group (2022). Top Risks 2022. Accessible at https://www.eurasiagroup.net/live-post/top-risks-2022-2-technopolar-world.

- **Techno-utopians**. These firms see technology not just as a global business opportunity but also as a potentially revolutionary force in human affairs, beyond the nation-state paradigm. This type tends to center on the personalities and ambitions of technology CEOs rather than the operations of the companies themselves. This might be the case of Tesla and SpaceX.

Still, there are **divided opinions on whether technology firms are or not geopolitical actors**. Some experts argue that they play a major role[13] in geopolitics because they are creating new topics to be dealt at the highest levels of decision-making, and they are receiving attention from governments (either positively or by imposing regulations on them). Others argue that they cannot be categorized[14] as geopolitical actors because the international order is still largely marked by physical challenges, such as refugee flows, drought and war.

In any case, EU's regulation over markets and competition has had an important effect on the way technology firms act in EU territory.

1.1.3. Data Act

The Data Act is perceived as the opportunity for the manufacturing industry. Platforms generate data, but Data Act is aimed at the usage of this data by the manufacturing sector. It is a horizontal legislation, so it affects all sectors.

While it may be seen only as a single market-oriented regulation, the reality is that it aims to influence the way the EU harness its strategic autonomy or digital sovereignty with third countries and actors.

Two critical points exist on this matter. First, with regards to Intellectual Property, as the European Commission's definition in their first proposal left an open definition, the European Parliament had to refine the definition. Since the definition of **"trade secret"** cannot be changed because it is closed, the Parliament decided to focus on the definition of "data" (this is, the scope of what is included and what is not). While raw data will always fall under the obligations of the regulation, it has to be readable to avoid a lack of usability and misinterpretation of the data received. On the other hand, data which are the function of (sophisticated) processing will be excluded in order not to hamper previous investment and respect IP rights and trade secrets.

Second, defense-related data has been excluded because it raised concerns over the potential weaponization of the Data Act by certain companies from third countries. Airbus has been excluded from the Data Act as it handles with sensitive information from the defense sector.

In both cases, a geopolitical risk that the Data Act aims to prevent from is that companies from third countries complying with the regulation might use economic security policies to enter into the European market with less guardrails. In this line, it will remain important

[13] Bremmer, I. (2021). The technopolar moment: How digital powers will reshape the global order. *Foreign Aff.*, *100*, 112.
[14] Walt, S. (2021). Big tech won't remake the global order. *Foreign Policy*, *8*.

to make sure that the Data Act is effectively aligned with the export control regimes currently agreed at the EU level. However, more than this, it will be paramount to guarantee that the interpretation and implementation of those export control standards by Member States -which are the final policy shapers of this regime- are carried out in a harmonized, transparent, and comprehensive manner to prevent risks. These export control regimes should tackle high-technology services and sensitive data that is shared.

Similarly, the EU should carry out a risk assessment on the weaponization of data to affect EU's priorities, interests and vision based on the three primary streams of data that are available for harvesting: user-generated content, information purchased from Original Data Suppliers (ODS), and third-party data services from intermediaries[15].

1.1.4. Data Governance Act (DGA) and European Data Spaces

The DGA aims to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data. The main output of the DGA is the development of common European data spaces in strategic domains, such as public administration, health, environment, energy, agriculture, mobility, finance, manufacturing and skills.

The main vision of the European data spaces is to create the idea of "sovereign data ecosystems", governed by a cross-sector common infrastructure of cloud, data, and AI. It relies on federated communities, the value of trust (transparency and compliance across all spaces), innovation, and the generation of economic competitiveness. The final goal of creating a federated community and fostering trust is to contribute to the EU's role of strategic autonomy.

1.1.5. International data transfers: the case of the EU-US transatlantic framework

After the blockade of the Privacy Shield in July 2020 by the Court of Justice of the European Union due to EU's concerns over the misapplication of the transatlantic data flows framework by the United States, in 2022 the two sides announced that they had reached an agreement on a new EU-U.S. Data Privacy Framework. With President Biden's Executive Order from October 2022 on 'Enhancing Safeguards for United States Signals Intelligence Activities', the introduction of new binding safeguards to address all the points raised by the EU Court of Justice, limiting access to EU data by U.S. intelligence services and establishing a Data Protection Review Court, the European Commission is preparing a draft adequacy decision to be adopted soon[16].

However, regulation is not the single approach that the EU should take in the geopolitics of data. To do so, two other approaches are as important as strategic: the role of multilateral initiatives, "coalitions of the willing" and international meetings; and the importance of technology diplomacy as a policy area to institutionalize the geopolitics of data, alongside other technological challenges.

[15] Capri, A. (2022). Geopolitics and the race for data supremacy. *Hinrich Foundation*. Accessible at https://www.hinrichfoundation.com/research/wp/tech/geopolitics-and-data-supremacy/.
[16] European Commission (2022). *Questions & Answers: EU-U.S. Data Privacy Framework*. Accessed on May 24, 2023. Accessible at https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045.

1.2. The role of multilateral initiatives and "coalitions of the willing"

The exposure to threats and opportunities in the weaponization of data cannot be only addressed through the lens of regulation. This is why countries are increasingly moving up their proposals on data to the level of multilateral meetings.

These meetings may be divided in two types: institutionalized organizations and spaces with long-lasting history, and *ad hoc*, recent coalitions which are aimed at pushing forward specific, tailored topics, at specific speeds, and through expected deliverables.

On the first group, the most prominent ones are the G7 - the informal grouping of seven of the world's advanced economies, including Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States, as well as the European Union, which participates but has no vote capacity -, the United Nations -which is hosting the Special Envoy on Technology and the implementation of the Roadmap on Digital Cooperation as well as the UN Global Digital Compact -, the OECD -which devotes initiatives to data policy, such as the Declaration on Trusted Government Access to Data[17], and also to Artificial Intelligence, such as OECD.AI and the Global Partnership on AI -, and regional organizations such as the African Union, ASEAN -with its Digital Masterplan- and regional development banks that are arranging discussions over data policies and the importance of multilateral collaboration.

On the second group, countries are inching toward creating alliances with like-minded countries on a bilateral or multilateral basis. Most prominent examples are the Quadrilateral Security Dialogue or Quad -U.S., Australia, India and Japan-, which leverage the collaboration on data to activities[18] such as maritime security (for example, by providing near-real-time, integrated maritime domain data to maritime agencies in Southeast Asia and the Pacific), Earth Observation data (to ensure peaceful, safe and sustainable use of outer space), or data analysis to map threats to supply chain disruptions or resilience in critical technologies.
It is also the case of the Digital Economy Partnership Agreement or DEPA -composed of Chile, New Zealand, and Singapore to tackle digital trade challenges. China aimed to join DEPA in the past in this strategic partnership based on partnerships between Latin America, Southeast Asia and Oceanic.

Other initiatives have been launched – D-10[19], Tech-10[20], T-12[21] -, but with limited success, complete failure, or ineffectiveness[22] due to expectations mismatch, lack of

[17] OECD (2022). Declaration on Government Access to Personal Data Held by Private Sector Entities. Accessible at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.
[18] White House (2023). *Quad Leaders' Joint Statement.* May 20, 2023. Accessible at https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-joint-statement/.
[19] Brattberg, E., Judah, B. (2020). Forget the G-7, Build the D-10. *Foreign Policy.* Accessible at https://foreignpolicy.com/2020/06/10/g7-d10-democracy-trump-europe/.
[20] Manuel, A. (2020). The Tech 10: A Flexible Approach for International Technology Governance. Accessible at http://anjamanuel.com/new-page-40.
[21] Cohen, J., Fontaine, R. (2020). Uniting the Techno-Democracies: How to Build Digital Cooperation. *Foreign Affairs* (November/December 2020). Accessible at https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies.
[22] Rasser, M., Arceasti, R. Oya, S., Riikonen, A., Bochert, M. (2020). Common Code: An Alliance Framework for Democratic Technology Policy. *Center for A New American Security.* Accessible at https://www.cnas.org/publications/reports/common-code.

delivery, or too simple low-hanging fruits that did not provides the needed incentives for actors to keep collaborating.

In all cases, data has been addressed through several lens: data privacy, cross-border flows of industrial, non-personal data (which impinges on the core of critical infrastructure, critical technologies, and economic security instruments such as export controls and Foreign Direct Investment), how to foster R&D and joint consortiums across countries with sensitive or critical data, or the impact of data usage on fundamental rights.

In the case of the EU, the Union has participated in several initiatives, particularly the G7 and G20. Some initiatives have been particularly critical for the geopolitics of data. In 2019, the then-Prime Minister Abe Shinzo from Japan proposed, during its Presidency of the G20, the Data Free Flows with Trust (DFFT) approach to guarantee the enhancement of cross-border data flows, based on the combination of privacy and security of personal and sensitive data. As the data governance approach is getting balkanized by blocs which propose different, if not contrasting, data models -see China's state-controlled model, the EU's regulation focus, and the U.S. liberal approach-, Japan decided to pursue a new proposal based on an interoperable global governance of the data, that ensures the promotion of free data to foster economic growth as well as the protection of individual privacy, national security, and Intellectual Property rights through trusted regulations.

Since the Declaration supporting the DFFT model in 2019, Japan has advanced the concept in several ways[23], also with the support from the European Union. For example, in April 2021, the G7 launched a Roadmap for Cooperation on DFFT[24] which focuses on four streams: data localization, regulatory cooperation, government access to data, and data sharing for priority sectors. This roadmap was translated into an Action Plan[25] to promote the DFFT. The implementation has been also materialized in bilateral agreements, such as the Japan-U.S. Digital Trade Agreement, the Japan-UK Comprehensive Economic Partnership Agreement, and the EU-Japan Digital Partnership Agreement.

While cooperation with U.S., UK, EU, Canada and like-minded countries is straightforward, the main challenge lies in how to agree on policies to counter the proliferation of data localization policies with those countries where Japan would aim to partner with, but have different opinions on this issue. A paradigmatic case is India, which is part of the G20 and, during the preparation of the declaration supporting the DFFT in 2019, was against this statement. India argued that the DFFT approach was not comprehensive enough in the legislation of its country, and could lead to inequalities across developing and developed countries. However, it is important to note that India is

[23] Arasasingham, A., Goodman, M. (2023). Operationalizing Data Free Flow with Trust (DFFT). *CSIS*. Accessible at https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft.
[24] G7 Roadmap for Cooperation on Data Free Flow with Trust (2021). Accessible at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986160/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf.
[25] G7 Action Plan for Promoting Data Free Flow with Trust (2022). Accessible at https://bmdv.bund.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-final-declaration-annex-1.pdf?__blob=publicationFile.

one of the countries that has invested much more efforts in data localization policies worldwide, what explains its opposition to the DFFT model.

This is why the EU has an opportunity[26] to partner with Japan and engage closely with the Indo-Pacific region. Japan is gaining traction in *ad hoc* coalitions –from the Quad to Blue Dot Network– and has also been proactive in pursuing technology principles as well as leading relevant ecosystems –such as GPAI, Osaka Track and the PQII–. At the same time, the country also relies on traditional multilateral settings as it aims to seize leadership in Asia by means of regional cooperation and on some previous attempts to reach out to African governments jointly with India. However, Japan's approach to technology competition is cautious: it does not intend to become confrontational with China. This places it in an inter-theatre position where it has opportunities to cooperate with the EU to project a democracy-affirming technology governance at the multilateral level without renouncing to cooperation with China when deemed appropriate.

1.3. The building-up of EU's technology diplomacy

The European Union has been developing its foreign policy on technology since several years. It has done it in three main forms. First, by strengthening the number and scope of technical assistance projects in third countries -mostly through the Directorate General of International Partnerships, which was before the development cooperation branch of the European Commission. Second, by launching a number of regional initiatives with specific partners, focused on digitalization. Third, by setting up the first-ever framework on Digital Diplomacy in July 2022. The two latter are analyzed.

1.3.1. Regional initiatives for technology partnerships

Alongside the Digital Partnership Agreement with Japan, the EU has established a number of regional initiatives with third countries and regions where data is a key focus of the discussion:

- **EU-U.S. Trade and Technology Council**, which serves as a "forum for the European Union and the United States to coordinate approaches to key global trade, economic, and technology issues and to deepen transatlantic trade and economic relations based on shared democratic values".

The TTC has ten Working Groups, out of which one is devoted to data governance and platforms, and others address technology standards cooperation, where data is approached to create joint roadmaps on evaluation and measurements tools to create trustworthy Artificial Intelligence. Also, data is approached by the Working Group on ICT security and competitiveness, which decides on how to address security risks from high-risk vendors and suppliers. Likewise, the Working Group on "Misuse of Technology Threatening Security and Human Rights" has four main areas of work: (1) combatting arbitrary or unlawful surveillance; (2) protecting human rights defenders online; (3)

[26] Jorge Ricart, R. (2022). The EU and Japan: forging joint opportunities for global technology governance beyond great power rivalry. *Elcano Royal Institute*. Accessible at https://www.realinstitutoelcano.org/en/analyses/the-eu-and-japan-forging-joint-opportunities-for-global-technology-governance-beyond-great-power-rivalry/.

technical and diplomatic coordination to Internet shutdowns; (4) identification of state-sponsored information manipulation and interference. Their cooperation goals refer to info-sharing, joint mapping of risks and support with techniques to identify vulnerabilities, by leveraging data.

Additionally, in December 2022 the TTC agreed on joint infrastructure and connectivity projects globally, concretely in Jamaica (connecting to the Internet 1000 public schools and children's homes) and in Kenya (expanding Internet access for schools), which will leverage the EU and U.S. approach to data flows and governance in third countries.

- **EU-India Trade and Technology Council**, which aims to establish India as a strategic partner after several years of blockade of their diplomatic relationships. This is framed in the revamped negotiation over a bilateral Free Trade Agreement. Out of the three working groups, one is devoted to strategic technologies, digital governance and digital connectivity, where both sides aim to discuss about the role of data for Digital Public Infrastructures and some industrial data spaces -but no discussions on data localizations have been set up so far, due to differences on this vision.

- **Digital Partnership Agreements (DPAs) with Japan, Republic of Korea, and Singapore.**

As the Japan's DPA has been explained, the main goal of the DPA with Korea is to guide the governance of data through the values of freedom and human rights, as well as to ensure solidarity for the freedom of digital citizens in their use of data to protect rights. The DPA with Singapore does not focus on rights, but rather on the leverage of data for digital trade, 5G and 6G, online platforms, SMEs digital transformation, fintech, digital skills and standards.

- **Digital Agenda for Western Balkans**

Out of the four areas of work, three are devoted to data: investing in broadband connectivity and its roll-out; strengthening the digital economy and society through the deployment of open data and digitalization of the public administration and procurement processes; and boosting research and innovation by promoting data usage for R&D.

- **Eastern Partnership's EU4Digital Initiative**

Main areas of data governance are the development of regulatory convergence in telecom rules, trust and security, eHealth and eSkills. Central to the EU4Digital Initiative is the three-year EU-funded EU4Digital Facility (2019-2022), or EU4Digital Facility, which promotes key areas of the digital economy and society, in line with EU norms and practices, and communicates EU support across the digital agenda in the region.

- **Joint Commitment to Digital Transformation in the EU-Africa Joint Vision for 2030**

This partnership aims to provide a win-win approach and agreed tangible outcomes, which includes an Africa-Europe Investment Package of at least EUR 150 billion that will support their common ambition for 2030 and AU Agenda 2063, enhancing digital infrastructure and facilitating digital transformation.

Also, the **EU-Nigeria Digital Economy** Package, under the Global Gateway initiative, is planned to invest at least €820 million in Nigeria's digital transformation. With a combination of €160 million in grants and €660 million in loans, the EU aims to comprehensively support Nigeria's digitalization strategy.

- **EU-Latin America and Caribbean Digital Alliance**

Launched in March 2023, it aims to be a platform for an institutionalized dialogue at both the political and working levels on digital challenges and opportunities for both regions. The four areas of work align with the leverage of data as a geopolitical tool of cooperation: regulatory and policy cooperation, extension of connectivity infrastructures, innovation and private sector cooperation, and digitally-enabled products and e-services. However, still it remains to be seen how this alliance will be translated into specific outcomes, as LAC countries have strong differences on the political willingness and approach to deal with the UE in digital issues. Likewise, no political declaration was made during the launch day of the alliance. Additionally, the Digital for Development (D4D) Hub that accompanies this Alliance will need to deliver further publicly available outcomes, such as monitoring of needs and the actual implementation of actions.

- **Global Gateway**

This infrastructure investment initiative led by the EU, which aims to accompany the Build Back Better World (B3W) by the U.S. and be an alternative to the Chinese Belt and Road Initiative, ranks digitalization as its first priority out of five.

There are six references to specific data-oriented initiatives. These are the deployment of digital networks and cloud and data infrastructures with partner countries, the promotion of green data centers, the deployment of underwater cables equipped with ocean monitoring sensors, the offering of digital economy packages that combine infrastructure investments with country-level assistance on ensuring the protection of personal data, and international cooperation on data protection under the EU-LAC Digital Alliance.

1.3.2. The first-ever framework on Digital Diplomacy

Technology and digital policy have been long addressed as an economic issue. In 2019, the EU started to look at technology through the lens of "ethics" -see the High-Level Expert Group on AI Ethics-, and as a political and geopolitical issue. This explains why the DG INTPA's Unit on Science, Technology, Innovation and Digitalization was pushed forward in early 2020, although it mainly focuses on technical assistance projects. No strong political decisions have been made at the highest level of decision-making, and human rights have been limitedly included in the political and policy discussion.

The EU Council Conclusions on digital diplomacy from July 2022[27] is the landmark, the starting point, for the EU to 'institutionalize' all things related to the external agenda in third countries on digital policy as a single line of foreign policy by the EU. The wording

[27] European Union Council (2022). *Council Conclusions on EU Digital Diplomacy*. Accessible at https://data.consilium.europa.eu/doc/document/ST-11406-2022-INIT/en/pdf.

'digital diplomacy' aims to put all scattered initiatives that had been done so far into the same box.

Digital policy is no longer only a domestic issue. It is also part of the foreign policy agenda. It is not about digitalizing the diplomatic communications or protecting the information that flows through diplomatic corps. It is about identifying how a country aims to protect, promote and guarantee their vision about the world, about the international order, and how to govern technology to do so.

In the specific case of data geopolitics, the EU Council Conclusions address the geopolitics of data in several aspects.

- First, how to address the role of "trust" in data governance with third countries.
- Second, how to support European businesses' global reach and promote European examples of ethical approaches to data usage, since responsible use of data by businesses and governments forms the basis for the development of trustworthy and responsible digital ecosystems.
- Third, how to improve the EU's capability to monitor global digital regulatory activity, international data flows and the data privacy of EU citizens, patterns of digital trade, partnerships between third countries and their effects on the competition framework in the global market for digital technologies and services.
- Fourth, the leverage of datasets for EU outer space goals and security and defense.
- Fifth, how to commit relevant instruments and funding to combat Internet shutdowns, arbitrary or indiscriminate digital surveillance and data retention alongside a concerted policy to promote human rights online e.g. through Human Rights dialogues, to protect human rights defenders and civil society online and expand civic space.
- Sixth, how promote digitalization and data sharing in favor of sustainability and the SDGs in governments and the private sector.

Still, to govern the geopolitics of data, it would be recommended that the EU adds up new activities much more oriented to restrictive measures and punishment initiatives. For example, how to condemn, sanction or apply conditionality requisites when the EU partners with a third country that violates certain principles, rules or rights that are on the top priority of the Union. Likewise, there should be further lines of action on mapping of risks derived from the cooperation with certain third countries. Also, digital diplomacy might tackle whether or not EU call for tenders' criteria should be stricter when it comes down to public procurement and risk assessment, mostly from those companies that store, collect and capture data that might be sensitive if transferred to a third country.

Alongside this challenge on the scope of ambition -which may increase over time-, there are three additional challenges.

First, **how to address the role of EU member states in the geopolitics of data**. Most foreign and security policy mandates depend on the unanimous support by all 27 countries at the EU Council. This might difficult how certain data governance activities might be approved. Also, member states tend to address international governance over data through the lens of purely regulatory issues -or economic issues-, but limitedly in terms of security and foreign policy. Likewise, member states largely differ in four areas when it comes down to how to interact in the geopolitics of data:

(1) political willingness (to include data as a new line of their foreign policy);

(2) situational awareness (about the importance of data in human rights and security);

(3) they have limitedly evaluated and addressed the risks of data on rights. This topic has not been included in National Action Plans on Business and Human Rights. Also, the EU Declaration on Digital Rights and Principles[28] is positive that was launched in 2022 is a positive effort, although it still requires to be mandatory and more influential across countries;

(4) Currently it would be difficult to find complementarity and coherence across EU member states' external tech policy initiatives. Most of the work led by the (few) existing tech ambassadors in EU territory do focus on business, R&D and entrepreneurship. The lens of security and rights is far limited if compared to economy.

Second, a key challenge for the EU is how to partner with developing countries or, particularly, digitally non-aligned countries[29]. While there is still no movement similar to the formation of the Non-Aligned Movement in 1961, which was the product of not wanting to enter into geopolitical affiliations at a time of great powers rivalry, there are some dynamics that are pointing out to certain countries that might have the incentives to relook at traditional notions of non-alignment. This issue is still largely uncovered, but should be an area to delve into.

Three, all digital diplomacy branches should pay attention to certain technologies that are still underdeveloped, not too marketized or not in place, but that could generate major competition across countries. For example, a Chinese state-owned think tank flagged national security risks of metaverse[30], considering potential political and social issues. Metaverse will be fed by data, both personal and non-personal, from a large array of sectors ranging from healthcare and education to political advertising and retail.

[28] European Commission (2022). European Declaration on Digital Rights and Principles. Accessible at https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles#:~:text=The%20Declaration%20on%20Digital%20Rights%20and%20Principles%20presents%20the%20EU's,version%20of%20the%20Declaration%20available.
[29] Reddy, L., Soni, A. (2021). Is There Space for a Digital Non-Aligned Movement? *Cyberstability Paper: Series New Conditions and Constellations in Cyber*. Accessible at https://hcss.nl/wp-content/uploads/2021/09/Is-There-Space-for-a-Digital-Non-Aligned-Movement.pdf.
[30] China Institute of Contemporary International Relations (2021). *The Metaverse and National Security*. CICIR.

2. Conclusion

Data is one of the most valuable resources in today's global competition – but it is not yet seen as a global common that leads to collaboration. So far, global data flows are still governed through a maze of multilateral, bilateral, unilateral, and *ad hoc* rules, principles, and voluntary frameworks that are not always accepted or applied by all actors. Cross-border international collaboration on this issue is far limited, with ups and downs in the success of a common global agenda on data governance.

The European Union is developing an increasing package to address the governance of data globally speaking. To do so effectively, it will need to face a number of challenges - from the perspectives of security, economy, and rights- that are not always framed under the existing policies. New scope, intensities, stakeholders' engagement and a higher level of ambition and monitoring will be the drivers to make the EU's leverage of its Data Strategy worldwide successfully with partners.