INSTITUT Montaigne

institutmontaigne.org/en
NAC2304-03

POLICY PAPER - April 2023

Cross-Border Data Flows: The Choices for Europe

1. Introduction

More or less everything we do today is governed by cross-border data flows. So long as nation-states exist, they will face a dilemma between protecting data from other state actors – or cyberhackers – and profiting from free data flows. **Choices must be made between the guarantees that sovereignty is meant to offer, and the tangible benefits provided by international data exchange**.

However, there are **obstacles to creating truly multilateral data regimes** due to issues of trust, verification, legal arbitration and systemic differences. While this policy paper does not disregard the possibilities remaining open for truly multilateral data regimes, it will take as a starting point that for all practical purposes, the digital world has already fragmented. We must therefore look for second-best solutions to a seamless digital space with universally accepted rules.

2. Defining the issue

Not all nations are equal. The trade-off between data sovereignty and free flow efficiency varies greatly depending on **a country's level of digital proficiency**.

- **The United States leads the digital field globally**, with its large companies giving it a de facto digital sovereignty over cross-border data flows.
- **Nations in intermediary positions** include huge digital markets (India), particularly competent nations (Israel or Estonia), and authoritarian nations that prioritize data control and access by authorities over any other consideration (China) – China and India are addressed as case studies in this policy paper. The combination of China's level of digital achievement and across-the-board move for control, including on all companies, is unique and on the rise.
- **Smaller or less advanced nations** have little choice but to accept the supremacy of foreign providers, often at the cost of their data sovereignty. Yet they retain the option of gravitating between what is an American-led tech framework and an authoritarian model provided chiefly by China.

Is European digital sovereignty therefore realistic? Europe remains a digital industry dwarf and underdog competitor for innovation and start-ups, but it has a more rationally organized market; and the "Brussels effect" ensures some influence for European personal data regulation beyond its borders. However, digital infrastructure and market dominance by firms matter.

Choosing between data sovereignty and free flow efficiency intersects a third issue: **digital privacy** against commercial harvesting or state surveillance, for which rules and effective enforcement are required. Regarding commercial harvesting, the American and European approaches differ on the issue of consent: notice-and-choice versus express user consent. For surveillance, the contrast is often made between democracies and authoritarian systems. **This opposition is neither absolute nor simple**. While authoritarian states are unlikely to safeguard their citizens from state surveillance, the level of personal data protection provided by democracies can vary greatly.

Economic interest also shapes the emphasis on sovereignty. A number of US firms have a first mover advantage and a deep venture capital market. Europe struggles with a more dispersed industry, a difficulty for new entrants to match the economies of scale of entrenched competitors, and less effective policies to steer innovation. This situation may push the creation of an "industrial cocoon" to nurture an indigenous ecosystem. This is easier said than done.

Policies for cross-border data flows therefore face two fundamental dilemmas: one is the **triangle between the goals of efficiency, privacy, and security**; the other is both **geopolitical and geoeconomic, with the US, the European Union, and China** seeking to control their own data while accessing the data of others. These dilemmas cannot be fully resolved but only arbitrated.

3. Regulating cross-border data flows

Regulating data flows – including cross-border transfers – does not mean hindering or preventing them. On the contrary, it is a condition for their development. Indeed, regulation ensures that several goals are met: privacy and trust for individuals and companies, meeting public requirements such as national security and public order, and prevention of crime.

The challenge lies in **arbitrating between different legal systems and enforcing the choices that are made**. To address this issue, various collective arrangements have emerged over time, including non-binding recommendations from the OECD, the legally binding Convention 108 of the Council of Europe, and regional initiatives like APEC and ASEAN. Much more significant is **the adoption of the General Data Protection Regulation (GDPR) of the European Union**. It includes provisions for data transfer outside the EU, such as adequacy decisions, standard contractual clauses, and binding corporate rules, as well as a list of derogations.

Beyond these initiatives, which come closest to multilateral arrangements, **a fully multilateral approach currently remains out of reach**. We see initiatives by various organizations such as the UN, the WTO, and the World Bank. Increasingly, recent FTAs include (sometimes binding) provisions on digital transfers. Chile, New Zealand and Singapore have started a pragmatic but non-binding Digital Economy Partnership Agreement (DEPA) that is proving attractive to others.

The other push for better regulation takes place at the G7 and G20 levels, and it is largely driven by Japan's government. Through **its Data Free Flow with Trust (DFFT)** initiative, Japan is attempting to bridge the gap between an idealistic universal regime that ensures a seamless digital world and the practical reality of a plurilateral regime as the only option to move ahead in the short term.

In contrast, the US seeks **bilateral agreements** on data transfer and is likely to become the center of a "hub-and-spoke" model of direct access mechanisms.

4. Digital Sovereignty

The exponential growth of the digital revolution has benefited the US and China, with respective dominance in soft and hard components. Europe may be a world leader in creating influential digital regulation, but **"referees do not win matches"**. The European data market remains smaller in relative size per inhabitant than the American or Japanese ones. The European Commission, after some Member States, seeks to address this gap by aiming for digital sovereignty. After all, **who would not wish to "take back control"**?

We must therefore clarify what is meant by sovereignty in the digital area. Whereas sovereignty was a taboo term in the EU, it is constantly referred to at the Commission level and in Member State pronouncements. Overall, Europeans mostly view **sovereignty as a means for autonomy** without sacrificing interdependence or free data flows, and not as complete self-reliance such as China's Great Firewall. Independence is a commendable path, but also one that is unrealistic. Moreover, the European approach to digital sovereignty is largely limited to defensive options, contrary to the American one with both **defensive and offensive features**.

Many politicians have jumped on the sovereignty bandwagon, with a plurality of motives. In Europe, the sovereignist advocacy on digital issues has moved from the national to the European level, as no Member State alone has the necessary scale for investment, innovation, and market. **Pooling at the European level** is in many cases a prerequisite for effectiveness. But the very strength of European commitments to values such as data privacy and personal rights has another consequence: **legal hurdles for reforms** accelerating innovation and scaling up the digital sector are larger than anywhere else. And our **own reluctance towards data-sharing**, based on precautionary principles, is also a problem that needs to be addressed.

We need to have an accurate understanding of the disadvantages of our own limits. The lack of European digital champions, its present dependence on non-European technology and software providers, and the dispersion of private actors are true impediments. Public decision-makers must keep moving to facilitate a bottom-up mobilization of resources. **An overall change in European mentalities** should thus prioritize science and technology-based developments over a defensive approach driven by mistrust and a recurring preference for the precautionary principle.

5. Clouds and infrastructures

In terms of priority for data security, one might have thought that undersea cables and nodes would come out on top. Yet, they are merely the object of a strenuous but silent economic and political competition between the US and China, with the balance shifting from Chinese actors to American companies. In addition, **dependencies in hardware supply chains for IoT create risks of data extraction or remote sabotage**.

But these competitions pale in comparison to the public debates over cloud service operators and supply chain, with concerns over data security and control. Clouds may be located in another country, or cloud suppliers, operators and apps may be from another country with different jurisdictions. This makes it **difficult for users to maintain control over their data and its possible onward uses**.

The dominance of US cloud providers in the European internal market has led to discussions on self-sufficiency and independence from foreign suppliers for clouds, both at the Member State and European levels. The issue has initially been framed

by many as one of cloud localization – as if having a cloud on "our" territory ensured its cyber and legal security. But clouds are no longer just data containers, physical infrastructures resembling bank vaults.

France and Germany's attempts at sovereign clouds have faced challenges. While private clouds for governments have been successful, creating commercially viable solutions without established cloud companies is difficult. So far, it seems to be **impossible to build a competitive cloud without tapping into American technology**.

Questions remain about the extraterritorial reach of the CLOUD Act and other legislation. France has renewed efforts to create clouds with varying degrees of sovereignty, and to push both at the French and European levels for cloud certification schemes. Yet, **debates on immunity from extraterritorial laws continue** as all companies rely to some degree on US-based technology providers, and some on Chinese suppliers also. The debate is mirrored at the supra-national level, where the inclusion of non-EU industry members became controversial for Gaia-X, which was trying to develop a reliable European digital infrastructure and an ecosystem for innovation.

The road to European clouds is important from a security and economic perspective, but it should be gradual and predictable. In the short term, **a decisive competition policy is key to limiting the rentier advantages of first movers**. In the medium and long terms, a competition policy must be coupled with a well-defined public purchase policy for more results.

6. Keeping the digital transatlantic space open

In the end, **making rules for the international digital space boils down to choosing whom you want to consort with and to what extent**. On data flows, advocating radical stands and requiring not so much adequacy but identical rules and norms, would preclude exchange. Keeping open the transatlantic digital space requires concessions on both sides.

There are good reasons for Europe to seek innovation and supply chains in the digital sector, not at the expense of efficiency, scalability and cost though. Even in the most restricted and sensitive digital space, it is going to be difficult not to rely on some non-EU suppliers, especially when domestic alternatives are still developing.

The EU should seek common ground with the US. That implies restraining localization subsidies on both sides, accepting mixed solutions, and a strong competition policy in Europe – and in the US – to succeed in creating a more level-playing field. **This is a competition, finance and innovation issue, not a strategic divide**. In contrast, fragmentation on grounds of self-sufficiency would isolate Europe, including from many third markets and parties, and create fertile ground for unhelpful political strife.

7. Conclusion and Recommendations

Europe faces both a threat and a challenge on cross-border data flows. The threat is clearly from China, and derives from the combination of forward digital footprint and total lack of accountability for its own data management. The challenge is the US advantage as first mover, largest R&D and capacity investor with a stellar ability to combine public and private actors. With this two-front environment in mind, this note provides a list of recommendations for Europe:

1) Moving towards a **more effective common European data space** is a crucial first step, which can only be **achieved through a realistic sequencing of priorities**. The EU has no competence

on national security issues. In the short term, it should target the next level of critical data for European cloud solutions, and leverage its competition policy to create a level-playing field.

2) The EU needs to **increase public and private financial resources beyond the traditional Commission support to innovation mechanisms** to create more synergy with industry.

3) The EU should **adopt a pragmatic and inclusive approach in the design of funding and employment policies** to attract start-ups, research centers, foreign firms and talent.

4) **Europe's market power and regulating ability go a long way to achieve more data security** without pursuing radical self-sufficiency, or "going Chinese".

5) The EU must **contain regulatory requirements and avoid promulgating broad and sweeping rules** that are either overextended or unrealistic. The risk is that less demanding standards such as DEPA prevail outside Europe.

6) No full convergence on democracy, values, and local rules between systems exists. Despite the difficulties encountered through the years, **compromise for a renewed transatlantic cross-border agreement** is strategically necessary.

7) Regarding data localization, it is crucial to differentiate between cybersecurity and legal security. **Focusing on Europe's ability to deploy and enforce sanctions, including through extraterritorial leverage on data**, would put the EU in a better position to require consultation and joint decisions, including from the US.

8) While there are no absolute guarantees for data confidentiality and integrity, **data minimization and retention time limits can help reduce the risk of data breaches and energy consumption**.

9) Current liability laws can be reinforced. In the US, they are currently very limited, with little pre-defined penalties for insufficient action to prevent security leaks. This reduces the incentive for IT providers – hard, soft, platforms, CSOs – to invest in cybersecurity. **Increasing liability for providers could help narrow the transatlantic gap on data use**.

10) We must look beyond the transatlantic relationship and seek the right international format. Japan's proposals for their ongoing G7 presidency, which aim to be **inclusive but do not push for universality**, could be a promising avenue for coordinating international efforts.