
Cross-Border Data Flows: The Choices for Europe

POLICY PAPER - APRIL 2023




Institut Montaigne is a leading independent think tank based in Paris. Our pragmatic research and new ideas aim to help governments, industry and societies adapt to our complex world. Institut Montaigne's publications and events focus on major economic, societal, technological, environmental and geopolitical changes. We aim to serve the public interest through instructive analysis on French and European public policies and by providing an open and safe space for rigorous policy debates.

POLICY PAPER - April 2023

Cross-Border Data Flows: The Choices for Europe



Through our policy papers, we aim to provide practical recommendations to help senior politicians, public servants and industry leaders adapt and respond to today's challenges.



Europe is confronted with a threat and a challenge on cross-border data flows, within a fragmenting digital world. The threat is posed by authoritarian China, seeking to assert state-access to data while maintaining connection to global data flows. The challenge is posed by the digitally predominant US, whose market lead and first-mover advantages constrain the growth of European domestic challengers. In this context, debates around European digital sovereignty have gained ground, particularly as national and European policy-makers balance competing interests of free flow efficiency and protection of their data from other state actors. Multilateral efforts to regulate cross-border data flows have stumbled, facing questions of enforcement, mutual distrust, and systemic differences. From the EU's GDPR, to China's cybersecurity and data protection legislation and India's 'fence-sitting', to multi-state agreements such as DEPA, governments and other actors are increasingly opting for national or at best plurilateral solutions. With case studies of China and India as well as a focus on cloud and infrastructure issues, this policy paper takes stock of a rapidly evolving international context. From the analysis of the various facets of this debate and of existing arrangements, ten lessons for regulating cross-border data flows are drawn.

In all this, what should the EU do? The strength of its common market and renowned "Brussels effect" in exporting regulatory norms are unquestionable assets. But facing this threat and challenge, Europe must go further. The EU's steadfast commitment to data privacy sets it at odds with others, including the US, as well as challenges Europe's objective of maintaining mutual data access with international partners. As such it must step up its domestic capabilities with a common European digital space and mobilize greater funding for innovation. Skilled education, immigration, and competition policies, avoiding overregulation, adopting our own extraterritorial instruments are all more practical than a rush to tech sovereignty. Likewise – whether through transatlantic compromises or proposals such as that of Japan's Data Free Flow with Trust

now at the G7 – international cooperation is key. To guarantee open data flows while upholding data security and protection, policymakers must act now, with the risk otherwise of accelerating the fragmentation of the digital arena.

François Godement

François Godement is Institut Montaigne's Special Advisor and Resident Senior Fellow – Asia and America. He is also a Nonresident Senior Fellow of the Carnegie Endowment for International Peace in Washington, D.C., and an external consultant for the Policy Planning Staff of the French Ministry for Europe and Foreign Affairs. Until December 2018, he was the Director of ECFR's Asia & China Program and a Senior Policy Fellow at ECFR. A long-time professor at France's National Institute of Oriental Languages and Civilisations (INALCO) and Sciences Po, he created Centre Asie IFRI at the Paris-based Institut français des relations internationales (1985-2005), and Asia Centre (Paris) in 2005.

His last published books are *Les mots de Xi Jinping*, Dalloz, 2021 and *La Chine à nos portes – une stratégie pour l'Europe* (with Abigaël Vasselier), Odile Jacob, 2018. For Institut Montaigne, he recently authored, among others publications, the following policy papers: “*China's Change of Economic Model: Not So Fast!*” (June 2022), “*Rebooting Europe's China Strategy*” (May 2022, with Ian Bond, Hanns W. Maull and Volker Stanzel), “*Wins and Losses in the EU-China Investment Agreement (CAI)*” (January 2021), “*Europe's Pushback on China*” (June 2020), “*Digital Privacy, How Can We Win the Battle?*” (December 2019) and “*Europe and 5G: the Huawei Case*” (May 2019, with Mathieu Duchâtel).

Viviana Zhu

Viviana Zhu is a China analyst who closely follows EU-China relations and China's economic and digital developments. She was Research Fellow at Institut Montaigne's Asia Program until January 2023, and editor-in-chief of China Trends, the Institute's quarterly publication. She joined Institut Montaigne in January 2019 as Policy Officer for the Asia Program. Prior to that, she was Coordinator of the Asia Program of the European Council on Foreign Relations (ECFR). She holds a Master's degree in International Politics and a Bachelor's degree in Politics and Economics from the School of Oriental and African Studies (SOAS), University of London. For Institut Montaigne, Viviana Zhu authored "China's FinTech: the End of the Wild West" (April 2021), and co-authored "Fighting COVID-19: East Asian Responses to the Pandemic" (May 2020, with Mathieu Duchâtel and François Godement).

Abstract 5

Introduction 11

1 Defining the issue 14

1.1 Data sovereignty and free flow efficiency 14

1.2 Digital Privacy 19

1.3 Enforcement 22

1.4 The two triangles 25

1.5 Lessons 26

2 Regulating cross-border data flows 27

2.1 Existing arrangements and initiatives 28

2.2 Lessons 35

3 Digital sovereignty 36

3.1 The facets of the European sovereignty debate 38

3.2 Chasing the right degree of sovereignty 42

3.3 The single digital space versus national sovereignty dilemma 44

3.4 A science and technology based development approach 48

3.5 Lessons 51

4	China's pursuit of digital sovereignty	52
5	India, a major fence-sitter	64
6	Clouds and infrastructures	69
	6.1 The cloud issue is central	71
	6.2 Designing cloud sovereignty	75
	6.3 Clouds with varying degrees of sovereignty	80
	6.4 Lessons	83
7	Keeping the digital transatlantic space open	87
	Conclusion and Recommendations	93
	Acknowledgements	118

Being able to transfer data across borders is fundamental in this digital era for everything from social media use to international trade and cooperation on global health issues. Yet, without common principles and safeguards, the sharing of personal data across jurisdictions raises privacy concerns, particularly in sensitive areas like national security.

—Mathias Cormann, OECD secretary-general,
December 14, 2022¹

More or less everything we do today is governed by cross-border data flows: they are integral to our mode of production, economy and society. Yet the issue of data sovereignty, implying control and eventually curtailment of cross-border data flows, is fast becoming the digital equivalent of strategic autonomy or strategic sovereignty.

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. We know that trade in goods faces a choice between the law of comparative advantage and the potential gains to be had from mercantilism. In the digital world, the decision to exchange data among nations is based on the balance of benefits and costs. These include scaling and therefore growth, information gains against dependency and security risks.

Still, all systems can be more or less closed, more or less open. We increasingly see two different approaches to the way data is shared and stored: one has a focus on data sovereignty, and eventually data localization,

¹ OECD, “Landmark agreement adopted on safeguarding privacy in law enforcement and national security data access”, December 14, 2022, <https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm>

complemented by specific circumstances enabling the transfer of data; and the other advocating for a safe infrastructure and legal environment for free data flows, including guarantees for access by third parties. Of these two approaches, it is data sovereignty and security, sometimes mistakenly understood as data localization, that is a buzzword often appealing to public opinion and individuals as citizens. Yet the same individuals, as consumers, prioritize easy data flows and efficient access, whether inside or across borders. **Making the choices between high standards of data protection and facilitating cross-border data flows is therefore a public interest prerogative**, because these choices – starting from well-known consent requirements – are beyond the knowledge and psychological capacity of individuals. It is not in the commercial interest of companies to offer guarantees by design. In between the regulating state and the citizen/consumer, civil society groups (NGOs, think tanks) attempt to bridge the gap.

This policy paper does not disregard the possibilities remaining open for truly multilateral data regimes. But it will take as a starting point that for all practical purposes, the digital world has already fragmented – and is likely to continue to fragment increasingly as more and more emerging and developing nations access new technological capabilities. We therefore make no apology for looking at **second-best solutions to a seamless digital space with universally accepted rules**. These solutions involve answers to several questions:

1. Where does the need for **sovereign control over critical data stop**? Is this an issue of national security, public order, and protecting innovation? Some of the issues involved – such as intellectual property and cybertheft – are equally present for companies and inside domestic data markets.
2. Is **data and server localization** a security priority, including because of intelligence data collection for economic purposes, or also an issue of gaining a larger share of the data storage and treatment market?

As is the case with the semiconductor industry, how realistic is it to invest in competitors to the first movers? If a European rather than nationally-based cloud industry seems the only one likely to offer economies of scale, does it meet the national security requirements of Member States? How open can these layers be to third-party procurement, particularly concerning the cybersecurity of data storage and flows?

3. Should there be different layers of approach to **the security of digital clouds, according to their private or public use, to the criticality of the data and to the need for data treatment**?
4. How can we resolve, in the post-Snowden world, the contradiction between intelligence collection – which all states practice relative to their means – and guarantees for the protection of personal data and proprietary company data? Can we reach **a balance among states** with similar if not identical values – yet often with diverging interests – to limit data collection, ensure that there are limits to its overt use, and redress for identifiable harm resulting from illegal data collection? Should we even be trying?

1 Defining the issue

A few years back, data was seen as the new oil – a resource for leapfrogging in productivity and efficiency. Today, the focus is also on the privacy and security implications. Data can be combined into accurate description or modeling of an individual or of an event. This may be done in real time, or by later backtracking or recombining previously unmined data points. **Data never disappears and can be indefinitely used and reinterpreted in the context of newer digital footprints or more sophisticated algorithms**, unless a global catastrophe were to occur that would liquidate our servers.

Although this is also true of domestic data flows, technological progress is **shifting the debate from domestic data protection to cross-border flows**. The advent of cloud-based data storage and AI capacities to sift through that data changes the nature of the problem. One country's companies have a huge lead in the cloud industry, while others either try a cooperative regulatory approach or move towards greater technological independence and safeguards, up to tightly controlled or domestic-based servers. **Since a degree of interdependence is very likely to remain, these choices are relative rather than absolute.**

1.1. DATA SOVEREIGNTY AND FREE FLOW EFFICIENCY

Not all nations are equal in this respect too. Their digital abilities differ widely. The US is the global leader in the digital field. Because of the international clout of large digital companies, the US has achieved a form of digital sovereignty over cross-border data flows, even if it does promote free flow over, for example, data localization. The data flow issue in the **United States looks very different in other nations or regional groupings with substantial yet more limited digital assets, or to smaller or far less digitally proficient countries.**

Seen from Europe, all aspects of cross-border digital flows are more dependent on the United States and its companies, from the actual pipes and nodes that transport the flows to data storage and clouds, and to the hardware and software tools used. **More than 80% of European data is hosted by non-European CSOs or cloud service operators, which are mostly American.** Amazon Web Services (AWS), Microsoft Azure and Google Cloud alone account for more than two-thirds of the European market.²

For the United States, data sovereignty is not a defensive but an offensive issue: extraterritorial reach over data is deemed essential for national security, judiciary or fiscal objectives. The CLOUD Act of 2018, which superseded the Stored Communications Act (SCA) of 1986, crystallizes the extraterritorial reach of American legislation through its companies and all entities dealing in some way with the United States. The 2008 Section 702 of the Foreign Intelligence Surveillance Act (FISA) and the 1981 Executive Order 12333, though less cited, established the legal foundation for the NSA's collection and use of intelligence from foreign networks. FISA's Section 702 is set to expire at the end of 2023. Calling for the reauthorization of Section 702, Director of National Intelligence Avril Haines notes that **"we just would not be able to do our job without it"**.³ In 2021, an estimated 232,432 non-U.S. persons were targeted under Section 702.⁴

² Florence Verzelen, "[Avis d'expert] La présidence française de l'Union européenne, une opportunité unique pour l'Europe du digital", *L'Usine nouvelle*, January 16, 2022, <https://www.usinenouvelle.com/article/avis-d-expert-la-presidence-francaise-de-l-union-europeenne-une-opportunit-e-unique-pour-l-europe-du-digital.N1175557>

³ Ali Juell, "Director of National Intelligence, Texas Senator discuss classified documents and security threats surrounding TikTok", *The Daily Texan*, January 29, 2023, <https://thedailytexan.com/2023/01/29/director-of-national-intelligence-texas-senator-discuss-classified-documents-and-security-threats-surrounding-tiktok/>

⁴ Congressional Research Service, "Reauthorization of Title VII of the Foreign Intelligence Surveillance Act", CRS Report R47477, March 17, 2023, <https://crsreports.congress.gov/product/pdf/R/R47477>, p. 10.

As is the case for defense issues, **the next best achievers must decide whether their interests are best served by joining the winner and acting in common, or by adopting catch-up policies that may include protective or protectionist measures** – perhaps renouncing some scaling, and without the benefits from exchange of information. They must also decide how to deal with the legal and technological tools of others – but primarily the United States – to extract data abroad. By contrast, the European Union’s envisaged e-evidence package, on the table since 2018⁵, mandates data access for judicial authorities across the EU, but only obligates third-party providers if the European request does not conflict with third-party law.

Nations in intermediary positions include huge digital markets such as India, particularly competent nations such as Israel or Estonia in specific categories, and a mass of authoritarian nations that prioritize data control and access by authorities over any other consideration. **No country, except possibly North Korea, sits at the complete opposite of the scale from free data flows.** Strategic competitors and systemic rivals such as **China** are in a different position. Their hostility to the United States and to open societies implies that **political imperatives trump economic interests.** They tilt the balance towards full data sovereignty at the cost of restricting outward data flows. Yet they too must find a balance between their own needs for external data flows and shutting themselves off from the global web. The choice becomes more acute as their companies’ global ambitions grow. Russia – and Vietnam – had retained until recently a degree of internet openness. In July 2022, Russian lawmakers approved a bill that would restrict Russians’ personal data from being transferred abroad and require entities planning on doing so to notify the communications regulator in advance.⁶ This move is seen as a response to the

⁵ European Commission, “Proposal for Regulation on cross-border access to e-Evidence”, 2018, https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

⁶ The Federal Law of 14 July 2022 No. 266-FZ on Amending the Federal Law on Personal Data Reuters, “Russian lawmakers approve restrictions on personal data transfers”, July 5, 2022, <https://www.reuters.com/world/europe/russian-lawmakers-approve-restrictions-personal-data-transfers-2022-07-05/>

hefty Western sanctions imposed on Moscow following the invasion of Ukraine.

The opposition between democracy and dictatorship is neither absolute nor simple. For instance, within recognized democracies, the issues of separation of power, independent control and arbitration of data privacy and flows also exist, as is shown by the persistent difficulty of achieving a legally valid transatlantic agreement over personal data cross-border flows. All democracies have national security exceptions allowing for data access, with varying degrees of oversight and effective control over these exceptions.

An Indonesian approach identifies **a trilemma for less digitally advanced countries: they cannot achieve data mobility across borders, personal privacy and security, and data processing or monetization** (or use for third parties) **at the same time.**⁷ One of the three goals must give way. There is therefore an argument for more flexible rules applying to less digitally advanced countries, with tailor-made and case-by-case solutions. This is in fact the case with delocalized back offices, from health to banking and consumer support services, which require the exchange of sensitive personal and non-personal intra-firm data across borders.

As to smaller or digitally least advanced nations, not only is the choice between efficiency and data security more radical, but there may be in fact little choice given the hold of foreign technology, platforms and software providers. They have to accept the supremacy of these key foreign actors in managing data infrastructures and data flows, which in turn may preclude data sovereignty. In theory, they should be leading promoters of multilateral norms and standards. However, in practice, they are often more sensitive to the influence of key providers, and deeply skeptical

⁷ Ibrahim Kholilul Rohman et al., “Cross-border Data Flow: A Trilemma of Mobility, Monetization, and Privacy”, *Indonesia Financial Group, Economic Bulletin Issue 9*, June 8, 2022, https://ifgprogress.id/wp-content/uploads/2022/06/Econ.-Bulletin-Issue-9-Cross-Border-Data-Flow_7-June-2022.pdf

of multilateral agreements brokered by the most influential countries. At the World Trade Organization (WTO), for example, the African group noted in 2017 that “attempts to introduce a ‘digital trade agenda’ in the WTO multilateral framework will constrain the ability of governments to implement industrial policy and catch-up”.⁸ Yet **they retain the option of gravitating between what is an “America plus” framework and providers, and an authoritarian model provided chiefly by China.** In the latter case, an even larger question mark hangs over data protection.

Is there a European “third way” for digital sovereignty, as is sometimes suggested for overall strategic issues? **Playing catch-up, defying the odds of winner-take-all situations, benefiting from scalability for late-comers, and ensuring data security with less available frontline tools are key issues for Europe, as well as for others who do not integrate completely with the US digital space and norms.**

A digital industry dwarf and an underdog competitor for innovation and start-ups, Europe has the advantage of a more rationally organized European market – even the division between 27 Member States is less of a regulatory obstacle for data usage than the planned state of anarchy of US federal and state data rules and implementation. Unlike Silicon Valley, the “Brussels effect”⁹ is ensured through the influence of rules, particularly those protecting personal data: anywhere between 137 to 142 nations have a form of personal data protection, which are at least partly influenced by GDPR.¹⁰ We shall see in some cases (China being the most obvious) that the differences may matter greatly. An OECD paper notes that in Asian data protection laws, data localization and data

⁸ World Trade Organisation, “Report of Panel Discussion on “Digital Industry Policy and Development””, July 21, 2017, p.2, <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/Jobs/GC/133.pdf&Open=True>

⁹ Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, 2019, <https://academic.oup.com/book/36491>

¹⁰ UNCTAD, “Data Protection and Privacy Legislation Worldwide”, <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

transfer safeguards often co-exist and the uncertainty of their interplay is a source of confusion.¹¹ According to a 2022 McKinsey paper, around 75% of countries have some level of data localization rules in place.¹² Given that the European Union is the most advanced supranational digital space, with rules that seek to ensure data flows, data security and public order across the European digital space, it is tempting to see this as a potential regulatory model and a way to make up for what it lacks in terms of industry champions and technological strength. Yet, as we shall see, there are key elements missing in order to achieve this goal. **Digital infrastructure and market dominance by firms matter.**

1.2. DIGITAL PRIVACY

As if this complexity and the arbitration between data sovereignty and free flow efficiency weren’t enough, the choices also intersect a third issue – that of digital privacy and the protection of personal data, or the security of non-personal data such as proprietary company data within national borders. Protection of personal data is still a huge subject of debate within national borders. **The advent of data harvesting, algorithms and AI have made our personal data a gold mine for commercial purposes, and for intelligence gathering by governments – others or our own.** It is impossible to separate the issue of cross-border data flows from that of data privacy risks, which will keep expanding through the use of AI tools.

A key difference between American and European approaches to the data privacy issue is that of consent, perhaps the most visible aspect of GDPR

¹¹ Lisa Robinson, Kosuke Kizawa, and Elettra Ronchi, “Interoperability of privacy and data protection frameworks”, OECD, *Going Digital Policy Toolkit Note*, No.21, 2021, https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf

¹² Satyajit Parekh et al., “Localization of data privacy regulations creates competitive opportunities”, McKinsey & Company, June 30, 2022, <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities>

to any internet user. The difference can be summed up easily: **the American approach is by notice-and-choice**: access to a website is conditional on a contract, and a user who denies the terms of the contract cannot get access to the service. By contrast, **GDPR requires express consent by the user to data harvesting**, and rules out cookie walls¹³ as a valid and freely given consent. This is the gist of the recent issue between Meta (Facebook's parent company) and the European Data Protection Board. The Irish Data Protection Commission (DPC) largely sided with Meta, but finally bowed in January 2023 to the EPDB's decision, if not to the scale of the fine for Meta's conduct since GDPR was promulgated.¹⁴ Limiting the advertising and third-party sales of hyperscalers who depend on these revenues is a momentous decision that will even the odds for smaller companies. It is a decision that has as much or more impact on transatlantic digital space as taxation, reversing the adage that "if the product is free, it means you are the product".

Yet it is neither strategic nor a component of public order. We must be able to entertain these transatlantic differences – and hope that they inspire privacy advocates in the United States – without fragmenting the digital space.

The two purposes – commercial and intelligence or broadly speaking public order – can, in fact, overlap, although different political systems put more emphasis on one or the other. **The contrast is often made between democracies and authoritarian systems.** Indeed, no authoritarian system will adequately protect its citizens from the reach of the state. But within democracies, separation of power, the independence and reach of regulatory bodies, the actual ability of citizens to refuse

¹³ "In order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so called cookie walls)" - European Data Protection Board, "Guidelines 05/2020 on consent under Regulation 2016/679", https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

¹⁴ noyb, "Breaking: Meta prohibited from use of personal data for advertising", January 4, 2023, <https://noyb.eu/en/breaking-meta-prohibited-use-personal-data-advertising>

extraction of their personal data or to retain control over its onward use, as well as the right to identify privacy breaches and to obtain redress, can vary widely. One should read the recent resignation letter of the Dutch regulator for intelligence and security services.¹⁵ His complaints against a proposed legislative change include the suppression of *ex ante* oversight and the introduction of algorithmic treatment of bulk intercepted data. As to authoritarian systems, even if they prioritize state access to personal and non-personal data under various pretexts or reasons, they still need to maintain cross-border data flows. They also have to contend with the lack of trust. **A major digital state such as China, however authoritarian, has an incentive to limit personal data mining by platforms that create monopolies;** "surveillance capitalism" and the "surveillance state" are likely to exist in different proportions in democratic and authoritarian systems. Containing and repelling these two hydras requires different institutions. Protecting data privacy from commercial harvesting requires many tools, from rules on data gathering and consent to competition laws that keep consumer choices open. Fighting state surveillance, including excesses in our societies, requires above all a separation of powers with independent oversight.

Between the two systemic approaches, India appears as a major fence-sitter. Its digital economy is forecast to reach 1 trillion dollars (approx. 896 billion euros) by 2025.¹⁶ For years, India has considered a data protection act closely similar to Europe's General Data Protection Regulation (GDPR) – only to abandon the bill on August 4, 2022. It has now introduced a new bill, enabling cross-border data sharing agreements but incorporating large exceptions to data privacy for India's state governments under broad reasons of national security (for more details on the case of India, see Chapter 6 Page 69).

¹⁵ Bert Hubert, "On my resignation as regulator of the Dutch intelligence and security services", September 9, 2022, <https://berthub.eu/articles/posts/resignation-as-intelligence-regulator/>

¹⁶ "India's Trillion Dollar Digital Opportunity", Indian Ministry of Electronics and Information Technology, May 24, 2019, <https://www.meity.gov.in/content/india%E2%80%99s-trillion-dollar-digital-opportunity>

1.3. ENFORCEMENT

The cases of commercial harvesting or state surveillance are very different. Yet, enforcement remains a common issue in both. **As data becomes the ubiquitous prime mover of economy and society – think Internet of Things, for example – actual oversight becomes more difficult.** To the credit of the European Union, GDPR represents the first concerted effort to tame the commercial use of personal data with rules that also limit data gathering for public purposes. That first attempt did include loopholes. A study by the Irish Council for Civil Liberties (ICCL) found that the average European user's data is shared 376 times per day through real-time bidding (RTB).¹⁷ The figure rises to 747 times daily for US-based users. Another evaluation, while recognizing the superiority of GDPR's express consent requirement over the US notice-by-choice approach, usefully lists many impasses that internet users have experienced for themselves in the consent approach: "The notice-and-choice approach is farcical; the express consent approach is impractical". This suggests the need for a combination of limited consent (what the author calls "murky consent") and government guardrails that make up for an individual's inability to give enlightened consent in most situations.¹⁸

Enforcement is also an issue where no adequacy agreement for cross-border data flows has been reached. **The European Court of Justice (CJEU) Schrems II decision¹⁹ invalidating the US-EU Privacy Shield due to the lack of truly independent oversight has led to a situation where much business data transfer is "alegal"²⁰,** as one knowledgeable

Commission official puts it, or illegal, if one follows other insiders. The same might be said of the post-Brexit issue of EU-UK data flows. The difficulties for companies in implementing complex and far-reaching requirements have been underlined. Binding corporate rules (BCRs), standard contractual clauses (SCCs) and GDPR derogations are sub-optimal solutions in the absence of an adequacy agreement. BCRs are only feasible for large multinational corporations. SCCs require, in many cases, additional risk mitigation decisions by companies that bear responsibility for their partner's compliance. Derogations to GDPR are not stable but rather occasional arrangements. Other avenues, such as codes of conduct or certification, are still in the making.²¹ Many companies will actually transfer data without the adequate legal framework – and there is no sufficient enforcement capacity to prevent this.²²

Indeed, **on the European side, much more regulation has been coming, canceling the "one-size-fits-all" approach that GDPR seemed to deliver.**²³ The European approach to cross-border flows is also via adequacy decisions²⁴ requiring common purpose and equivalent means from international partners, complemented by tools for data transfer to a country that doesn't ensure an adequate level of data protection by EU standards (standard contractual clauses, binding corporate rules, certification mechanism, codes of conduct, so-called "derogations", etc). These are important steps to tame what has quickly become an international

¹⁷ Brandon Vigliarolo, "Your data's auctioned off up to 987 times a day, NGO reports", *The Register*, May 18, 2022, https://www.theregister.com/2022/05/18/advertisers_broadcast_pii_more_than/

¹⁸ Daniel J. Solove, "Murky Consent: An Approach to the Fictions of Consent in Privacy Law", George Washington University Law School, January 15, 2023, <http://dx.doi.org/10.2139/ssrn.4333743>

¹⁹ Hendrik Mildebrath, "The CJEU judgment in the Schrems II case", European Parliamentary Research Service, September 2020, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA\(2020\)652073_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf)

²⁰ An act that is not within the framework of the law, yet not expressly illegal.

²¹ Hendrik Mildebrath, "EU-UK private sector data flows after Brexit: Settling on adequacy", European Parliamentary Research Service, April 2021, [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690536/EPRS_IDA\(2021\)690536_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690536/EPRS_IDA(2021)690536_EN.pdf)

²² Interview with a former data security Member State official.

²³ Glyn Moody, "EU to Use ePrivacy and GDPR to Tackle Illegal Cookie Walls", *PIA Blog*, January 31, 2023, <https://www.privateinternetaccess.com/blog/eu-illegal-cookie-walls/>

²⁴ As of January 2022, the EU has granted adequacy to Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED (Law Enforcement Directive), and Uruguay. See: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

black hole – the handling and exploitation of data by many public and private actors beyond our grasp.

The GDPR may not be perfect – a frequent criticism is that it is too wieldy to enforce, and that it leaves aside issues of cybersecurity. GDPR-based approaches require every country to determine the suitability of cross-border flows to and from every other country. A simple calculus should make one realize that “if 194 countries adopted this approach (with 28 EU countries acting as one bloc), over 14,000 bilateral determinations would be required”.²⁵ But GDPR would still be a giant step forward for Europe if it was not for a new reality: more data crosses Member States and EU borders than at any time in history.

Yet it is not only a landmark event such as the Edward Snowden revelations, nor the planned asymmetry of digital systems like China’s – a one-way street where data flows in easily but is much more constrained on the way out – that drive the new cross-border issues. There are also issues of **economic interest. This is manifested with the issues of “winner takes all” or “first-mover advantage” which make it more difficult for new entrants to scale up.** It is also present in the issue of a digital tax that would be based on the place where data is used and where sellers earn income rather than where it is processed or where the company is based. A single digital space needs to balance the differences in domestic rules with the magnitude of cross-border data flows. What’s more, non-personal data, with the accompanying issues of intellectual property and business confidentiality, have also reached a threshold where they must be considered as just as important as personal data. This is the case even if public debate focuses more on the latter because it speaks to the individual.

²⁵ Seharish Gillani et al., “The role of cross-border data flows in the digital economy”, *UNCDF Brief*, July 2022, p.8, <https://web-assets.bcg.com/7a/2b/9a0cb4b545ad87cf7e901301ad27/en-uncdf-brief-cross-border-data-flows-2022.pdf>

1.4. THE TWO TRIANGLES

Any policy on cross-border data flows must therefore recognize several dilemmas, which cannot be fully resolved but only arbitrated.

One is **the triangle between goals of efficiency, privacy and security.** Efficiency is created by the powers of data extraction, storage, and of their use through algorithms and artificial intelligence. Today, it is the global economy’s chief source of productivity, and any entity – be it a nation, a company or an individual – shutting itself off from this source is greatly decreasing its own abilities. **Privacy** – perhaps the best-advertised side of this triangle – is the need to preserve personal data from extraction, recombination and unauthorized third party or detrimental use. Here too, compromises will always be made. Health is the sector that comes up most frequently in this context because the contrast is stark between the need for data protection and the potential benefits of data sharing. **Security** – all the way from protecting the non-personal but crucial manufacturing, design, or marketing data of a company to the national security of a state – seems an obvious requirement but also runs into compromises between the state, business and individuals. For example, where should policy-makers draw the line for critical data in a new world where recombination of what appears to be trivial data points leads to major intelligence results?

Another triangle is both geopolitical and geoeconomic: to simplify this, consider the United States, the European Union and China. Each side seeks, even in different ways, to achieve some control over their own data and accessing and aggregating the data from each other and from third-party data spaces. The contrast between American or European values and practices with China’s is stark: Chinese data management is always open to the Party-state’s look-through capacity. Where technical obstacles exist – for example, the superior data-gathering abilities of Chinese platform companies compared to the Party-state itself – new rules will tip the balance again towards the Party-state. Yet huge

commercial interests still bind major Western companies and venture capital to the Chinese data market. The global expansion of Chinese data firms – a process that with few exceptions is still behind that of American firms – also relies on their acceptance in other markets.

The free flow of data between Europe and the United States is not a given either. Concerns exist about data sovereignty and the issue of access and extra-territorial reach for national security reasons. The European approach is based on rules enhancing privacy and human rights, while American rules derive from business law, the main tension being over consumer rights. The present solutions considered for some of these problems – from agreed rules for intelligence collection of personal data to digital tax regimes – have led to renewed hopes of a single transatlantic space. American rearguard action against the digital tax at the OECD, and the potential intransigence of the European Union’s legal requirements as interpreted by the European Court of Justice put this very much in question.

1.5. LESSONS

The global internet has often been likened to a free and open commons, much like the high seas. Like the narrative of data as the new oil, this dream was never true, if only because the infrastructure nodes, the protocols and the assignment of IP addresses (by ICANN) were always embedded with states. The unsavory alternative is **a world of digital firewalls and moats, designed with data security for the states that erect them.** Ultimately, this would be the “splinternet” that there are many reasons to fear.

In between these two alternatives are **rules and enforcement capacities of these rules.** But it is very unlikely that our multilateral institutions, riddled with competition for influence, can gain acceptance for rules that would truly restrain state actors. The issues of **trust, verification and**

legal arbitration divide competing political systems. Other global commons that are far less controversial – such as carbon emissions – encounter these same obstacles. Digital data is far more strategic and central to geopolitical and geoeconomic competition.

2 Regulating cross-border data flows

Regulating data flows – including cross-border transfers – is not hindering or preventing them. On the contrary, it is a condition for their development because it 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 difficulty in meeting these goals lies not only in threading the needle between data protection and data access. In the case of cross-border flows, it is also **to arbitrate between different legal systems and actors, and enforce the choices that are made and agreed upon.** A law is only as good as its enforceability, and this is even more difficult in the digital domain where “code is law” to some extent. In this sense, the complete fragmentation of the internet that is often talked about is a risk but also a practical impossibility: as long as human, cultural, technological, and economic exchanges occur, the internet and digital industries have become a leading actor and one of the main forces of innovation and productivity.

In view of the divergences among countries at different stages of digital development discussed in the previous chapter, there has been an attempt to classify cross-border rules in four categories:

- a **“bourgeois” European concept** protective of human rights and privacy;
- a **trade-based US environment** with large public and private cooperation;

- a **Chinese authoritarian model** that prioritizes state control;
- a **Russian or North Korean hacker’s model**.²⁶

These categories are seductive, but they often don’t fit. The European model recognizes public needs of access, and more reluctantly the role of the private sector. In the United States, “surveillance capitalism” has come to symbolize the hold of companies over data, and the collection of data by intelligence agencies is not wholly supervised, even for American citizens. China has a stake in preserving competition in the interest of innovation – it is the only country that has created tech giants matching the size of American ones. Finally, cases like Stuxnet and the open development of offensive cyber capacities demonstrate that cybercriminals do not have a monopoly on hacking.

2.1. EXISTING ARRANGEMENTS AND INITIATIVES

Largely because of the above considerations, **various collective arrangements have sprung up over time to regulate cross-border data flows**. They are well known in specialized literature, and will therefore only be listed here, in historical order:

- **The OECD had issued non-binding recommendations on privacy protection** and cross-border personal data flows as early as 1980 (last revised in 2013).²⁷ Most of these recommendations would be incorporated by **the European Union in its first Data Protection Directive in 1995**.
- **The Convention 108 of the Council of Europe** followed in 1981 and now has 55 signatory states.²⁸ As of today, Convention 108 is the only

²⁶ Kieron O’Hara & Wendy Hall, *Four Internets: Data, Geopolitics, and the Governance of Cyberspace* (2021), <https://academic.oup.com/book/40014>

²⁷ OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. OECD/LEGAL/0188, 2022, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>

²⁸ Council of Europe, “Chart of signatures and ratifications of Treaty 108”, <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=108>

legally binding international instrument in the data protection field and contains key concepts regarding data protection and privacy laws that have emerged afterwards, including GDPR (and its predecessor the Data Protection Directive). An **update in 2001 (the Additional Protocol)** concerns necessary levels of protection by third parties in order to authorize data transfers and requires parties to set up independent supervisory authorities.²⁹ **A larger revamping in 2018, known as “Convention 108+”**³⁰ is still open to signing before it comes into force. It aims to ensure its compatibility with normative frameworks across the world and allows for further protection of personal data by regional organizations.

- The **Asia-Pacific Economic Cooperation (APEC)** adopted in 2005 a Privacy Framework, followed by **Guidelines and Cross-Border Privacy Rules (CBPR)** in 2011. It is not mandatory, with only seven of twenty-one APEC economies participating. Similarly, **ASEAN adopted a Framework on Personal Data Protection** in 2016 – but it is neither binding nor mandatory for signatories. It has led to the **ASEAN Model Contractual Clauses (MCC)** for cross-border data flows in 2021. However, none of these regional initiatives address the government-to-government trust issues highlighted by the Schrems rulings.
- Recently, in December 2022, the OECD adopted the **first intergovernmental agreement on common principles to safeguard privacy and other human rights and freedoms when accessing personal data** for law enforcement and national security.³¹
- Some states have bilaterally proposed standard contractual clauses for cross-border data transfers – the United Kingdom, New Zealand and Argentina.

²⁹ Council of Europe, “Details of Treaty No.181”, ETS No. 181, <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty=181>

³⁰ Council of Europe, “Modernisation of the Data Protection “Convention 108””, <https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet>

³¹ OECD, *Declaration of Government Access to Personal Data Held By Private Sector Entities*, OECD/LEGAL/0487, 2023, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>

Much more significant is the adoption in 2016, and in force since 2018, of the **General Data Protection Regulation** of the European Union. In addition to the well-known provisions of the GDPR regarding the protection of personal data, **it has a full chapter regarding data transfer outside the EU**. This includes adequacy decision with a third country or an international organization (Article 45), other tools when such a decision is absent (Article 46), such as the standard contractual clauses (SCC) and binding corporate rules (BCR), and a list of derogations for specific situations (Article 49), such as when it is necessary for important reasons of public interest or legal claims. Notably, Article 48, and its corresponding Recital 115, also provide that decisions from third-country authorities, courts or tribunals do not in themselves constitute a legal basis for data transfers to third countries. This has been followed in 2018 by a **regulation on non-personal data which prohibits data localization requirements between Member States except for public security reasons** – a major step to create a single EU space for non-personal data. Since 2022, the **EU Data Governance Act** regulates the exchange of protected public data, including with third parties to the EU, with requirements on the data intermediaries and an emphasis on non-profit (“altruistic”) use of the transferred data.

The Council of Europe’s **Convention 108**, improved by 108+, and the successive OECD Recommendations (1980 and 2013) come closest to multilateral arrangements, and the OECD’s are also the most detailed. A fully multilateral approach is far from achieved at this point. The United Nations, through a 2021 UNCTAD report,³² emphasizes free flow against digital fragmentation and warns against the hold of some companies over data. In 2022, the UN launched a Privacy Enhancing Technologies (PET) lab aiming to facilitate cross-border statistical exchanges.

³² UNCTAD, *Digital Economy Report 2021*, New York, 2021, <https://unctad.org/webflyer/digital-economy-report-2021>

Far more important would be concrete and binding regulations issued by the World Trade Organization on non-personal flows. This would be part of the extension of WTO disciplines from goods to services, including data transfers. The World Bank issued a report in 2021 that also considers issues such as digital taxation. But GATT, the original agreement that led to the WTO, is about goods. GATS, the corresponding agreement for services arrived in 1995, has few provisions regarding data. Data is, at best, a by-product, considered only as a tradable good. **So far, the WTO has initiated since 2017 a negotiation on e-commerce, which is still pending. A joint Industry Statement on these issues has been issued in 2021, encouraging negotiators to close a deal.**

This is by no means the end of the multilateral or nearly multilateral story.³³ There have been several informal or private attempts at furthering data protection within transfers. One is the United Nations Special Rapporteur on digital privacy rights’ Working Draft Legal Instrument on Government-led Surveillance and Privacy³⁴ which draws heavily on the inspiration of EU legislation. The other is a Digital Geneva Convention (DGC, 2017), presented by Microsoft’s chairman Bradley Smith, that has led to a code of conduct among 34 digital and security companies. The **LIGSC importantly does not consider metadata in its survey** – a critical gap nowadays. On the other hand, it excludes economic interest from the permissible range of state surveillance, and broadly notes the importance of restricting bulk surveillance. It finally proposes the creation of an independent international body with experts drawn from participating states. By contrast, the **DGC includes the notion of “neutrality”** which Microsoft has also been emphasizing commercially, as it has no horizontal platform activity or advertising revenue from the data it collects and stores. However, its actual implementation rests with the existence

³³ OECD, *Cross-border Data Flows: Taking Stock of Key Policies and Initiatives*, OECD Publishing, Paris, <https://www.oecd.org/publications/cross-border-data-flows-5031dd97-en.htm>

³⁴ Office of the United Nations High Commissioner for Human Rights, “Appendix 7: Draft Legal Instrument on Government Led Surveillance”, in *Report of the Special Rapporteur on the right to privacy*, February 28, 2018, https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf

of legally secure firewalls and not only with the technological capacities that Microsoft undoubtedly possesses.

Europeans should be well aware of more intergovernmental approaches to a plurilateral agreement on digital flows – where previous attempts at broad trade and investment agreements have failed. The Indo-Pacific Economic Framework for Prosperity (IPEF) launched by the Biden administration in May 2022, targeting the 11 CPTPP members plus India, includes standards on cross-border data flows and data localization.³⁵ A detailed agreement, DEPA, the **Digital Economy Partnership Agreement** has been signed by Chile, New Zealand, and Singapore in 2020. It is broadly based on provisions of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the APEC guidelines, and the 2019 U.S.-Japan Digital Agreement. In December 2022, Xi Jinping cited DEPA, along with CPTPP, as the main goals for China's future participation into international organizations.³⁶ **A key issue for the European Union will be its emphasis on arbitration rather than legal enforcement**, although the WTO's Dispute Settlement Mechanism is invoked as a last resort: we have seen that the WTO has little to offer in this area. The DEPA places a major emphasis on trust. It also prohibits data localization requirements and custom duties on electronic transmissions, including digital goods and their contents, but takes no position on digital taxes. It requires technological neutrality – including no requirement on cryptography and only limited exceptions to this rule and to access by parties to the Agreement: the allowed exceptions are for government networks and investigations on financial institutions and markets.³⁷

³⁵ The White House, "FACT SHEET: In Asia, President Biden and a Dozen Indo-Pacific Partners Launch the Indo-Pacific Economic Framework for Prosperity", May 23, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-in-asia-president-biden-and-a-dozen-indo-pacific-partners-launch-the-indo-pacific-economic-framework-for-prosperity/>

³⁶ Qiushi, "Several major issues in the current economic work (当前经济工作的几个重大问题)", February 15, 2023, http://web.archive.org/web/20230329084010/http://www.qstheory.cn/dukan/qs/2023-02/15/c_1129362874.htm

³⁷ New Zealand Ministry of Foreign Affairs and Trade, *Digital Economy Partnership Agreement*, June 11, 2020, Article 3.4, <https://www.mfat.govt.nz/assets/Uploads/DEPA-Signing-Text-11-June-2020-GMT.pdf>

A Russian legal think-tank analysis indicates that this is indeed contradictory to requirements from Russia's Federal Security Service (FSB) and other intelligence agencies in the Eurasian Economic Union (EAEU), but finds few other faults with the Agreement.³⁸ Indeed, countries as diverse as China and Canada have applied to join DEPA. EU analysts may find its content minimal and with insufficient means of legal enforcement. Yet, **Europeans should take notice** that if, following the requests of the CJEU, they have too many requirements for cross-border data agreements, they **risk being encircled by less demanding agreements that will focus on the practical aspects of these cross-border flows**.

The other push for better regulation takes place within G7 and G20 institutions, and it is largely at the initiative of Japan's government. **Japan has a special interest in promoting a regulated and open regime for data transfer**: it is at the frontier of economic interaction with the world's largest authoritarian system – China; it has security interests tightly linked to the United States; and finally, it is a commercial power that has signed a Free Trade Agreement with Europe and has incorporated, through an adequacy decision, the same values protecting individual rights as the EU. Its **Data Free Flow with Trust (DFFT)** initiative at the 2019 G20 summit in Osaka has been consistently followed through in both the G7 and G20 formats: the emphasis differs, however, with the G7 format insisting on "the shared values of like-minded, democratic and outward-looking nations", while G20 declarations insist on potential convergences among different systems to foster interoperability. The European Union is also launching digital partnerships with key Asian countries, starting from Japan in May 2022, developing towards Korea (November 2022) and Singapore (November 2022). These partnerships are broadly conceived and voluntary rather than binding. There are aspects related to semiconductors (where the EU has also designated Taiwan as a partner), supply chain security, and telecom standards. They also include dialogue on digital trade

³⁸ International and Comparative Law Research Center, *Rules for Digital Trade: The Digital Economy Partnership Agreement (DEPA)*, Moscow 2020, https://iclr.ru/storage/publication_pdf/ICLRC_DEPA_1649174353.pdf

facilitation, data flow standards in general, and in Japan's case, "certain emerging technologies on privacy, privacy-enhancing technologies and enforcement cooperation between supervisory authorities responsible for data protection".³⁹

Clearly, **Japan is also attempting to bridge the gap between idealism and realism on data transfer** – between a universal regime that would ensure a seamless digital world, and the practical reality that a less than fully multilateral regime is the only option to move ahead in the short term. The proposals have spanned trade rule-making, regulatory cooperation and enabling technologies. Presiding over the G7 in 2023, Japan goes one step further by proposing an "International Arrangement" that would include both a Government panel and a Stakeholder panel, with public, private and expert cooperation. This move is in line with the LIGSC proposal outlined above, and it also looks very much like the type of bipartite or tripartite consultation that the OECD had led in other areas. If approved, **the scheme is likely to lead to a Secretariate embedded within the OECD – less than a new fully-fledged international organization, but much more than a coordination and negotiation format.** As a start, the arrangement would spawn test projects for transparency, data certification and privacy enhancing technologies (PETs).

In the cybercrime domain, the Council of Europe's **Convention on Cybercrime** (known as the Budapest Convention) is the first and the most widespread international treaty to address criminal sanctions in cyberspace. In force since 2004, it has been signed by 67 states, including non-Council of Europe states such as the US and Japan. Russia has not joined the Budapest Convention on the ground of Russian sovereignty, despite being a member of the Council of Europe. The UN is currently negotiating a major Cybercrime Convention – ironically, Russia was the country that pushed for the Resolution at the 2019 UN General Assembly, with the support of China, North Korea, and other co-sponsors.

³⁹ Ministry of Foreign Affairs of Japan, *Japan-EU Digital Partnership*, May 2022, <https://www.mofa.go.jp/files/100343128.pdf>

2.2. LESSONS

All these proposals testify to the failure of the WTO to create new disciplines regarding digital flows. This is unfortunate since many of the issues regarding cross-border data flows, whether non-personal or even personal, fall under trade agreements or include aspects of trade. It is the case of Convention 108 itself. Increasingly, recent Free Trade Agreements (FTAs) include provisions, often binding, on digital transfers. Overall, 72 economies have introduced digital provisions in preferential trade agreements. These provisions are sometimes weighted towards ensuring free data flows, sometimes towards exceptions and restrictions under reasons of public interest. **The divide does show that cross-border data flows are not comparable to tradable goods, but imply systemic choices and values.**

In contrast with the multilateral or quasi-multilateral approaches, the United States, benefitting from the scale of its market and the strength of its digital service providers, seeks bilateral agreements on data transfer. It is **likely to become the center of a "hub-and-spoke" model of direct access mechanisms.**⁴⁰ The controversial CLOUD Act has been incorporated in a US-UK data access agreement, the first agreement of its kind and in force since October 2022. Australia has signed a similar arrangement in December 2021. Negotiations are on-going with Canada, and New Zealand is also considering one. It is no accident, of course, that this list is also that of the Five Eyes countries which have agreed to fully share infrastructures for intelligence data collection.

Despite being the subject of complaints, **the CLOUD Act can be a handy tool: it opens a window for foreign countries to overcome the cumbersome Mutual Legal Assistance Treaty (MLAT) process**⁴¹ and to

⁴⁰ Tim Cochrane, "Hiding in the Eye of the Storm Cloud: How CLOUD Act Agreements Expand U.S. Extraterritorial Investigatory Powers", *Duke Journal of Comparative & International Law*, Vol. 32, No. 1, 2021, pp.153-210.

⁴¹ UK Home Office, "Policy factsheet on the UK-US Data Access Agreement", July 21, 2022, <https://www.gov.uk/government/publications/uk-us-data-access-agreement-factsheet/policy-factsheet-on-the-uk-us-data-access-agreement>

request data from telecommunications services operating within US jurisdiction – most of the world’s popular telecommunications services fall under that umbrella. By contrast, immediately after the CJEU’s Schrems II decision, Switzerland and Israel, for very different reasons, have found that the Privacy Shield did not afford enough protection to their citizens.⁴² Israel, which reinforced its Privacy Protection Act in January 2022, has announced in October of the same year that its Privacy Protection Authority would be “independent in applying the powers vested (...) under the law”.⁴³ This is an effort to avoid rejection by the EU Commission or by the CJEU of data transfers, and the Israeli decision appears similar to the White House’s Executive Order of the same month.

3 Digital sovereignty

A seamless, largely unregulated digital world, may have been an utopia. However, that utopia brought both a Schumpeterian era of innovation, with immense economies of scale and productivity gains, and an unprecedented intrusiveness into former areas of state sovereignty and the individual sphere of rights. It is no surprise that notions of sovereignty, of strategic autonomy and a goal to “take back control” coexist within the same individual: **the citizen wishes for data privacy while the consumer (of information, products, services...) hails the range of choices and broadened information that the digital era offers.**

⁴² Christakis, Theodore, 'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy (December 7, 2020). Available at SSRN: <https://ssrn.com/abstract=3748098> or <http://dx.doi.org/10.2139/ssrn.3748098>

⁴³ Omer Tene, “Data transfer theater: The US and Israel take the stage”, *iapp*, October 4, 2022, <https://iapp.org/news/a/data-transfer-theater-the-us-and-israel-take-the-stage/>

Additionally, scaling has immensely helped the gains of first movers, with increasing returns for diminishing outlays. In this sense the digital revolution differs from earlier industrial eras, because the time to return has greatly shortened, as exemplified by Moore’s law. The automobile, for example, spread much more slowly than the mobile phone, and very few if any of the first auto companies survived the long span needed for return. The latter stages of the digital revolution have arrived even more quickly. The first Blackberry appeared in 1999, the first iPhone in 2007. Today, smartphone ownership is estimated around 7 billion.⁴⁴ Instagram reached 100 million users in two and a half years, TikTok in nine months, ChatGPT in two months – with India right behind the United States in usage. **It is no surprise that this exponential growth has benefitted the companies and sites that were the first movers or who captured best the industrial consequences.**

This is reflected in the dominance of US and Chinese companies, given their respective dominance of soft and hard components. The same is true of several other digital sectors, although few Europeans take notice that the European data market is underdeveloped compared to other industrialized countries. The value of the European data market (including the UK and the European Economic Area) reached 63.6 billion euros for the EU27 in 2021, with a 4.9 per cent growth rate. While Germany represented 28% of this market, France grew fastest. However, a similar evaluation for the United States in the same year is 240 billion dollars (approx. 226 billion euros), and for Japan (population 125 m. as against 447 m. for the EEA) is 40 billion dollars (approx. 37.7 billion euros).⁴⁵

The future may not be so different: The EU’s AI investment in 2016 was only 3.2 billion euros, against 12.1 billion euros in North America and

⁴⁴ Statista, “Number of smartphone subscriptions worldwide from 2016 to 2021, with forecasts from 2022 to 2027”, <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>

⁴⁵ European Commission, “Results of the new European Data Market study 2021-2023”, February 22, 2023, <https://digital-strategy.ec.europa.eu/en/library/results-new-european-data-market-study-2021-2023>

6.5 billion euros in Asia.⁴⁶ **Europe may be a world leader in creating influential digital regulation, but “referees do not win matches”.** To its credit, the European Commission is aware of this gap, and stated in its 2020 digital strategy the goal that “by 2030, the EU’s share of the data economy – data stored, processed, and put to valuable use in Europe – at least corresponds to its economic weight, not by fiat but by choice.”⁴⁷

It is against this backdrop, where informational and economic gains are balanced by intrusiveness on sovereign, personal and non-personal data, and where there are unprecedented asymmetries in capacities, that a **push for digital sovereignty or strategic autonomy occurs.** These terms also cover more general or ideological concepts of sovereignty. The resulting debates, involving political issues and/or public opinion in an era when globalization is generally questioned, are heavily weighted towards one end of the scale: sovereignty. Who would not be for the protection of national security and public order? Who would stand against personal data privacy? **Who would not wish to “take back control”** instead of perpetuating dependencies towards foreign actors, whether public or private, which obey rules that are not our own?

3.1. THE FACETS OF THE EUROPEAN SOVEREIGNTY DEBATE

It is important but would require much more space to discuss all the facets of this sovereignty debate, and we will refer to a recent study that captures at least the European end of it.⁴⁸ Where sovereignty was a taboo term in the European Union, it is constantly referred to at the Commission

level and in Member State pronouncements, with perhaps a special mention for France, where Emmanuel Macron has used the term fifteen times in a single speech.⁴⁹ Yet **Europeans, including the French, mostly mean sovereignty as the technological means necessary for autonomy, excluding neither interdependence nor free data flows, and not in the sense of complete self-reliance** or as what has come to be known as the Great Chinese Firewall. In Thierry Breton’s own words, “sovereignty, as we know, is a loaded – sometimes divisive – term which lends itself to various interpretations even across our European continent. Others prefer to talk of resilience, others of (open, strategic, or plain and simple) autonomy.”⁵⁰ Language coincidences should not be taken as signs of similar or convergent policies, even if, in all areas of industrial policy, including innovation and the digital sector, temptations exist to “do as the Chinese do”, conflating sovereignty with self-sufficiency.

The other feature of the European approach, at least for now, is that it has focused on defensive rather than offensive digital sovereignty.

There may be exceptions, for example in cybersecurity, where France acknowledges offensive military capacities in cyberspace.⁵¹ The general approach is in line with the EU’s trade defense policies since 2016. It differs from the American approach where offensive sovereignty is an important feature: first because of the huge international footprint of American digital firms, second because of its use of extraterritorial rules in the digital sector on a par with financial and tax legislation, and third because of a highly diversified US cyber force.⁵²

⁴⁶ European Commission, “White Paper on Artificial Intelligence: a European approach to excellence and trust”, February 19, 2020, https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

⁴⁷ European Data Protection Board, *A European strategy for data*, February 19, 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&from=EN>

⁴⁸ Theodore Christakis, “European Digital Sovereignty: Successfully Navigating Between the ‘Brussels Effect’ and Europe’s Quest for Strategic Autonomy”, Grenoble: Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute, Studies on Digital Governance, Dec 18, 2020.

⁴⁹ *The Economist*, “Emmanuel Macron in his own words (English)”, November 7, 2019, <https://www.economist.com/europe/2019/11/07/emmanuel-macron-in-his-own-words-english>

⁵⁰ European Commissioner, “Speech by Commissioner Thierry Breton: Sovereignty, self-assurance and solidarity: Europe in today’s geopolitics”, September 5, 2022, https://ec.europa.eu/commission/presscorner/detail/de/speech_22_5350

⁵¹ Le Ministère des Armées, “Le commandement de la cyberdéfense (COMCYBER)”, May 2017, <https://www.defense.gouv.fr/ema/commandement-cyberdefense-comcyber#title-21530>

⁵² U.S. Cyber Command, “Our Service Cyber Partners”, <https://www.cybercom.mil/Components/>

The offensive capacities of the United States in cybersecurity are not well known, except through Edward Snowden’s revelations. The U.S. Cyber Command (USCYBERCOM) has among its primary missions to “engage our enemies in the cyber domain” with what it calls Hunt Forward Operations. Hunt Forward Operations involve the deployment of USCYBERCOM Hunt Forward Teams to partner nations, at their own request, to observe and detect malicious cyber activity on host nation networks. The U.S. Department of Defense (DoD) has acknowledged 30 such operations before the war in Ukraine.⁵³ In the wake of Russia’s invasion of Ukraine, the French commander of an analogous COMCYBER commented that the technical support “opens to Americans the networks of countries which ask for their intervention”.⁵⁴ In 2022, an official Chinese source attributed to the NSA the hacking of a leading aerospace institute: this was a rare recognition of an actual weakness.⁵⁵ One can easily infer from the US digital superiority that the country also possesses the most advanced offensive capacities in this domain. At the same time, the US continues to invest in its defensive capabilities. The US National Cybersecurity Strategy released in March 2023 identified five pillars of actions to enhance security in cyberspace.⁵⁶ **The combination of both offensive and defensive strengths puts the US in a very powerful position** in this regard. It would therefore require other strategic or altruistic motives for the United States to agree to international cybersecurity rules it has not tailor-made. This is a risky assumption for others to make.

⁵³ Élise Vincent, “France’s cyber defense force questions role of US support in Europe”, *Le Monde*, January 15, 2023, https://www.lemonde.fr/en/international/article/2023/01/15/france-s-cyber-defense-force-questions-the-role-of-us-support-in-europe_6011684_4.html

⁵⁴ Assemblée nationale, *Compte rendu : Commission de la défense nationale et des forces armées*, Compte rendu no 27, December 7, 2022, https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/cion_def/16cion_def2223027_compte-rendu.pdf, p. 8.

⁵⁵ China Virus Emergency Response Center, cited by Roger Creemers, <https://eucyberdirect.eu/research/china-s-digital-policies-in-its-new-era>, p. 35.

⁵⁶ The White House, *National Cybersecurity Strategy*, March 1, 2023, <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

There are reasons, not always good, for this European approach to be limited to defensive options. National security and defense should be a common denominator, except that it is not a European prerogative, even on the basis of delegation. It is only among Member States that rules such as the e-evidence package designed to fight crime do represent an extra-territorial step – within the EU. **Extraterritorial jurisdiction is not an accepted concept, despite the “Brussels effect” on foreign legislations. On the contrary, it is often considered an unacceptable American prerogative.** Others, with some exaggeration, do call Europe’s GDPR and insistence on privacy “an extraterritorial jurisdiction model”.⁵⁷ At best, this is passive sovereignty relying on the power of the European market base.

We must therefore clarify what is meant by sovereignty in the digital area. Is it the power to regulate, which by definition should be shared if one is taking into consideration cross-border data? Is it control over data, a notion that can be challenged by privacy advocates against the state, and a goal which balances against efficiency? Does data security include stored data or also the algorithms and the software analyzing this data and drawing conclusions? Is it the hardware supply chain that transports and stores data, and are we talking then about cybersecurity and legal security, or do we include economic goals such as a share of the IT equipment down to semiconductors? There are also varying definitions of critical data. From national security to intellectual rights for innovations to marketing data, and again onwards to sensitive personal data such as health records, banking data but also all sorts of behavioral records that can create an exact portrait of an individual, **the scale of control ceaselessly grows. And the frontier is constantly shifting between critical and routine data.** New algorithms appear; new data banks may be aggregated and recombined, and deanonymization may occur, not to mention the promises of quantum physics to unlock any encryption some time in the future.

⁵⁷ Yik-Chan Chin and Jingwu Zhao, “Governing Cross-Border Data Flows: International Trade Agreements and Their Limits”, *Laws*, Vol 11, Issue 4, 2022, p.5, <https://www.mdpi.com/2075-471X/11/4/63>

3.2. CHASING THE RIGHT DEGREE OF SOVEREIGNTY

It appears, therefore, that **there is no one-size-fits-all solution or radical choice for sovereignty**. Even the most sensitive national security data needs more than a hosting safe vault. It may also require apps and algorithms with enough calculating power to perform complex operations. This may involve an external or foreign supplier. There is almost no data regarding human activity or environmental issues (another apparently innocuous domain), which cannot be recombined.

What precedes would suggest that self-reliance and an integral soft and hard supply chain with very limited cross-border transfers are the only solution. It is out of reach by definition within the European Union, where **no Member State has by itself the necessary scale for investment, innovation, and market, and where pooling at the European level is a prerequisite** in many cases for effectiveness. To quote the former director of France's National Agency for Information Systems Security (ANSSI), "We are currently not able to create high-level clouds in France with technologies developed exclusively in France".⁵⁸ This is a key reason why, on digital issues, sovereignist advocacy has moved from the national to the European level. Sovereignists now advocate "*l'Europe puissance*" in this case, and in France they argue at the European level for a "strategic autonomy" that was originally defined with French national defense criteria: "an autonomous capacity of judgment, decision and action". This leads them down a path where they rather uncharacteristically advocate European reforms and more power to the EU, while urging leading European states to "reconsider the very notion of what "allied" means".⁵⁹

⁵⁸ Originally published in French, "Nous ne sommes pas capables de faire du cloud de haut niveau en France aujourd'hui avec des technologies exclusivement françaises développées en France". Michel Cabriol, "« Sur le cloud de confiance, on ne parle pas de souveraineté absolue » (Guillaume Poupard, Anssi)", *La Tribune*, October 8, 2022, <https://www.latribune.fr/entreprises-finance/industrie/aero-nautique-defense/sur-le-cloud-de-confiance-on-ne-parle-pas-de-souverainete-absolue-guillaume-poupard-935510.html>

⁵⁹ Jennyfer Chretien and Etienne Drouard, "La Souveraineté technologique européenne", *Renaissance Numérique*, January 13, 2022, <https://www.renaissancenumerique.org/publications/la-souverainete-technologique-europeenne/>

Independence is a commendable path, but also one that is unrealistic even in a mid-term perspective. For all its qualities, Europe moves slowly, with a deliberative process that is not only between branches of the European institutions, but also with and among Member States, their domestic constituencies and varied interests. The very strength of European commitments to values such as data privacy and personal rights means that **the legal hurdles for reforms that would speed up the process of innovation and scaling up the digital sector are larger than anywhere else**. This is the not so hidden negative side of the power to regulate and its "Brussels effect". To stay within the limits of the digital and IT sectors, there is as yet no unified telecom market, and rules of the game differ from one Member State to another. Free roaming is the counterexample, but this is an exception that has been sold and resold to the general public. For data regulation, companies and clients must contend with 27 national data boards in addition to the European Data Protection Board (EDPB) that was created following the GDPR.

Digital sovereignty, strategic autonomy, or even resilience cannot be achieved without sequential steps and the conjunction of public decisions and investment, a market competition that ensures a level-playing field and picks winners, something that is very rarely in the hands of governments. It requires laying bricks in many areas, and all of this will be undertaken as others benefit from the advantage of having been first movers and the scale of the investment they have already deployed.

"It is notable how fast that some European policy-makers are jumping to the conclusion that radical measures are needed to create notional data sovereignty, reinforcing a misguided view that in order to create a greater digital autonomy, Europe must close itself off from the rest of the world".⁶⁰ The reason **many politicians have jumped on the sovereignty bandwagon**

⁶⁰ Matthias Bauer and Fredrik Erixon, "Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls", *European Centre for International Political Economy*, No.02, 2022, https://ecipe.org/wp-content/uploads/2020/05/ECI_20_OccPaper_02_2020_Technology_LY02.pdf

is that it appeals to voters and to their fantasies about globalization, big brothers lurking at every corner of the digital sector, and fantasies about hyperscalers and the hegemony they provide for America – and China.

3.3. THE SINGLE DIGITAL SPACE VERSUS NATIONAL SOVEREIGNTY DILEMMA

While there is a trend to criticize the Biden administration's creation of a Data Protection Review Court as an ancillary justice within the executive branch, how independent are Europe's 27 data protection boards? What about the fragmentation of oversight and control authorities between 27 digital spaces? What about the dilemma between the requirements of European intelligence services and personal data protection?

Strikingly, the **EU ePrivacy Regulation draft now includes a full exemption from oversight by the European Court of Justice for data collection in the name of national security and defense**, including requests to private operators.⁶¹ Different from the 2002 ePrivacy Directive, it is a regulation that will have a direct effect in all EU Member States, without the need of transforming it into national legislation. France has also petitioned its own higher administrative Court (*Conseil d'État*) to invalidate a CJEU ruling on a case introduced by a French NGO because the Court was exceeding EU prerogatives by including national security issues in its decision. While refusing to assess the prerogatives of the CJEU, the French administrative Court invalidated its ruling on a key issue: the conservation of metadata in cases involving national security, serious crime, "radical or extremist groups (...) industrial spying or sabotage, reputational attacks and expert poaching" (*sic, "débauchage d'expert"*).⁶²

⁶¹ Theodore Christakis and Kenneth Propp, "How Europe's Intelligence Services Aim to Avoid the EU's Highest Court - and What It Means for the United States", *Lawfare*, March 8, 2021, <https://www.lawfareblog.com/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states#>

⁶² *Conseil d'État, Assemblée, 21/04/2021, 393099, Publié au recueil Lebon*, April 21, 2021, § 44, <https://www.legifrance.gouv.fr/ceta/id/CETATEXT000043411127>

It is beyond the scope of this note to opine on a court case involving data privacy and national security. What matters here is that the CJEU does not have final say. Two aspects broadly intersect the cross-border data issue. One, the French administrative court ruling, much like Germany's Constitutional Court rulings on public deficits, limits the oversight at the European level – and, in fact, **entrusts oversight to an administrative jurisdiction, much like the Biden executive order on signals intelligence**. Two, this also impairs the possibility of any transatlantic agreement on data flows at an EU level, raising again the issue of differences in treatment among Member States. One familiar complaint with US legislation and the CLOUD Act was that it offered far fewer guarantees and recourse to foreign citizens compared to US citizens. The White House executive order requires reciprocity in data protection from partners abroad. But strangely, the proposed e-privacy draft would offer fewer guarantees to EU citizens than comparable US legislation does for US citizens. Whatever the motives, this raises questions that one could sum up as follows: while we do not want other (non-EU) gentlemen to read our people's mail, some of us (EU) gentlemen are happy to do so under a broad definition of due cause.

The dilemma between a single digital space and national sovereignty runs everywhere, including in the recently adopted Digital Services Act, which states that in a cross-border context, orders to act against illegal content "should in principle be limited to the territory of the issuing Member State, unless the illegality of the content derives directly from Union law or the issuing authority considers that the rights at stake require a wider territorial scope" (Recital 36).⁶³

Precautionary principles are indeed needed. It is conceivable that America's National Security Agency (NSA) or China's Ministry of State

⁶³ European Parliament and the Council, "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)", PE/30/2022/REV/1, October 27, 2022, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014>

Security (with less access to global data) recombine much of the world's digital data to reach actionable decisions – much as weather prediction has become more accurate with the help of gigantic calculating power. But on the other side of the issue, do we consider accurately the disadvantages and losses that come from our own limited, often dysfunctional access to data? This limited access may be for the best reasons in the world, such as personal data protection, or for less commendable motives such as companies and even individuals holding on to proprietary information rather than cooperating for the common good. Or, in the worst case, simply from bureaucratic incompetence and indifference. In the case of France, several knowledgeable observers point out that the difficulties and possibly the failure of a Health Data Hub hinge not so much on the initial choice of Microsoft as the operator, but on the reluctance of various health institutions to share their data, using Microsoft as a scapegoat. A more general case can be made with data collection and AI algorithms. Hampering both, or putting many ex ante obstacles in their way – rather than self-assessment and ex post control – will limit the ability of companies operating from the European database market to innovate and keep level with other regions, and will incite these companies to invest elsewhere. **Certification, self-assessment and ex post control, and in some cases “regulatory sandboxes” allowing innovation and trial uses of AI in a controlled way are important to consider.**

The recent spate of regulatory acts and guidelines by the Commission shows that it is well aware of these pitfalls. **It seeks to navigate between the promotion of free data flows, the protection of personal and increasing non-personal data and the needs for innovation.** GDPR was a major step in creating a level playing field of rules for all companies, European and non-European. More recent regulations aim directly at evening the capacities in play, between first movers with a huge acquired

⁶⁴ Frances G. Burwell and Kenneth Propp, “Digital Sovereignty in Practice: The EU’s Push to Shape the New Global Economy”, Atlantic Council, October 2022, <https://www.atlanticcouncil.org/wp-content/uploads/2022/11/Digital-sovereignty-in-practice-The-EUs-push-to-shape-the-new-global-economy.pdf>

advantage, and more recent entrants. While an Atlantic Council report⁶⁴ levels charges of digital discrimination, protectionism and unilateralism at Europe, Digital Europe asserts “a legal maze of new and existing rules to govern data transfers and access of non-personal data by non-EU governments. This regulatory uncertainty will be damaging to data-intensive industries.”⁶⁵

While there is some truth in this statement when one considers the many jurisdictions and boards that have been created, it is also a paradox. One of the main complaints in the digital sector was that **GDPR was too much of a top-down, logical law construction to fit very different situations.** Instead, hyperscalers and other large American digital companies have now turned to approval of a unitary approach that makes for consistent rules across a single digital space – even with all the caveats mentioned above about implementation. In Mark Zuckerberg’s words, “it would be good for the internet if more countries adopted regulations such as GDPR as a common framework.”⁶⁶

One knowledgeable observer explains that **the hyperscalers are putting their best face on new regulation – for instance, now the Digital Market Act – while using massive legal resources to find and exploit loopholes.** It is of course notable that Meta is at the same time a company which seems to have consistently sought to escape GDPR requirements on consent and cookies, as shown by the proceedings unfolding with the EDPB and the Irish Data Protection Commission (DPC) in 2022, leading to a 390 million euro fine. In addition, triggered by the “Schrems II” ruling by the CJEU, the Irish DPC initiated an inquiry in 2020 into the legality

⁶⁵ Digital Europe, “Data transfers in the data strategy: Understanding myth and reality”, June 16, 2022, <https://www.digitaleurope.org/resources/data-transfers-in-the-data-strategy-understanding-myth-and-reality/>

⁶⁶ Mark Zuckerberg, “Mark Zuckerberg: The Internet Needs New Rules. Let’s Start in these Four Areas.”, *Washington Post*, March 30, 2019, https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html

of Meta's personal data transfers from the EU to the US through its use of standard contractual clauses. On April 13, 2023, the EDPB announced that the dispute had been resolved, although the actual ruling has yet to be published.⁶⁷ It is reported that it will reaffirm the Irish draft decision to ban Meta's data transfer from the EU to the US under an SCC agreement.⁶⁸

3.4. A SCIENCE AND TECHNOLOGY BASED DEVELOPMENT APPROACH

As it advances, **European regulation moves to specific sectors and issues, while enlarging its scope to encompass new developments such as clouds and AI.** On non-personal data, the EU adopted in 2018 a regulation on free flow inside the bloc. This would cover non-personal data such as “aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimize the use of pesticides and water, or data on maintenance needs for industrial machines.”⁶⁹

Thierry Breton's own statements praise industrial policy, asking that Europe produce “the most powerful computers in the world”, store and process data in Europe: on data localization, he has been cited as saying “the Chinese and Russians are doing it, we'll do it too.”⁷⁰ These declarations

⁶⁷ European Data Protection Board, “EDPB resolves dispute on transfers by Meta and creates task force on Chat GPT”, April 13, 2023, https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en

⁶⁸ Reuters, “Irish regulator has month to make order on EU-US Facebook data transfers”, April 13, 2023, <https://www.reuters.com/technology/irish-regulator-has-month-make-order-eu-us-facebook-data-transfers-2023-04-13/>

⁶⁹ European Parliament and the Council, “Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union”, PE/53/2018/REV/1, November 18, 2018, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>

⁷⁰ Hugues Garnier, “Thierry Breton: “Je souhaite que les données des Européens soient et stockées en Europe””, *BFM Business*, August 25, 2020, https://www.bfmtv.com/economie/thierry-breton-je-souhaite-que-les-donnees-des-europeens-soient-traitees-et-stockees-en-europe_AD-202008250281.html

are balanced in areas under her purview by Margrethe Vestager, and the word “open” figures in literally every EU statement on digital issues. Still, the **Commission's move to regulate is not only motivated by data protection, fighting anti-competition behavior or considerations on public order.** A recent assessment suggests that a form of regulatory mercantilism is at stake.⁷¹ Past common market policies on agriculture and trade, the European Coal and Steel Community, did include companies operating from a different base and a large degree of protection – in a very different global trading environment.

A major goal today is to tap the huge pools of data that are largely unused in Europe. At present, a double standard often prevails. Pharma companies and other sectors needing personal data will often buy it in the United States – or China in some cases. Having radical regulatory requirements in the European Union can backfire against innovation and advantage cloud service operators who refrain from re-selling their data in Europe while having different practices in the United States. The emphasis is moving towards non-personal data, AI and pooling. **New rules prevent data localization within one Member State and vendor lock-in** (where users cannot leave easily or costlessly a provider), **facilitate and even promote the sharing of public data with the proper guardrails.**

This includes two parallel developments: non-personal data transfer is to follow rules that mirror the GDPR on personal data, including with adequacy decisions. **Not only is the EU taking into account the CJEU's Schrems II ruling, but it is adding non-personal data.** This will put European and non-European firms under the same constraints. Anonymization and pseudonymization for personal data are accepted as a basis for transfer and treatment, again with guardrails, which should open new prospects for the transport and energy sectors' sobriety measures and demand management (health being dealt with a separate regulation).

⁷¹ Pascal D. König, “Fortress Europe 4.0? An analysis of EU data governance through the lens of the resource regime concept”, *European Policy Analysis*, Vol 8, Iss 4, 2022, pp.484-504, <https://doi.org/10.1002/epa2.1160>

In the other direction, personal data can now be transferred through “altruistic” intermediaries, making the data available without cost for research. Similarly, the AI regulation promotes both privacy and transparency (on algorithms), enhancing a European AI market which could be separate from the global market.

As to legal security, the proposed **European Union Cybersecurity Certification Scheme for Cloud Services (EUCS)**, the first certificate under the EU’s Cybersecurity Act, not only requires a foreign company to have an affiliated subsidiary or a legal representative in Europe, but also that providers of cloud services be headquartered in Europe and not be controlled – directly or indirectly, individually or collectively – by any non-EU entities.⁷² The new requirement, reportedly⁷³ pushed forward by France, Germany, Italy and Spain, while opposed by countries like the Netherlands,⁷⁴ follows the French model (SecNumCloud)⁷⁵ for clouds, and provides immunity from extra-European legislation under the heading of Art 19.6. From the Snowden case to the multiple extraterritorial laws that the United States enforces through the international system, **legal security has become a key factor in advocating European digital sovereignty.**

Technological developments are also sought. Encryption or tokenization of data allows work while keeping the data unreadable by cloud operators.

⁷² Digital Europe “Data transfers in the data strategy: Understanding myth and reality”, June 16, 2022, <https://www.digitaleurope.org/resources/data-transfers-in-the-data-strategy-understanding-myth-and-reality/>

⁷³ Laura Kebelka, “Sovereignty requirements remain in cloud certification scheme despite backlash”, *Euractiv*, June 16, 2022, <https://www.euractiv.com/section/cybersecurity/news/sovereignty-requirements-remain-in-cloud-certification-scheme-despite-backlash/>

⁷⁴ Luca Bertuzzi, “EU countries seek way out of impasse on sovereignty requirements for cloud services”, *Euractiv*, January 30, 2023, <https://www.euractiv.com/section/cybersecurity/news/eu-countries-seek-way-out-of-impasse-on-sovereignty-requirements-for-cloud-services/>

⁷⁵ Agence nationale de la sécurité des systèmes d’information, *Prestataires de services d’informatique en nuage (SecNumCloud)*, March 8, 2022, <https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud-referentiel-exigences-v3.2.pdf>

3.5. LESSONS

Unquestionably, **there is a plurality of motives in the quest for digital sovereignty.** A single market that has lagged behind in digital development is bound to adopt elements of a catch-up economic policy, while the leader’s advantage and the de facto localization that it has achieved – software, apps, platforms and hyperscalers, storage, public-private cooperation – allow it to pursue free data flows from this position.

There are strong arguments on both sides of the Atlantic to avoid a slide from this divergence of interests into a more fragmented transatlantic space. Some of the European arguments against extra-territorial jurisdiction are real, but they would be more convincing to the United States if Europe itself possessed some extra-territorial capacity in this regard apart from the “Brussels effect”. Conversely, the lack of European digital champions, its present dependence on non-European technology and software providers, the dispersion of private actors that has been found also in the banking, telecom and defense sectors, are true impediments. They should not only prevent, but actually require, that **public decision-makers keep moving to facilitate a bottom-up mobilization of resources.** As we shall see, this involves better dynamics between public and private actors, more shared resources, education and skills training and targeted immigration policies. **There must be an overall change in European mentalities that would prioritize science and technology based developments over a defensive approach based on mistrust and a recurring preference for the precautionary principle.** Any kind of data sovereignty – without the emphasis on the constitutional definition of a term that simply lacks a sovereign at the European level to be fully exercised – can only be achieved by a building blocks approach.

4 China's pursuit of digital sovereignty

With regards to data protection and cybersecurity, **three major pieces of legislation** have been introduced in China in recent years: the 2017 Cybersecurity Law (网络安全法), the 2021 Data Security Law (数据安全法) and the 2021 Personal Information Protection Law (个人信息保护法). Together, they provide us with a general direction on cross-border data transfers.

China's **Cybersecurity Law (CSL)**⁷⁶ is formulated to satisfy a wide range of goals: to ensure cybersecurity; to safeguard cyberspace sovereignty and national security, and social and public interests; to protect the lawful rights and interests of citizens, legal persons, and other organizations; and to promote the healthy development of the informatization of the economy and society.⁷⁷ It requires, without specifics, national operators to provide technical support and assistance to the public security and state security organs in their activities related to safeguarding state security and crime investigation (Article 28). It also mandates that **personal information and important data collected and generated by critical information infrastructure operators within China to be stored within the country, and a security assessment to be conducted for truly necessary outward data transfer** (Article 37). Due to the de facto requirements for **data localization**, many non-Chinese tech firms were forced to shift their Chinese users' data into domestic data centers. Apple complied, and has apparently ceded control of its data to its Chinese state-owned counterparts in 2018.⁷⁸

⁷⁶ Cyberspace Administration of China, *Cybersecurity Law of the People's Republic of China* (中华人民共和国网络安全法), November 7, 2016, http://web.archive.org/web/20230405075551/http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

⁷⁷ Rogier Creemers, Graham Webster, and Paul Triolo, "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)", *DigiChina*, June 29, 2018, <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>

⁷⁸ Nick Statt, "Apple's iCloud partner in China will store user data on servers of state-run telecom", *The Verge*, July 18, 2018, <https://www.theverge.com/2018/7/18/17587304/apple-icloud-china-user-data-state-run-telecom-privacy-security>

For its part, AWS has partnered with two companies in Beijing and Ningxia,⁷⁹ whereas Microsoft Azure cloud services are hosted on Beijing-based 21Vianet's data centers.⁸⁰ Data localization requirements have helped China's domestic data center industry flourish, as large multinationals work with local firms in joint ventures to run data centers in China. 80% of China's domestic cloud computing market is taken by its own top four cloud suppliers: Alibaba Cloud (36%), Huawei Cloud (19%), Tencent Cloud (16%) and Baidu AI Cloud (9%).⁸¹ Five years after it took effect, the Cyberspace Administration of China published in September 2022 a draft decision to amend the law to better align with other relevant laws released after 2017.⁸²

The **Data Security Law (DSL)**⁸³ fills the gap left by the cybersecurity law, which only governs cyber data, by addressing all types of data and establishing a system of data classification. It also broadened China's extraterritorial reach by applying the law to **any overseas data processing that jeopardizes the national security, public interests, or the lawful rights and interests of individuals or organizations of China** (Article 2). It is generally seen as a response to the US CLOUD Act and prohibits providing of data stored in China to any foreign judicial or law enforcement body without the prior approval of the relevant PRC authorities (Article 36). Interestingly, the DSL also authorizes China to take

⁷⁹ Amazon Web Services, "Amazon Web Services in China", <https://www.amazonaws.cn/en/about-aws/china/>

⁸⁰ Microsoft, "Microsoft Azure in China", August 5, 2020, <https://docs.microsoft.com/en-us/azure/china/overview-operations>

⁸¹ "Cloud services spend in China hit US\$7.8 billion in Q3 2022", Canalis, <https://www.canalys.com/newsroom/china-cloud-market-Q3-2022>

⁸² Cyberspace Administration of China, "Notice of Public Consultation on the Decision on Amending the Cybersecurity Law of the People's Republic of China (Draft for Comments) (关于公开征求《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》意见的通知)", September 14, 2022, http://web.archive.org/web/20220915034645/http://www.gov.cn/xinwen/2022-09/14/content_5709805.htm

⁸³ National People's Congress of the People's Republic of China, *Data Security Law of the People's Republic of China*, June 10, 2021, <http://web.archive.org/web/20230123094630/http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml>

countermeasures in response to any discriminatory prohibitions against China in respect of investment, trade or any other field related to data and data development and utilization technologies (Article 26).

The **Personal Information Protection Law (PIPL)**⁸⁴ is said to be “China’s GDPR”. Although it might share some of the languages of the GDPR, it is a whole different animal. For instance, the PIPL provides undefined exceptions for the personal information handling activities of State organs (Articles 44 & 45). In addition, although it applies to both public and private organizations, it lacks an independent authority overseeing the enforcement of the law. Instead, it stipulates an internal oversight mechanism. In the case of cross-border transfer of personal information, similar to the GDPR, the PIPL provides a list of allowed channels for cross-border data transfer out of China (Article 38): security assessment, standard contractual clauses (SCCs), and security certification, and other conditions set forth by laws and administrative regulations or by the national cyberspace department. However, **it provides for a much shorter list of permissible grounds for outbound data transfer compared to the GDPR**, which also provides a list of derogations for specific situations (Articles 49) as a subsidiary vehicle to transfer of personal data.

On July 21, 2022, after a year-long investigation, the Cyberspace Administration of China (CAC) announced an 8 billion yuan (approx. 1.16 billion euros) fine on **Didi Global** for violating China’s three major data protection laws – CSL, DSL and PIPL – for seven years, since June 2015. The investigation started right after Didi’s initial public offering on the New York Stock Exchange (NYSE) in July 2021. It is reported that Didi pushed ahead with its New York IPO without completing a CAC security assessment, which was not yet an institutional part of the listing process.⁸⁵

⁸⁴ National People’s Congress of the People’s Republic of China, *Personal Information Protection Law of the People’s Republic of China*, December 29, 2021, http://web.archive.org/web/20221013152625/http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559_2.htm

⁸⁵ Coco Feng et al., “Didi Chuxing ‘forced its way’ to a New York listing, triggering data security review, sources say”, *South China Morning Post*, July 6, 2021, <https://www.scmp.com/tech/policy/article/3140044/didi-chuxing-forced-its-way-new-york-listing-triggering-data-security>

Beijing was worried that the listing could grant American regulators access to sensitive Chinese data.⁸⁶ Didi delisted from NYSE in June 2022. The revised 2022 **Cybersecurity Review Measures** (网络安全审查办法) **made cybersecurity review a requisite for online platform operators holding more than one million users’ personal information before listing on foreign markets** (Article 7).⁸⁷ It also added “foreign governments’ influence, control or malicious use of critical information infrastructure, core data, important data or a large amount of personal information due to the listing” to the assessment factors with a national security impact (Article 10.6).

China’s legal framework for data protection and cybersecurity has continued to develop through various regulations and standards that add details and specifications. Among them, the following ones are key to navigating the issue of cross-border data transfer and provide details about the three conditions listed under PIPL:

- The Security Certification Guidelines on Cross-border Transfer of Personal Data (网络安全标准实践指南 – 个人信息跨境处理活动安全认证规范) from June 2022 applies to intra-group transfer by a data exporter located in China. It shares similarities with the BCR under article 47 of the GDPR, but goes one step beyond as it requires disclosure of the identity of the third country. The updated version issued in December 2022 with immediate effect expanded its application scope by including onward transfer of personal data beyond the group.
- The Cyberspace Administration of China released **the Measures for Security Assessment of Cross-border Data Transfer** (数据出境安全评

⁸⁶ Cissy Zhou, “Didi to exit NYSE on June 10 amid uncertainty about China restart”, June 9, 2022, <https://asia.nikkei.com/Business/Transportation/Didi-to-exit-NYSE-on-June-10-amid-uncertainty-about-China-restart>

⁸⁷ Cyberspace Administration of China, “Cybersecurity Review Measures (网络安全审查办法)”, January 4, 2023, http://web.archive.org/web/20220809065220/http://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm

估办法)⁸⁸ in July 2022 and the **Guidelines on Application for Security Assessment of Cross-border Data Transfers – 1st Edition** (数据出境安全评估申报指南 – 第一版)⁸⁹ the following month. Both went into effect in September 2022, with March 1 as the deadline for the ratification of previous non-compliant transfers. It provides details for security reviews for cross-border data transfer under Article 38 of PIPL. Under the new rules, a security review is mandatory for a firm that handles the personal information of more than 1 million Chinese residents, that have exported personal information of 100,000 people or sensitive personal information of 10,000 people since 2021.

- The **Provisions on the Standard Contract for Cross-border Transfer of Personal Information** (个人信息出境标准合同办法)⁹⁰ issued in February 2023 specify the rights and obligations of exporters and their recipients abroad. The Provisions are accompanied by a standard contract template, which is considered the Chinese equivalent of the EU's Standard Contractual Clauses.

In January 2023, China's first case of security assessment for data export was approved, which concerns a collaborative research project between a Beijing-based hospital and an Amsterdam-based university medical center.⁹¹ **Due to the low threshold and broad scope, the applicability of the regulation is very wide, creating burdensome reporting obligations for companies.** And some companies are concerned about

⁸⁸ Cyberspace Administration of China, "Measures for Security Assessment of Cross-border Data Transfer (数据出境安全评估办法)", July 7, 2022, http://web.archive.org/web/20230315031231/http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm

⁸⁹ Cyberspace Administration of China, "Guidelines on Application for Security Assessment of Cross-border Data Transfers – 1st Edition (数据出境安全评估申报指南 第一版)", August 31, 2022, http://web.archive.org/web/20221019182119/http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm

⁹⁰ Cyberspace Administration of China, "Provisions on the Standard Contract for Cross-border Transfer of Personal Information (个人信息出境标准合同办法)" <http://archive.today/GTgtZ>

⁹¹ Global Times, "China's first case of data export security assessment for data export approved in Beijing", January 18, 2023, <http://web.archive.org/web/20230201001801/https://www.globaltimes.cn/page/202301/1284015.shtml>

disclosing information concerning companies' overseas technology infrastructure and personnel involved in data transfers, which are required during the security assessment. The International Air Transport Association (IATA) called for an extension of the deadline.⁹²

Due to the burden carried by Beijing's restrictions on cross-border data flow, Hong Kong is trying to create a mechanism with the Cyberspace Administration of China (CAC) that allows data transfer from mainland China to Hong Kong, with the condition that the data will not be transferred further and leave Hong Kong.⁹³ According to Allen Yeung, founding chairman of the Institute of Big Data Governance (iBDG), **China's data export compliance requirements demand "quite a lot of work,"** "many big companies are having a hard time processing it, let alone small and medium-sized enterprises".

Many government departments are involved in data regulation in China. The former chairman of the China Securities Regulatory Commission (CSRC) also highlighted this inefficiency, noting that **there were about 15 government departments holding regulatory power over data in China.**⁹⁴ In March 2023, a coordinating authority, the National Data Bureau, was created.⁹⁵ Placed under the National Development and Reform Commission, its appearance coincides with the publicity now given to a national cyber strategy.

⁹² Raffaele Huang, "American Firms Race to Meet China's Data Rule Deadline", *Wall Street Journal*, March 1, 2023, <https://www.wsj.com/articles/china-data-transfer-law-adds-to-strains-on-multinationals-91b9764f>

⁹³ Xinmei Shen "Hong Kong in talks with Beijing to ease cross-border data flow as new rules threaten city's gateway status", *South China Morning Post*, July 24, 2022, <https://www.scmp.com/tech/policy/article/3186094/hong-kong-talks-beijing-ease-cross-border-data-flow-new-rules-threaten>

⁹⁴ People's Political Consultative Daily, "Enhancing the contribution of data elements to economic growth (提高数据要素对经济增长的贡献度)", February 15, 2022, <http://web.archive.org/web/20230322225740/http://www.rmzxb.com.cn/c/2022-02-15/3049320.shtml>

⁹⁵ Xinhua, "The Communist Party of China (CPC) Central Committee and the State Council's release of Party and state Institutional Reform plan (中共中央 国务院印发《党和国家机构改革方案》)", March 16, 2023, http://web.archive.org/web/20230316104523/http://www.news.cn/politics/zywj/2023-03/16/c_1129437368.htm

An adverse result, pointed out for example in the international banking sector, is that **“if nothing can leave, nothing comes in”**: almost universally, banks establish their back offices in India, rather than in China. That echoes the analysis of Chen Hongna from the Development Research Center of the State Council.⁹⁶ She notes that China's current data flow regulatory efforts focus on "protection 防", but there is a lack of means to serve Chinese companies in transferring data from abroad back to China. He concludes that an overly strict regulatory mechanism may objectively "block 堵" the data outside the country.

Adding to the above complication is the “notorious” **2017 National Intelligence Law** (国家情报法, amended in 2018), especially its Article 7, which is interpreted as legalizing all intelligence gathering activities of the government and making it an obligation for any organization or citizen to cooperate with intelligence requests. The law has been at the heart of the TikTok discussion, both in Europe and in the US.

It should be noted that TikTok has risen to an unprecedented level of use, especially among the young, because its algorithms are extremely sophisticated, creating consumer addiction.

On February 23, 2023, the European Commission **suspended the use of TikTok** on its corporate devices and on personal devices enrolled in the Commission mobile device service **“to protect the Commission against cybersecurity threats and actions which may be exploited for cyber-attacks against the corporate environment of the Commission”**.⁹⁷ The European Council followed suit on the same day. Several European governments have also taken action against TikTok.⁹⁸ Back in November 2022, TikTok revealed a Privacy Policy Update which applies to

⁹⁶ Chen Hongna, “The US-China Digital Economy Competition and China's Responding Approaches (中美数字经济博弈及中国的应对思路)”, February 28, 2022, <http://web.archive.org/web/20220516142232/https://www.chinathinktanks.org.cn/content/detail?id=glve8784>

⁹⁷ European Commission, “Commission strengthens cybersecurity and suspends the use of TikTok on its corporate devices”, Press release, February 24, 2023, https://ec.europa.eu/commission/presscorner/detail/en/IP_23_1161

the European Economic Area, the UK and Switzerland. It acknowledges that while its European user data is currently stored in the US and Singapore, it can be remotely accessed by certain employees located in China and a number of other countries, “based on a demonstrated need to do their job” and through methods recognised under the GDPR.⁹⁹

In an attempt to prevent further EU bans, in March 2023, TikTok unveiled a plan, known as Project Clover, which promises the introduction of “a number of new measures to strengthen existing protections” and further alignment of its “data governance with the principle of European data sovereignty”.¹⁰⁰ It also announces its commitment to store European TikTok user data locally, with the process starting this year and continuing into 2024. **TikTok has been the subject of an ongoing investigation by Ireland's Data Protection Commission since September 2021, following concerns over the platform's potential transfer of EU users' data to China in violation of the EU GDPR.**

On the other side of the Atlantic, the US has put a series of bills on the table since late 2019 to constrain TikTok. Most recently, on March 7, the White House backed a bipartisan bill called the Restricting the Emergence of Security Threats that Risk Information and Communications Technology (RESTRICT) Act. The bill would enable the US Commerce Department to impose restrictions and ban technologies from China, Russia, North Korea, Iran, Venezuela and Cuba that pose national security risks, including TikTok.¹⁰¹ Earlier in December 2022, the US congress passed a bill

⁹⁸ Politico, “Mapped: TikTok faces bans, blocks and probes across Europe”, March 5, 2023, <https://www.politico.eu/article/mapped-tiktok-faces-bans-probes-blocks-across-europe-security-privacy/>

⁹⁹ Elaine Fox, “Sharing an Update to our Privacy Policy”, *TikTok*, November 2, 2022, <https://newsroom.tiktok.com/en-gb/an-update-to-our-privacy-policy>

¹⁰⁰ TikTok, “Setting a new standard in European data security with Project Clover”, March 8, 2023, <https://newsroom.tiktok.com/en-ie/project-clover-ireland>

¹⁰¹ The White House, “Statement from National Security Advisor Jake Sullivan on the Introduction of the RESTRICT Act”, March 7, 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/07/statement-from-national-security-advisor-jake-sullivan-on-the-introduction-of-the-restrict-act/>

containing a provision banning TikTok on federal government devices. A current arrangement under discussion, known as Project Texas, proposes the creation of a local company, with data flows supervised by Oracle, and gives the final say to CFIUS,¹⁰² which could ask Byte Dance, TikTok's parent company, to divest its investment. This demand was reportedly made by the White House on March 15, 2023, according to TikTok executives¹⁰³. However, Project Texas is not fully operational. For the time being, Byte Dance's engineers continue to have access to TikTok data, as confirmed by the TikTok CEO during a recent US congressional hearing.¹⁰⁴

Suspicion goes both ways. In 2021, China restricted the use of Tesla cars by military staff and employees of key state-owned companies, citing national security concerns caused by data collection by cameras on the cars.¹⁰⁵ But a Chinese company, Quectel, supplies IoT cellular modules to many Tesla cars, and in the UK, similar IoT modules have been found to include sealed geolocation devices in government cars.

In 2020, China announced its own initiative to set global standards on data security, in an attempt to counter the US Clean Network effort, or to contribute "Chinese wisdom to international rules-making" on data governance in Chinese official wording. As all the other initiatives proposed by China, the **Global Initiative on Data Security** is short on details, leaving China with flexibility to fill in details as the time goes by.

¹⁰² Matt Perault and Samm Sacks, "Project Texas: The Details of TikTok's Plan to Remain Operational in the United States", *Lawfare*, January 26, 2023, <https://www.lawfareblog.com/project-texas-details-tiktoks-plan-remain-operational-united-states>

¹⁰³ David McCabe and Cecilia Kang, "U.S. Pushes for TikTok to Resolve National Security Concerns", *The New York Times*, March 15, 2023, <https://www.nytimes.com/2023/03/15/technology/tiktok-biden-pushes-sale.html>

¹⁰⁴ Transcript: TikTok CEO Testifies to Congress, Tech Policy Press, March 24, 2023, <https://techpolicy.press/transcript-tiktok-ceo-testifies-to-congress/>

¹⁰⁵ Shunsuke Tabeta, "China bans use of Tesla by military, citing security concerns", *Nikkei Asia*, March 19, 2021, <https://asia.nikkei.com/Politics/International-relations/US-China-tensions/China-bans-use-of-Tesla-by-military-citing-security-concerns>

The Initiative gained support from ASEAN¹⁰⁶ and the League of Arab States (LAS) though.¹⁰⁷ The China-Russia "no limit" partnership is likewise evident in this realm, with the Russian support of the initiative inked by a February 2022 joint statement, noting that "any attempts to limit their sovereign right to regulate national segments of the Internet and ensure their security are unacceptable".¹⁰⁸ However, **China has yet to reach a treaty with major economies regarding cross-border data transfer.**

China's sale of surveillance technology is an important concern for cross-border data flows. According to a private census, 6.3 million camera networks have been installed abroad by two Chinese companies, Hikvision and Dahua, with Vietnam, the United States, Mexico and the UK topping the list.¹⁰⁹ In November 2022, the Federal Communications Commission (FCC) banned five Chinese companies, Huawei, ZTE, Hikvision, Hytera, and Dahua, from the American market. Even more broadly, Huawei claims to have created 700 "smart city" networks in over 100 countries, a claim many believe to be exaggerated.¹¹⁰ In many cases, these include facial recognition systems and AI processing to detect, for example, loitering or crowds, or what can be termed "an autocrat's toolkit". There are also indications that China is ready to export digital macro-economic tools under the **Thousand Cities Strategic Algorithms**

¹⁰⁶ Ministry of Foreign Affairs of the People's Republic of China, "ASEAN highly values the Global Data Security Initiative proposed by China (东盟高度重视中方提出的《全球数据安全倡议》)", September 9, 2020, <https://archive.ph/kSZAm>

¹⁰⁷ Ministry of Foreign Affairs of the People's Republic of China, "China-League of Arab States Cooperation Initiative on Data Security", March 29, 2021, http://web.archive.org/web/20230216225211/https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202103/t20210329_9170559.html

¹⁰⁸ Kremlin, "Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development", February 4, 2022, <http://web.archive.org/web/20230322194109/http://en.kremlin.ru/supplement/5770>

¹⁰⁹ Simon Migliano and Samuel Woodhams, "Global Locations of Hikvision and Dahua Surveillance Cameras: Global Locations Report", *Top 10 VPN*, December 3, 2020, <https://www.top10vpn.com/research/hikvision-dahua-surveillance-cameras-global-locations/>

¹¹⁰ Tate Ryan-Mosley, "The world is moving closer to a new cold war fought with authoritarian tech", *MIT Technology Review*, September 22, 2022, <https://www.technologyreview.com/2022/09/22/1059823/cold-war-authoritarian-tech-china-iran-sco/>

designation. In other areas – such as agricultural crop mapping – having access to predatory data can give an economic advantage to a supplier which can access the data itself.

The issue for our present concern is not the surveillance potential in itself: **China competes with other providers, and there are many debates worldwide on the use of these surveillance technologies**, for the use of which countries classified as democracies come first.¹¹¹ It is the model provided to other governments, and the feedback loop of data to China. It is important to note in this context that the **Chinese IT sector** – including platforms, start-up firms – **which was always open to state scrutiny, is now more often under direct financial control of the state.** International funding into start-up and venture capital declined by 75% in 2022.¹¹² Instead, “guidance funds” from the government are more often providing the resources for these companies. The Cyberspace Administration of China is acquiring small minority shares into platform companies – including Alibaba, Tencent, Bytedance – which are likely to include a board seat, as has been the case for state entities inside private media.¹¹³ This is indeed the case for Bytedance, the parent company of controversial TikTok, now under attack for its vulnerability to personal data transfer.¹¹⁴ The long disappearance of the founder of China Renaissance, placed under investigation, is a sign: measures to increase state control have not abated.

¹¹¹ Steven Feldstein, “The Global Expansion of AI Surveillance”, *Carnegie Endowment for International Peace*, September 17, 2019, <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>

¹¹² Ryan McMorrow, Sun Yu, and Demetri Sevastopulo, “Dollar funding for Chinese start-ups dries up”, *Financial Times*, February 19, 2023, <https://www.ft.com/content/f9682546-76fb-4b65-9dce-73656aa55491>

¹¹³ Ryan McMorrow, Qianer Liu, Cheng Long, “China moves to take ‘golden shares’ in Alibaba and Tencent units”, *Financial Times*, January 13, 2023, <https://www.ft.com/content/65e60815-c5a0-4c4a-bcec-4af0f76462de>

¹¹⁴ Isabelle Feng, “Derrière TikTok se profile l'ombre du Parti communiste chinois”, *Le Monde*, April 14, 2023, https://www.lemonde.fr/idees/article/2023/04/14/derriere-tiktok-se-profile-l-ombre-du-parti-communiste-chinois_6169514_3232.html

The Chinese state’s priority for control may hinder the external expansion of its digital companies. This is increasingly evident for hardware, given the export and human resource restrictions to Chinese firms placed by others. But it is also real for software and platforms. The strict I.D. requirements laid out by the central bank for a digital yuan will inhibit its expansion – unless this serves as a model for other central banks which also have concerns about the perils of anonymous trading. The cumbersome registration needs for WeChat, the overseas version of Weixin, and the need to acquire a Chinese bank account, are also a deterrent. Although Alibaba’s volume of e-sales is several times that of Amazon, its external footprint is much smaller. After banning Google, Facebook, YouTube, Twitter, Reddit and Wikipedia, the government is now banning ChatGPT and related apps, for fear that AI-generated narratives may include criticism of policies. China will certainly introduce its own AI-generated chatbots, but the barriers that are erected work both ways. Political issues are indeed pervasive. In 2011, the founder and CEO of Meituan, one of China’s largest distribution platforms, made the mistake of posting a negative comment on the tyrannical emperor Qinshi Huangdi, which was understood as a veiled barb against Xi Jinping.¹¹⁵ Within weeks, Meituan came under regulatory scrutiny and lost 38 billion dollars (approx. 32 billion euros) in share value.

Finally, **the state has increasingly come down on the monopoly, rent-seeking and price gouging by China’s hyperscalers, and is splitting some of their horizontal activities**, such as finance and insurance, into separate companies. The break-up of Alibaba into six companies with specialized functions is a sign that a compromise has been reached with the most prominent case of data monopolization. Alibaba’s shares, which had plummeted since the ouster of its founder Jack Ma, actually rebounded on news of the break-up. This is exactly the type of choices that the EU comes up with in implementing competition laws. The US, with far less

¹¹⁵ Jane Li, “Meituan’s CEO is in the hot seat over a classical Chinese poem about book burning”, *Quartz*, May 10, 2021, <https://qz.com/2007084/meituans-ceo-is-in-hot-water-over-a-classical-chinese-poem>

regulation to promote competition until the issue of an antitrust action to break up monopolies is finally raised, will also need to move in the customer interest.

But in the meantime, China's moves against data monopolies also limit their financial resources for more expansion abroad. China is a security problem, both in terms of data collection, global network and software infrastructure and hardware dependency. Should it succeed in developing a rival chatbot to current AI engines such as ChatGPT, one shudders at the biases that the Party-state would surely introduce in the algorithms and data bases. This would put blinders on largely unaware users. But **in economic terms, China's digital sector is not as large a challenge as the US is.**

5 India, a major fence-sitter

India was once seen as a bridge combining data protection features from European and Chinese models. The **draft 2019 Personal Data Protection (PDP) Bill** adapted many principles and languages of the EU's GDPR, laying down obligations for data fiduciaries and data processors, while outlining the rights of individuals. However, it made the case for data localization with a full chapter on the restriction on transfer of personal data outside India (Chapter VII).¹¹⁶ It allowed the transfer of sensitive personal data under certain conditions, but required that copies of these data be available within India (Article 33.1), while critical personal data could only be processed in India (Article 33.2). There were mainly **three rationales** offered for the data localization requirement: **sovereignty, economic benefits, and the protection of civil liberties.** Interestingly,

¹¹⁶ Lok Sabha, *Bill No. 373 of 2019: The Personal Data Protection Bill*, 2019, 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

the **2019 draft was already a more relaxed version.** The earlier 2018 draft had required both personal data and sensitive personal data to be mirrored in the country.

In August 2022, India withdrew this long-awaited Bill after a joint parliamentary committee suggested 81 amendments in a Bill of 99 sections, stating the "need for a comprehensive redrawing of the laws and rules".¹¹⁷ The compliance burden was also cited as one of the reasons for withdrawing the bill. According to Rajeev Chandrasekhar, the Minister of State for Electronics and Technology, "Big tech firms would have just hired more lawyers to comply if there was a complicated privacy law. The burden of such legislation would hurt startups".¹¹⁸

The newly proposed draft of the **Digital Personal Data Protection Bill (DPDP)** offers some compromises and permits cross-border data transfers with certain notified countries and territories (Article 17). Provisions on data localization are not included in the draft. This is a shift away from the previous hard line stance on data localization, which had prevented India from engaging in some international initiatives. For instance, India refused to sign up to Abe's Osaka Initiative for "data free flow with trust". The explanatory note of the bill mentions Indian consideration of "the global best practices, including review of the personal data protection legislations of Singapore, Australia, European Union and prospective federal legislation of the United States of America".¹¹⁹ There are also signs of the EU and India coming together on the issue of data transfer, as we see from the chapter on Data Flows and Personal Data Protection in the draft text of the **EU-India Free Trade Agreement, and from the**

¹¹⁷ Press Trust of India, "Vaishnaw hopes new Data Protection Bill will be passed by Budget session", *Business Standard*, August 5, 2022, https://www.business-standard.com/article/current-affairs/vaishnaw-hopeful-of-getting-new-data-protection-bill-passed-by-budget-122080400290_1.html

¹¹⁸ Outlook Business Desk, "Personal Data Protection Bill: What's New In The Revised Draft And What It Means For You?", *Outlook India*, November 17, 2022, <https://www.outlookindia.com/business/what-is-personal-data-protection-bill-what-s-new-in-the-revised-draft-of-data-protection-bill-and-what-it-means-for-you-news-238163>

EU-India Trade and Technology Council (TTC) announced in February 2023. However, the DPDP incorporates large exceptions to data privacy for India's state governments under broad reasons of national security. This seems to doom a cross-border personal data transfer agreement with the European Union, which was a key part of a long-discussed free trade agreement. According to its transparency report, Meta has received 237,414 government requests for user data between January and June 2022, of which around 23% came from the Indian government, second only to the US.¹²⁰ To their credit, major US digital companies, for which the Indian data market is strategic, are currently criticizing these exceptions through the Asia Internet Coalition, an advocacy group that includes most major US and some European digital firms, and is in fact citing the GDPR as a model.¹²¹

All in all, the case of India illustrates a more general issue: **even once a policy is (or close to be) consolidated, it is still hard to develop a clear and all-encompassing strategy, due to the conflicting policy goals of interest groups.**

While the government continues its work on a comprehensive legal framework for data protection, there are **sectoral regulations in place with data localization requirements.** For instance, in April 2018, the Reserve Bank of India issued a directive on requiring payment system data to be stored in India, noting that "it is important to have unfettered supervisory access to data stored with these system providers".¹²² Restrictions on onboarding new customers were imposed on American Express,

Diners Club and MasterCard in 2021 over noncompliance with local data storage rules. Bans on all three were lifted later on "in view of the satisfactory compliance demonstrated".¹²³ Other examples can be found in the 2013 Companies Act, which requires covered organizations to store financial information at the registered office of the company (Article 94), or in the 2015 IRDAI (Maintenance of Insurance Records) Regulations, which requires insurers to hold insurance data in data centers located and maintained in India only (Article 3.9).¹²⁴

European legislators, who have taken the lead in a protective approach to data privacy, would do well to study other lessons regarding India's digital policy. This is most notably the India Stack, far less often commented on. It promises, through layers of software and sectoral regulation, to unlock the power of data for individuals while preserving data security. From Aadhaar, the eye recognition system, to the Unified Payments System, **India is achieving a mobilization of personal data for public use that is unprecedented in size.**

The most recent layer of the India Stack is DEPA, the Data Empowerment and Protection Architecture framework, which is being implemented by sector, starting from 2020 with finance, health and telecommunications. At the heart of the scheme is a granular consent based approach to data sharing by individuals, with the creation of private consent managers institutions, which are akin to the data intermediaries in the EU's Data Governance Act of 2022. They do not themselves see the personal data but serve as conduits for encrypted data flows.

¹¹⁹ Ministry of Electronics and Information Technology, *Explanatory Note - The Digital Personal Data Protection Bill, 2022*, <https://www.meity.gov.in/writereaddata/files/Explanatory%20Note-%20The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf>

¹²⁰ Meta, "Government Requests for User Data", <https://transparency.fb.com/data/government-data-requests/>

¹²¹ Jeff Paine, "Asia Internet Coalition (AIC) Industry Submission on The Draft Digital Personal Data Protection Bill, 2022", Asia Internet Coalition, December 20, 2022, <https://aicasia.org/download/554/>

¹²² Reserve Bank of India, "Storage of Payment System Data", RBI/2017-18/153, April 6, 2018, <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0>

¹²³ Reserve Bank of India, "Reserve Bank of India lifts the business restrictions imposed on MasterCard Asia/Pacific Pte. Ltd", Press release, June 16, 2022, https://www.rbi.org.in/scripts/FS_PressRelease.aspx?prid=53877&fn=9

¹²⁴ Ministry of Corporate Affairs, *The Companies Act, 2013, 2013*, <https://www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf>

The aim is to **break with the custodian-centric approach of data silos**. The project initiators explicitly criticize “walled gardens and barriers to exit”: the problem “is not that companies are benefiting from individuals’ data; the problem is that individuals and small firms do not benefit”.¹²⁵ For instance the financial sector under DEPA would unlock much banking data for third-party users, thus creating a more level-playing field with established banking institutions.¹²⁶ It is not a surprise that the country which invented microcredit has also come up with this type of innovation. Indeed, much of the Indian emphasis is on providing easy, homogeneous access to their own data for myriad users, while ensuring that the data pools managed by the DEPA platform create non personal data available for public use: **strong data governance allows for more, not less data access**. India claims this is a unique approach. It is clear that it is creating a huge pool of safely managed personal data that would have much international value, especially in the health sector.

Simultaneously, India’s government is considering a Non-Personal Data Authority that would not only promote, but also obligate sharing of non-personal – or anonymized data – and an Open Government Data Platform that would fulfill the same objective for public data (such as weather or road traffic information). These projects have yet to be put in place, but **they demonstrate a will to multiply data use, while maintaining certain guardrails**. For instance, even anonymized personal data, if originally deemed sensitive, must be stored at least in one mirror site in India.

¹²⁵ National Institute for Transforming India, *Data Empowerment and Protection Architecture*, August 2020, p.12, <https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf>

¹²⁶ Brijesh Singh and Khushbu Jain, “DEPA: The technology of consent, India style”, *The Daily Guardian*, October 9, 2020, <https://theguardian.com/depa-the-technology-of-consent-india-style/>

6 Clouds and infrastructures

In terms of priorities for data security, one might have thought that undersea cables and nodes would come out on top, since these infrastructures capture by definition much of the cross-border data flows. The construction of underwater cables requires far less capital investment than satellite networks or clouds, and they carry an estimated 95% of international data flows. Underwater cables are merely the subject of a strenuous but silent economic and political competition between the United States and China, with the balance shifting from Chinese investors and builders to American companies. **Ownership of cables is private, with also a big shift from telecom companies to top American digital investors such as Google, Amazon, Microsoft and Facebook**.

Only five years ago, this report would have highlighted a strong bid by Chinese state or quasi-state companies to conquer the sector. Perhaps because of quiet opposition and higher bids by US companies, Chinese efforts may now be abating. In Europe-Asia connections, China Unicom co-owns Asia Africa Europe-1 (AAE-1), a 25,000 kilometers fiber optic cable linking China and Marseille through South-East Asia and the Red Sea. Hengtong, a Chinese provincial-level state enterprise to which Huawei had divested its submarine cable business after the US sanctions, opened a second cable in 2022: PEACE connects France to the Indian Ocean and onwards to Malaysia. The attitude contrasts with that of the US, which has vetoed Chinese companies from several projects linking the United States to China and Hong Kong, although Orange also joins Google for two transatlantic cables (Dunant and Friendship). In a new development, two Chinese investor companies have pulled back from a third project, Sea-Me-We 6, after a US company was selected over Hengtong to lay the 19,200 kilometers cable.¹²⁷ In short, **European**

¹²⁷ Anna Gross and Alexandra Heal, “China pulls back from global subsea cable project as US tensions mount”, *Financial Times*, February 10, 2023, <https://www.ft.com/content/8f35bf1e-fe32-4998-9e13-a13bac23506d>

operators which were leveraging Chinese investment for cables under an implicit condition of seeking Chinese builders may now have to turn away from this option. Inversely, China is now using its claims over the South China Sea to exercise control over submarine cable projects in that area.¹²⁸

One could also point out as another priority the many dependencies in hardware supply chains that create a risk of data extraction or of sabotage by remote control. The case of UK cars, including government vehicles surreptitiously fitted with Chinese tracking devices, has been made public.¹²⁹ In addition to the well-known 5G case, two Chinese IT companies, Quectel and Fibocom, have captured 47% of the world's market wireless communication modules that are an essential component of the Internet of Things, and 75% of cellular IoT connections worldwide.¹³⁰ In turn, they depend on design and chipset supply from companies such as Qualcomm – which appears as a component of many modules on the Fibocom website, for instance.¹³¹ The Chinese companies also partner with many well-known companies such as AT&T and STMicroelectronics.

But these relatively silent competitions pale in comparison to the public debates over cloud service operators and supply chains. The use of clouds instead of local servers by companies, at 25%, is far less prevalent in Europe than in the United States or Japan, but it is rising rapidly. The EU's Digital Compass for 2030 includes the ambition that by that date, "75% of European enterprises have taken up cloud computing services, big data

¹²⁸ Anna Gross et al., "China exerts control over internet cable projects in South China Sea", *Financial Times*, March 13, 2023, <https://www.ft.com/content/89bc954d-64ed-4d80-bb8f-9f1852ec4eb1>

¹²⁹ Dominic Penna, "Chinese could be tracking ministers' cars with hi-tech chips, MPs fear", *The Telegraph*, January 12, 2023, <https://www.telegraph.co.uk/politics/2023/01/12/chinese-tracking-devices-could-present-british-government-ministers/>

¹³⁰ Charles Parton, "Cellular IoT modules – Supply Chain Security", January 2023, https://www.ooda-loop.com/wp-content/uploads/2023/02/Cellular_IoT_Paper_JAN_Master_PDF.pdf

¹³¹ Full list available at Fibocom: https://www.fibocom.com/en/search/index_key_Qualcomm.html

and Artificial Intelligence".¹³² **Storage is only the tip of the iceberg, since data treatment and apps using algorithms are necessary for almost all uses**, including what appears to be the most trivial to individual users (such as Microsoft 365, Netflix, Facebook, Siri and Alexa), and they take place in the cloud, on distant servers. Software as a Service (SaaS), the software layer of clouds, was already in 2022 a 251 billion dollars market, growing at a compound rate estimated between 19% and 25% each year.¹³³ Even if infrastructure investment still has higher numbers, it is the layer software that creates most opportunities for controlling access, market lock-in and oligopolies. Path dependency for users is in fact cited by new competitors. Very large users, for instance in the banking sector, point to the cost of system change, and to the adaptation they have to make in any case to new rules. The banking and fintech sector now has to implement across Europe the new Digital Operational Resilience Act (DORA) promulgated in November 2022, for example.¹³⁴ The size of data involved, the complexity of rules with added security requirements, favors established CSOs such as AWS or Microsoft comparatively to more recent entrants.

6.1. THE CLOUD ISSUE IS CENTRAL

Perhaps because they require such a massive financial investment, consume increasing amounts of energy and above all symbolize the action of entrusting data to a third party, clouds have become a major topic of public policy and debate. These issues intersect that of cross-border data flows in most cases: because clouds may be located in another

¹³² European Commission, 2030 *Digital Compass: the European Way for the Digital Decade*, Communication, March 9, 2021, https://commission.europa.eu/system/files/2023-01/cellar_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02_DOC_1.pdf p. 10.

¹³³ Fortune Business Insights, "Software as a Service [SAAS] Market Size", FBI102222, February 2023, <https://www.fortunebusinessinsights.com/software-as-a-service-saas-market-102222>

¹³⁴ Cyber Risk GmbH, "Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554", <https://www.digital-operational-resilience-act.com/>

country, or because cloud suppliers, operators and apps are from another country with different jurisdictions, making it **much more difficult for cloud users to keep control over their data and its possible onward uses.**

It is also hard to avoid the symbolic aspect of clouds. Whereas computer hardware, like railroad tracks, appears to be unmovable tangible assets, **the very denomination of cloud makes it clear that the data has been entrusted to a third party.** Even under the best data privacy regime which is still GDPR, users must consent to cookies that are necessary for the operation of a website and data use, and this technical requirement has also become controversial: this is the case in the United States with the long-standing TikTok case, where any data flow to its Chinese parent company ByteDance opened the way for access by Chinese authorities. In a US Senate hearing in March 2023, FBI Director Christopher Wray said that TikTok “is a tool that is ultimately within the control of the Chinese government – and to me, it screams out with national security concerns.”¹³⁵ In response to the comment, China Daily published a paper stressing the lack of evidence of such claims, and used the story reported by Business Insider to defend TikTok: Facebook and Google, not Tiktok, provide data to law enforcement to prosecute women seeking abortion.¹³⁶ (For more details on the TikTok case, see Chapter 5 Page 64).

This is what makes the stuff of political coalitions, since keeping in control or **“taking back control” is a popular leitmotiv.** Fictional Big Brother dystopias and Shoshana Zuboff’s very real depiction of “surveillance capitalism” feed a libertarian counterwave, from La Quadrature du Net to Maximilian Schrems’ NOYB (“None of your business”), the Electronic

¹³⁵ Reuters, “FBI chief says TikTok ‘screams’ of US national security concerns”, March 8, 2023, <https://www.reuters.com/technology/fbi-chief-says-tiktok-screams-us-national-security-concerns-2023-03-08/>

¹³⁶ China Daily, “TikTok becomes political football, again: China Daily editorial”, March 9, 2023, <http://web.archive.org/web/20230406092734/https://global.chinadaily.com.cn/a/202303/09/WS6409c-d77a31057c47ebb35bf.html>

Frontier Foundation (EFF) or Privacy India. It is also the subject of a complex fight that involves, in addition to data security concerns, preferences for digital sovereignty expressed in various degrees, and industry interests looking for a regulatory cocoon that would allow late coming native clouds to grow alongside the established giants and eventually replace them in a European or even national walled garden.

The motivations are unassailable. As the debate over transatlantic data flows has shown, **it is very hard to negotiate and ensure legal security for data that crosses into other jurisdictions, and impossible to require identical rules,** which is the reason the European Commission came up with the looser concept of adequacy. But this can easily be challenged, as is the case now for the Commission’s attempt to gain approval for an adequacy decision over data flows across the Atlantic (for more details, see Chapter Conclusion and Recommendations Page 93).

These are no longer prevailing views in the United States. Since 2022, three US Congress members have issued a bipartisan call for an American Data Privacy and Protection Act (ADPPA) that would override state legislation. As of January 2023, 10 American states have proposed new consumer data privacy legislation. As the libertarian Cato Institute notes, “a more regulatory European approach impacts companies and consumers well beyond its borders.”¹³⁷ This is also a form of extraterritorial reach, although very different from the direct intervention of US law. In his State of the Union address of February 2023, President Biden called for “bipartisan legislation to stop Big Tech from collecting personal data on kids and teenagers online, ban targeted advertising to children, and impose stricter limits on the personal data that companies collect on all of us.”¹³⁸

¹³⁷ Jennifer Huddleston, “Data Privacy Day 2023: Where Data Privacy Policy Stands at the Start of 2023”, *CATO Institute*, January 27, 2023, <https://www.cato.org/blog/data-privacy-day-2023-where-data-privacy-policy-stands-start-2023>

¹³⁸ Beth L. Goldstein, Jeffrey L. Turner, and Kristin L. Bryan, “Drive for Federal Privacy Legislation Continues in 2023”, *National Law Review*, February 14, 2023, <https://www.natlawreview.com/article/drive-federal-privacy-legislation-continues-2023>

The arguments do not cite cross-border data flows with Europe: both lawmakers and the administration are addressing first the concerns of American voters.

It may therefore be overreach for the European Parliament to require US Congress to pass legislation that will likely be debated on its domestic merits. Yet the two issues – data privacy and a transatlantic agreement – are linked. What is the degree of divergence between EU and US rules (or their absence) on digital privacy and protection that we can tolerate? In an environment where rule of law and democracy prevails, it should at least be possible to seek redress against abuses, and guarantees against cut-off from our own data and from the services and software we use. This is the condition for mutual trust, and maintaining a positive competition. By contrast, in an environment such as China's, not only is there no opportunity for legal redress, but the Chinese state's access to our data – personal or non-personal – is sure to be used in geoeconomic and geopolitical competition.

Turning down the third attempt at agreement would also be a risky bet, leaving all of us without a transatlantic framework for data flows if the US Congress does not agree on a federal data privacy act – or passes a law that is not fully recognized as adequate with GDPR standards. **Requiring a superiority of the European privacy model is a tough request, when Europe does not achieve technical parity in the field.** A small illustration may be given by the European Commission's registration system for researchers involved in EU contracts, a system supplied by ORCID, a private consortium. It requires consent by the researchers to their personal data being processed in the United States. In key areas of public order – such as the fight against terrorist financing, Europe is dependent on the United States. It was able in 2010 to conclude an EU-US Terrorist Finance Tracking Programme (TFTP) Agreement.¹³⁹ But several attempts

¹³⁹ European Commission, "Terrorist Finance Tracking Programme", *Migration and Home Affairs*, https://home-affairs.ec.europa.eu/pages/page/terrorist-finance-tracking-programme_en

by the Commission to create an equivalent programme for the European Union have failed.

The same radical impulse may be at work in the public fight over the degree of self-sufficiency and independence from foreign suppliers for clouds, both at the Member State and European level.

6.2. DESIGNING CLOUD SOVEREIGNTY

It is unquestionable that the use of clouds in Europe is dominated by US suppliers, which own a 90%+ market share. Globally, among the top ten cloud providers, there are only three non-American companies: Alibaba (6%), Tencent (2%), and French company OVH (close to 2% as of 2022). **There is every reason for any economy to regain some of its own market share, in addition to security and privacy concerns.** This could conceivably be achieved by a combination of investment, successful innovation and regulation. The question is, how fast and how effectively?

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 in the last decade, the issue has become much more complex. **Clouds are no longer just data containers, physical infrastructures resembling bank vaults.** The advent of infrastructures as a service (IaaS) such as Amazon Web Services (AWS), Platforms as a Service (PaaS) such as Google Pass Engine and Software as a Service (SaaS) such as Microsoft 365 implies that most platforms and application programming interfaces (API) are now cloud-native: algorithms and apps are also based in the cloud, and not on your local computer. **From the original data infrastructure, the different layers of cloud-based solutions have gained access and control inside the cloud.** A ubiquitous example is the cloud basing of common Microsoft 365 software, with the bonus of fast and easy updating. In a sense, platforms and software are now part of the infrastructure for data treatment. There are, of course, solutions

for these issues – from encryption to tokenization, edge processing, and partition of clouds denying access to tagged sensitive data.

What follows is therefore a rough account of basic sovereignty claims and solutions for data. None of them covers the full range of the issues involved, and this is the basic reason why sovereignty cannot be treated top-down, much less as a legal or ideological requirement, but has to be seen as a series of building blocks, which may never be complete as technology evolves.

The French and German cases, where there have been repeated attempts at fully sovereign clouds and currently a diversity of actors with varying degrees of sovereignty, may serve as an illustration.

An initial French attempt was made in 2011 for a sovereign public cloud called Andromède, but it did not attract its public and floundered in several stages, disappearing in 2020. A previous attempt to create a publicly funded search engine, Quaero, had also failed. Two French projects, Blue and Sn3s, relying respectively on Microsoft and Google technology, have been in the offing for some time. So far, it seems to be hard to build a competitive cloud without tapping into American technology. Meanwhile, the German government had created Bundescloud, a private secure cloud for government data in 2015, and Microsoft began promoting a “German cloud” for private users, operated with Deutsche Telekom. The Microsoft project emphasized technical separation from its global cloud, a data trustee security regime with Deutsche Telekom, and data sovereignty: a cloud with German laws on German soil. The “German cloud” was abandoned in 2018 by Microsoft, which instead created two data centers in Germany serving the Microsoft global cloud. Bundescloud has endured, managed by the government IT Zentrum Bund, and substituting about 400 dispersed government data networks. It is operated with Nextcloud, an open source file sharing collaborative platform that has also been adopted by Gaia-X, several government clouds and the European Commission.

Other governments have private clouds, for instance the Netherlands for its Ministry of Defence. **Italy has created a National Strategic Hub (Polo Strategico Nazionale)** which has begun to operate in December 2022,¹⁴⁰ and is meant to manage strategic and critical data and services from central public administrations, Local Health Authorities (ASLs), and other local public administrations. A public and private consortium, it also allows administrations to use the National Strategic Hub for hosting ordinary data. It therefore includes a private, hybrid and public cloud. Importantly, the Hub’s operational management is entrusted to qualified national providers on the basis of appropriate technical and organizational requirements, and does not include nationality criteria.¹⁴¹

These stories illustrate that **if a private cloud with a dedicated customer – government and its agencies – placing security as a top priority and with no emphasis on market competition can succeed, it is much harder to create a commercially viable solution without the established cloud companies.** Even governments tend to choose one of these companies for their private clouds. This is the case for the UK, which has entrusted its dual center government and defense cloud to Oracle, with a separation from the hyperscaler’s other centers. Oracle is moving forward with these solutions. It is launching in 2023 localized sovereign cloud solutions for private and public data in EU Member States, starting with Spain and Germany, with operations and support limited to EU residents (not citizens) and EU legal companies. France’s counterintelligence arm (DGSI), faced with mass terrorism, picked Palantir for data analysis. According to Palantir’s CEO, in counterintelligence, “our platform is really used massively in Europe. It is easier to identify countries that do not use us!”¹⁴²

¹⁴⁰ Cloud Italia, “Polo Strategico Nazionale”, <https://cloud.italia.it/strategia-cloud-pa/polo-strategico-nazionale>

¹⁴¹ National Cybersecurity Agency, <https://www.acn.gov.it/DecretoDirezionaleQualificazioneServiziCloud2genn23DEFsigned.pdf>

¹⁴² “Interview with Palantir CEO Alex Karp”, March 13, 2023, <https://www.palantir.com/newsroom/media/lobs3-13-2023/english/>

AU Cloud is a private company supplying the Australian government's needs at various levels. This Australian sovereign cloud uses Veeam (owned by Broadcom), Cisco and Microsoft 365. It makes a simple promise: "our data will never leave Australia. We also want certainty that no one and no foreign government can access our information".¹⁴³ It boasts of having developed the region's first Quantum Safe Symmetric Key, protecting governments and private customers against "harvest now, decrypt later" practices.

There is little debate that some of the solutions mentioned above are among the best in terms of cybersecurity. Yet, it is perhaps no accident that both the UK and Australia are members of the Five Eyes intelligence alliance with the United States. Others are not, and **this leads to questions on the reach of the CLOUD Act and other legislation**, including on US citizens working abroad, on EU companies or their subsidiaries with activities in the United States, on suppliers of software or hardware from the United States, or with the same liability to a presence in the United States. The Dutch government commissioned a legal study in 2022¹⁴⁴ that outlines a number of risks, some of them legal, some of them practical: among them is an estimate that 90% of nationals will willingly comply with a request for information, especially if the request is not disclosed to the person's employer. According to this legal counsel, **the extraterritorial reach is such that even an EU entity with no ties or presence in the United States may be asked to surrender data or face a court process**: "the EU Entity will bear the burden of demonstrating that foreign law does, in fact, prohibit disclosure of the information sought".¹⁴⁵ The same legal study argues, however, that using a US hardware component or software solution alone does not make a European company subject to

¹⁴³ AUCloud, "AUCloud Sovereign Bridge", <https://www.australiacloud.com.au/aucloud-sovereign-bridge/>

¹⁴⁴ National Cyber Security Centre, "Memo Cloud Act", Ministry of Justice and Security, August 16, 2022, <https://english.ncsc.nl/publications/publications/2022/augustus/16/memo-cloud-act>

¹⁴⁵ Ibidem, p. 14.

the CLOUD Act if their supplier does not have access to data. This analysis forms the basis for new "Europeanized" cloud services from the likes of Microsoft and Oracle, although some find this argument dubious.

This, along with the large commercial stakes involved, is a motivation for **more strict sovereignty requirements**. Alongside this need, cloud providers compete in the public arena to emphasize their own security – or to criticize the lack thereof in others' solutions. France has renewed efforts to create clouds with varying degrees of sovereignty, and to push both at the French and European level for cloud certification schemes that require strict European requirements in terms of data localization, company ownership and nationality of employees. **SecNumCloud, first drafted in 2015, was overhauled in March 2022 "with protective criteria against extra-European legislation with extraterritorial reach"**.¹⁴⁶ The most important was the obligation for CSOs to have their seat and main activities inside the EU, with share ownership capped for non-EU entities, thus excluding subsidiaries of non-EU firms. There is a ban on other suppliers or subcontractors accessing data obtained through the services.¹⁴⁷ Certification also requires all technical staff and operations to be based inside the EU – but not to be French citizens as some adverse lobbying claims.¹⁴⁸

A major strength for the argument that this is also a protectionist rule designed for French companies is that, to this day, only three companies, all of them French, have received the certification. Blue and Sn3s, partnering with Microsoft and Google, are also aiming for the certification. It is meant to be required for government agencies and for a growing list of critical companies. **Some hyperscalers have begun to adapt to new**

¹⁴⁶ <https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud-referentiel-exigences-v3.2.pdf>, p. 2.

¹⁴⁷ Ibidem, pp. 50-51.

¹⁴⁸ Nigel Cory, "'Sovereignty Requirements' in France - and potentially EU - cybersecurity regulations: the latest barrier to data flows, digital trade, and digital cooperation among likeminded partners", *Cross-Border Data Forum*, December 10, 2021, <https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likeminded/>

sovereignty and security requirements. Microsoft’s CEO Brad Smith, for example, recognized in May 2022 that “some governments may want to provide access to some sensitive workloads and data categories only to local providers, secured even from cloud infrastructure providers. Or alternatively, they may want to rely solely upon such a local partner for a subset of data processes or ensure that such a partner can provide oversight of the data flows of the infrastructure provider”.¹⁴⁹ Like any company, Microsoft remains bound by US law and the CLOUD Act. However, **if critical subdivisions of a cloud are managed with software that has been sold without access to data by the publisher, CSOs can repurpose themselves as software publishers, or cooperate with these.** Software publishers, like post offices, can legitimately claim they have no control over the data that uses their products, and therefore claim to be outside the realm of the CLOUD Act. This, with Veeam and Microsoft 365, is in fact the basic premise on which Australia’s AUCloud rests its promise that its data “will never leave Australia”. These arrangements must extend to updates, however.

6.3. CLOUDS WITH VARYING DEGREES OF SOVEREIGNTY

Debates about the relative safety and practicality of clouds with varying degrees of sovereignty abound in France, some of them promoted by newcomers in this activity. The first successful cloud claiming data security is OVH, which has indeed emerged as a serious commercial contender beyond France. It is said to compete on price. A physical fire in one of its two servers threatened its data integrity, but it has rebounded with more data duplication. It is also on the forefront of a complaint at the EU level against Microsoft for its anti-competitive practice of hefty fees to exit cloud contracts.

¹⁴⁹ Brad Smith, “Microsoft responds to European Cloud Provider feedback with new programs and principles”, *Microsoft*, EU Policy Blog, May 18, 2022, <https://blogs.microsoft.com/eupolicy/2022/05/18/microsoft-responds-to-european-cloud-provider-feedback-with-new-programs-and-principles/>

Indeed, reversibility is a common characteristic of all new French offers, and is also a guiding principle for Gaia-X: just as the obligation for internet platforms to obtain consent before harvesting – and reselling – personal data will lessen the financial advantage of hyperscalers, an EU wide action against anti-competitive cloud practices will certainly help to create a more level-playing field. Another new entrant is Iliad, the owner of Free which kicked off an intense competition in the internet box and mobile phone business, lastingly leading to lower prices in France and the EU. Free is now aiming at B2B customers for secure cloud services with a new offer that promises easy migration. The solution does rely on US based VMware, much like the sovereign Australian AU Cloud.¹⁵⁰ Finally, the most important new entrant is Numspot, an alliance created in October 2022 by the French Post Office’s digital subsidiary with Dassault Systèmes (3DS), a worldwide provider of software, France’s third mobile telecom operator Bouygues, and a public bank. Because Dassault Systèmes is a leader in secure software solutions and heavily emphasizes purely national solutions, the new group aims for a quick SecNumCloud certification.

Yet the debate on **immunity from extraterritorial laws and practicality** is not likely to disappear. Iliad uses Chinese-sourced components for its internet box, Bouygues and Orange are still using Huawei 5G gear and software. Blue and Sn3s rely on top US cloud providers. As for 3DS, according to its 2021 annual report, it employs 29% of its staff in America, where it hopes to achieve 38% of its turnover in 2023, and also has a subsidiary in China.¹⁵¹ OVH itself is present on the US market with a wholly-owned subsidiary, without operational links to the parent firm.

¹⁵⁰ Dominique Filipponne, “Uber fait un virage à 180° vers le cloud avec Oracle et Google”, *Le Monde informatique*, February 13, 2023, <https://www.lemondeinformatique.fr/actualites/lire-uber-fait-un-virage-a-180-vers-le-cloud-avec-oracle-et-google-89525.html> et <https://investor.3ds.com/static-files/17f38fe1-d8b-41e1-b4a1-73e1b7ec0ab6>

¹⁵¹ 3DS, *Universal Registration Document 2021: Annual financial report*, March 17, 2022, https://investor.3ds.com/system/files/encrypted/nasdaq_kms/assets/2022/04/01/4-08-51/3DS_2021_URD_31032022.pdf

In a February 2021 testimony to the French National Assembly, representatives from 3DS, OVH and Oracle sparred politely and usefully. Philippe Latombe, the Member of Parliament in charge of the hearing, advocated a more US-type policy of public purchases from indigenous suppliers, while the witness from OVH recognized the continuing dependence of Europe on US hardware, concurring at the same time with 3DS Outscale on the feasibility of sovereign software.¹⁵²

These debates are mirrored at the European level, focusing on the requirements for the localization and ownership of CSOs and their suppliers. This has prevented the further development of Gaia-X, the already mentioned private association of companies created in 2019 from **a Franco-German government impulse to “work towards a sovereign and reliable digital infrastructure and an ecosystem for innovation in Europe”**.¹⁵³ Best thought of as a hub, it had 21 founding members, among which 11 German and 8 French entities. The “open” nature of the hub has swelled those numbers to 367, including 9 companies from the United States and 4 Chinese members – among which only two companies and two state research institutions, but none of the big Chinese corporate names. Gaia-X is subdivided into nationally managed hubs. In France, this is managed by Cigref, an association of the country’s top companies with government ministries.

The goal remains to create common data spaces with de facto standards. But the **practice has shifted from working towards a European cloud to developing European cloud services**. The fractures described above have therefore opened up also around Gaia-X. The Italian president of

Gaia-X explains: “The European market has no alternative and must survive in a competitive market, and so we are trying to build an initiative that is competitive in the global market. And for that, we need non-European players.” While some French entrepreneurs decry the lack of European ambition on cloud software, leaving our data market to the hyperscalers and vulnerable to political decisions made elsewhere, public representatives take a more nuanced approach. According to the head of Cigref, sovereignty, and even more autarky, are not the terms that should be used. Rather, “Gaia-X is there to help in limiting dependencies on partners with which we will still be traveling.”¹⁵⁴

6.4. LESSONS

It is well-nigh impossible to draw a one-sided recommendation from these debates. Some conclusions do stand out. The lead of the major American CSOs and suppliers in terms of investment and breadth of service is recognized. **Recent or new competitors either team up with these while adding European requirements, or provide services with more limited functionalities**, which they claim to be as secure technically, often at lower cost, and more secure legally. So far, they are not reaching the capacity for data management, analysis and data recombination that comes with the hyperscalers’ algorithms and AI. Together, AWS, Google Cloud and Azure have been investing more than 100 billion dollars (92 billion euros) per year in new capacities and functionalities.¹⁵⁵ If Palantir, a company that is bound to be controversial because of its key supply role to the Pentagon and intelligence services in the United States, has so many government clients in Europe in defense, counter-intelligence, police (including Europol) and health, it is clearly because the

¹⁵² Assemblée nationale, *Compte rendu : Mission d’information de la Conférence des Présidents « Bâtir et promouvoir une souveraineté numérique nationale et européenne »*, Compte rendu no 26, February 9, 2021, https://www.assemblee-nationale.fr/dyn/15/comptes-rendus/souvnum/15souvnum2021026_compte-rendu#

¹⁵³ Gaia-X, “Gaia-X Takes Major Step Toward Sovereign European Digital Infrastructure”, Press release, September 15, 2020, https://www.data-infrastructure.eu/GAIX/Redaktion/EN/Downloads/gaia-press-release-september-15th-en.pdf?_blob=publicationFile&v=3

¹⁵⁴ Agathe Cherki, “Gaia-X, ou les illusions perdues d’un cloud européen”, *Contexte numérique*, May 30, 2022, https://www.contexte.com/article/numerique/gaia-x-souverainete-cloud_150712.html

¹⁵⁵ Leïla Marchand, David Barroux, and Nicolas Madelaine, “« Aucun pays n’est totalement souverain sur le numérique »”, *Les Echos*, Interview, January 20, 2023, <https://www.lesechos.fr/tech-medias/hightech/aucun-pays-nest-totalement-souverain-sur-le-numerique-1898918>

offer is technically irresistible so far. It also teams up with major European suppliers of digital solutions.

To make up for this, **more recent entrants have often chosen to compete on cost and flexibility** – in particular, the reversibility of service that ensures market competition. In contrast, exit clauses in the contracts of the dominant CSOs create an oligopoly, with users walled in their initial choice. That situation is also true of the American market. A bipartisan attempt was made twice (2019 and 2021) in the House Judiciary Committee to introduce an Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act. The Act would put an end to a situation where “too many tech companies are “roach motels” where our data enters but can never leave”.¹⁵⁶ In Europe, a complaint against Microsoft’s licensing practices has been introduced with the Commission by several companies and CISPE (Cloud Infrastructure Services Providers), a trade group based in Europe whose members¹⁵⁷ include Amazon. Microsoft is said to have come recently to a settlement by changing its licensing terms, although not with CISPE¹⁵⁸ and therefore its main U.S. competitor! The European Directorate General for Competition (DG COMP) has more leverage, if not more manpower, than the Federal Trade Commission (FTC), and can set a trend for Europe. The EU Data Act now under consideration would further increase this leverage by introducing formal interoperability and portability requirements.

Another conclusion is that **one must distinguish data hosting from apps, including AI, used to recombine this data**. It is easier to insulate the data, provided that one limits the functionalities, and therefore the

¹⁵⁶ Katharine Trendacosta et al, “The ACCESS ACT Takes a Step Towards a More Interoperable Future”, *Electronic Frontier Foundation*, June 11, 2021, <https://www.eff.org/deeplinks/2021/06/access-act-takes-step-towards-more-interoperable-future>

¹⁵⁷ CISPE, “Members”, <https://cispe.cloud/members/>

¹⁵⁸ Foo Yun Che, “Microsoft offers to change cloud practices to ward off EU antitrust probe - source”, *Reuters*, March 28, 2023, <https://www.reuters.com/technology/microsoft-offers-change-cloud-computing-practices-after-rivals-complaint-source-2023-03-28/>

apps used. Thus a 100% sovereign cloud would appear suited to national defense and some public order issues – except that these sectors also need some data recombination to effectively use the data. If there is one area where subsidies for research and innovation appear to be necessary, it is therefore the software layer where independent apps can be created. This would include strategic data. One can be more skeptical of major subsidies aiming at creating 100% sovereignty for critical (but not defense related) or ordinary data.

Almost no personal data is ordinary in the sense that it can be recombined, and on the other hand the issue of denying unauthorized access and use of critical data is not specific to cross-border flows and access by foreign actors. What difference does it make to users if health, financial, traffic and other non-personal data such as intellectual property is hacked by domestic or foreign agents? **There is an expert consensus that 100% security does not exist other than in an entirely closed and unconnected system**. Bugs are an important aspect of coding, and the verification needed to separate potential backdoors from “normal” lapses is impossible to generalize.

Another key conclusion is that **public procurement, unlike subsidies, can make a strong difference within market conditions**. The French social security system as a nationally unified buyer of drugs and health care has been able to exercise a strong downwards pressure on prices, coordinating public tenders among various agencies and levels of government: public purchases can have a major influence over providers. Ensuring the diversification of choices among bidders to public tenders can create a more secure incentive for private investment: technological innovation needs time and a sense of future markets to develop. Data security criteria can be adjusted to calibrate partially sovereign solutions and access restrictions for providers and suppliers in some cases. This is where European rules such as the Digital Market Act and the Digital Services Act, both fully applicable in 2024, can serve as a stimulus to technological improvement by European firms.

Cloud service operators and their suppliers are best placed to know their risks, especially if they are strongly liable to compensation for data leaks. Here, one might take a leaf from China's recent Data Security Law. Although the party-state proceeds from a broad and top-down security approach, it does leave some room for local authorities and operators to define which of the five planned security levels they want to choose for data. This flexible approach – alongside increasing penalties as the years go by – is typical of Chinese step-by-step policy making within a rigid strategic framework.

The road to European clouds is important from a security and economic perspective, but it should both be gradual and reflect a predictable scheme to all actors. In the short term, a decisive competition policy at the European level is key to limiting the rentier advantages of first movers. The idea of a digital tax seems to be also an option, especially if the proceeds are used to help research and development in the same sector. But locating tax with final consumption markets rather than in the producer countries is proving difficult to negotiate outside Europe. Besides what is categorized as Silicon Valley, other industries, from luxury goods to the extractive sector, also have to fear from such a reversal. **A decisive competition policy coupled with a well-defined public purchase policy would achieve more results in the medium and long term.** We highlight these solutions because they are a partial remedy for Europe's chronic underinvestment into education, research and development in the digital sector. The best initiatives pale when compared to the yearly budgets of global digital leaders. Enforcing competition laws would likely limit the cash hoardings of these companies. Strong, EU-wide public purchase policy would provide a horizon for investment by new entrants in the field.

7 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.** We have emphasized the futility of pretending to achieve total security in any data flow, within or across borders. 100 % safe data simply does not travel. This note also seeks to debunk the localization argument which would seem to flow from the previous sentence: **given the interdependence in hardware and software, total self-sufficiency is out of reach.** We do position that America's data sphere has an inborn advantage in localization and other tech advantages – first mover, amount invested, scale. It is clear that China, leveraging its large digital market and industries, is seeking a watertight localization of data at some unspecified date. Europe is in the position of a catch-up country on the digital front with the United States, but it shares much of the same aversion to closed authoritarian systems that do not only seek to exist alongside democracies, but also threaten them in very tangible ways. That, indeed, is a political, not a technical argument, and does not prevent the transatlantic floor from being littered with quarrels of the past and new debris.

At some point, **we must therefore pause and check our own hypocrisy.** The CLOUD Act has in fact become a lightning rod for all suspicions about American intentions – spying on friends and allies by using these requests to gain technological and economic advantage. On the American side, it is probably Commissioner Thierry Breton and his frequent declarations on industrial policy, strategic autonomy and the build-up of a sovereign digital industry that catch lightning. The US and many liberal economists suspect Europe of using data privacy and cybersecurity as a decoy to push a neo-mercantilist policy, discriminating against non-EU companies.¹⁵⁹

¹⁵⁹ Pascal D. König, "Fortress Europe 4.0? An analysis of EU data governance through the lens of the resource regime concept", *European Policy Analysis*, Vol. 8, Issue 4, 2022, pp.484-504, <https://doi.org/10.1002/epa2.1160>

The unpalatable truth is that these two allegations are both right and wrong. The liberal international order did not come into existence by itself, but as the result of a world war. It is now under a more diverse challenge than at any time during the Cold War: in part because it has succeeded in promoting newly developed economies which claim their place under the sun, in part because globalization limited to economic liberalism has greatly benefited adverse political systems and undermined the faith of people in their own democracies. **The CLOUD Act and other tools** – chiefly, sanctions such as those empowered by the dollar’s ubiquitous use – **are part of the defense of an international order that is embedded within the US as much or more than within the United Nations system.**

Lacking a common defense capacity and the will to underwrite it financially, lacking digital capabilities that would match those of US companies and their deep pockets, lacking extraterritorial jurisdiction for the fundamental reason that Europe’s transfer of sovereignty to the Union has never been complete, **Europe’s choice of clean hands risks coming at the expense of having no hands.** In fact, when it considers for itself issues such as e-evidence and limits to data privacy, the European Union and its members encounter domestically the same dilemma that exists vis-à-vis the United States. And the loudest voices in defiance of the ally across the Atlantic are often also the loudest voices for limits to data privacy, and for more power to the state and to governments inside the Union. Courts, including the CJEU in some cases, and even more NGOs advocating for unmitigated data protection for individuals, do ride on a European culture of individuality and privacy. The EPDB itself has recently reiterated the need “to strike a fair balance” between the objectives of fighting money laundering, terrorism, and rights to privacy including the protection of personal data.¹⁶⁰ But we have seen, in the case

¹⁶⁰ European Data Protection Board, “EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council’s mandate for negotiations”, March 28, 2023, https://edpb.europa.eu/system/files/2023-04/edpb_letter_out2023-0015_aml_cft_ep_en.pdf

of terrorism, how public opinion can reverse itself when fears rise. **On the present topic of data flows, advocating radical stands and requiring not so much adequacy, but identical rules and norms, leads to the impossibility of exchange.** Do we really think that along with noted differences of values (ranging from the death penalty to the consumer and commerce based approach of much US data legislation) we do not have more in common than with systems where no checks and balances exist? Should we not balance digital sovereignty with the many benefits of a joint digital space?

On the other side, **the winner-takes-all mentality is embedded in American economic behavior and neglects several facts.** First, although poorly developed, competition and antitrust policies do exist in the United States as well. Today’s giant platforms are at least the equivalent in size of the late 19th century railroad and energy companies. Second, industrial policy is unexpectedly finding a whole new life in the United States under the unambiguous goal of catching up with others (chiefly, China) which have gained a headstart in energy transition and may do the same in other sectors of innovation. Although that is not a satisfactory state of affairs, one might say that **the United States is simply turning to subsidy policies** in other areas, while it has always subsidized and steered innovation in a few key high tech sectors. **The EU regulates more than it subsidizes**, as befits an economy with less financial leverage. But it is consistently turning to more strategic innovation policies and more financial resources, whether by subsidy, by creating tax breaks or by challenging the data oligopoly that leading US companies have built.

As is the case for other key sectors (aerospace, defense industries), the United States, which leverages its own defense spending to secure key deals abroad, must recognize that building up European cloud capacities and data treatment is essential to economic growth and to welfare. **Keeping the transatlantic digital space open requires concessions on both sides.**

Probably the most important concession from the European side on security is to recognize, as the Commission does, that the Biden administration has moved on the issue of oversight regarding data and intelligence collection. We have an unhappy precedent, which is that of the Transatlantic Trade and Investment Partnership (TTIP), a comprehensive free trade agreement encompassing services. This was derailed by the Investor State Dispute Settlement (ISDS) issue in 2015-2017. Then as now, public opinion suspicious of arbitration mechanisms and hidden hands played a role. The compromise proposal by the EU of an Investment Court System (ICS) was shot down by both European opponents of the deal and US negotiators clinging to their defense of ISDS. TTIP never came about. **The European Parliament will have to decide whether it accepts by default a fragmented internet where Europeans do not hold the best cards**, and consider the American and Chinese systems to be almost equivalent and unacceptable to our “values”, or whether they choose the least worst option. There is unfortunately no advice that can be given to the CJEU – except perhaps that law is best interpreted in context.

On the US side, the main weakness of the March 2022 agreement with the Europeans and the subsequent White House executive order is not that they do not offer enough guarantees. **It is that these guarantees are a political decision, not a legal act.** The order could be overturned, whereas the main advantage of a transatlantic data agreement should be to create the legal certainty that allows for long-term investments and cooperation. In February 2023, the EDPB issued an opinion acknowledging the progress from the US side, but raised concerns over “certain rights of data subjects, onward transfers, the scope of exemptions, temporary bulk collection of data and the practical functioning of the redress mechanism”.¹⁶¹ The EU Parliament’s Committee for Civil liberties goes one step further by siding against the adequacy decision with a recent draft motion for

resolution,¹⁶² citing reasons that extend all the way from insufficient definitions of proportionality and lack of proven independence for the proposed US Data Protection Review Court to the much broader criticism that the US has no privacy legislation at the federal level. The resolution was adopted on April 13, 2023, calling for a lawsuit-proof regime for legal certainty. It notes that **the EU-US Data Privacy Framework is an improvement compared to previous mechanisms, but won’t “survive the test of the CJEU”**.¹⁶³ The committee decision, and even an EU Parliament decision, would not be binding on the Commission. But the Parliament has an influential political voice.

On the same day that the EU Parliamentary Committee's draft opinion was published, the American president of the influential Information Technology & Innovation Foundation Technology defiantly tweeted: “many in the EU defend privacy as ‘fundamental human right’. If so, they should ban: 1) drivers' licenses 2) license plates 3) credit cards 4) any requirement to show IDs (airports, gyms, hotels, etc.)”.¹⁶⁴ Others have contended that GDPR has provoked the exit of a third of available apps from the Google Play Store in Europe: however, these apps accounted only for 3% of total use.¹⁶⁵

¹⁶² European Parliament, *Draft Motion for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 132(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Data Privacy Framework*, (2023/2501(RSP)), February 14, 2023, https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf

¹⁶³ European Parliament, “MEPs against greenlighting personal data transfers with the U.S. under current rules”, April 13, 2023, <https://www.europarl.europa.eu/news/en/press-room/20230411-PR79501/meps-against-greenlighting-data-transfers-with-the-u-s-under-current-rules>

¹⁶⁴ Robert D. Atkinson (@RobAtkinsonITIF), “Many in EU defend privacy as “fundamental human right”. If so, they should ban: 1) drivers' licenses 2) license plates 3) credit cards 4) any requirement to show IDs (airports, gyms, hotels, etc.) So clearly, they don't really mean that privacy is a fundamental human right.”, *Twitter*, February 15, 2023, 5:06 p.m., <https://twitter.com/RobAtkinsonITIF/status/1625889367322513408>

¹⁶⁵ Rebecca Janßen et al, “GDPR and the Lost Generation of Innovative Apps”, *NBER Working Paper*, No. w30028, May 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4104014 and https://www.theregister.com/2022/05/09/gdpr_europe_apps/

¹⁶¹ European Data Protection Board, “EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain”, February 28, 2023, https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en

On the economic side, there is now less support across the board in America for its digital champions: they have created issues of excessive dominance on their own domestic ground.

America is able to leverage its home market by opening innovation and subsidy policies to foreign firms and research entities. The interdependence that these policies create works for American interests. But **the European answers should not be a closure “à la chinoise”**. Not only is this most often just a figure of speech, but those declarations of intent stir up hostility and contempt from the US side. There are very good reasons for Europe to seek innovation and supply chains in the digital sector. But this is not across the board, and it should not be at the expense of efficiency, scalability and cost.

Even in the most restricted and sensitive digital space, it is going to be extremely difficult not to rely on some non-EU suppliers: ironically, 5G and Huawei have shown this on the side of China, with a large cost for giving up risky Huawei equipment – which remains cost-effective and with advanced energy savings. There were excellent reasons to do without Huawei, but these were not economic in the main. The same reason does not apply equally to American hardware or software input. To cite one example, overemphasizing health data security at the expense of more efficient and innovative treatments allowed by AI is not a good choice. There is no reason why the US public would be less sensitive than Europeans on these issues, and the debate therefore exists on both sides of the Atlantic, not between one side and the other. There is also a strong argument to team up efforts on telecommunications and digital infrastructure with third countries – Indo-Pacific nations and more broadly the so-called “Global South” to match Chinese offers.¹⁶⁶ The Transatlantic Trade and Technology Council is the likely format to coordinate Global Gateways projects and American public and private initiatives.

¹⁶⁶ Mark Scott, “Digital Bridge: TTC planning – Twitter’s costly data – US-EU antitrust bosses”, *Politico*, March 30, 2023, <https://www.politico.eu/newsletter/digital-bridge/ttc-planning-twitters-costly-data-us-eu-antitrust-bosses/>

Under conditions of free trade in services, it is impossible to reserve a market, be it that of public procurement, to domestic suppliers. This is even more the case when the domestic alternatives are still on the drawing board or at an early take-off stage, as is the case for data clouds. The counter examples from post-war cocoon industrial policies in North-East Asia, neglect the fact that these countries’ domestic markets were negligible compared to their role as cheap and reliable suppliers of consumer goods to the most developed economies – in fact, to the United States, since the true opening of the European market took place at a later stage.

As much as the European Union should oppose an American subsidy war over energy transition and semiconductors, it should also seek common ground with the United States in the digital sector, from standards to infrastructure. That implies restraining localization subsidies on both sides, accepting mixed solutions, and a strong competition policy in Europe to create a more level-playing field with large US companies. **This is a finance and innovation issue, not a strategic divide**. The other option – fragmentation on grounds of self-sufficiency – would isolate Europe, including from many third markets and parties, and create the ground for unhelpful political strife.

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 an aggressive forward digital footprint and total lack of accountability for its own data management. China is not alone among authoritarian states in this respect, and even weaker actors for example can present large cyberhacking capacities. But China’s combination of IT industries, hyperscalers

with international presence and a vulnerability reduced by its own data localization requirements is unique.

The **challenge** – not a threat even if some may conceive future scenarios where transatlantic interests and actions are completely at odds – is the United States' advantage as first mover, largest R&D and capacity investor with a stellar ability to combine public and private actors. As we have seen, the debate on data sovereignty and localization is tipped by the fact that American companies have achieved de facto data localization while being the international leader in software and data management. For comparison, China's platforms are at least as large domestically but have a much smaller global footprint.

In some ways, the debate about cross-border data flows resembles two other debates. One is the issue of the US dollar's "exorbitant privilege", as both the leading currency of exchange and the predominant store of value in the world. The other is the old policy dilemma for developing economies to catch up with the most advanced – the choices between an industrial policy or cocoon and an open economy have never been simple. The money printing power of Silicon Valley and venture capital has been a private sector equivalent of the Fed's ability to manage the US dollar, or of China's subsidy policy for innovation and the digital sector.

Even more than for almost any previous industry, **scale matters for digital markets**. The European Union or European Economic Area do not really have a single digital market, nor do they have such a large venture capital pool, or the common budgetary capacity to subsidize innovation at a level that would match China's. Moves in Europe towards more independent digital capacities have a price if there are exclusionary or localization obligations. In an open trading economy context, that translates as less competitiveness, at least in the short term, in order to achieve some form of parity in the longer term. If one adds that the WTO, whose arbitration mechanism is semi-paralyzed, has very limited competence on digital service issues, it also means that Europe's reliance on multilateral

solutions is severely bounded by the lack of an internationally recognized and enforced legal environment.

The policy prescriptions that flow from this two-front environment – the relatively well-defined threat from China and the multiple challenges represented by the US – and from the policy dilemma summed up above are manifold.

Recommendation 1

Moving towards a **more effective common European data space is a crucial first step**. The changes can only be achieved through a **realistic sequencing of priorities**. For instance, there is no reason for Europe to seek European solutions in areas where alternatives are attractive and immediately available. Instead, beyond national defense-related data, Europe should target the next level of critical data for European cloud solutions, and leverage its competition policy to create a level-playing field.

The Euro achieved a pooling of currency reserves, but its sovereign power remains limited due to a small European common budget capacity and to the moral hazard created by 27 independent spending and fiscal policies. On cross-border digital flows, this is mirrored with the lack of delegated sovereignty for national security data, which has been a fundamental limit of European integration so far: **truly European capacities and rules can only be created for second-tier critical data, related to "public order", or for non-critical data**.

Secure data storage and movement is clearly not available in equal terms to all 27 states whose financial and digital capacities vary. This limitation almost guarantees that many states will need to choose non-EU

suppliers. Once that initial choice is made, **there is less reason to seek European solutions over others, which may be more immediately available.** That very issue has dogged health data policy over an emergency such as the Covid pandemic. The French Health Data Hub chose Microsoft solutions which were conveniently available, irrespective of their merits or demerits. The ensuing polemic has essentially delayed and possibly crippled the project, especially as it was used by key participants as a pretext to withhold data from common use.

In many areas, a fragmented digital space does not only exist institutionally between 27 Member States, but also in practice within each of these states. Data collection, norms for classification, and protection remain dispersed before one even begins to discuss data storage, analysis and further use. **The move to unifying specific European data spaces cannot be sudden, and this is not only due to political reasons of state sovereignty, but also to the efforts needed on scope, norms and technical choices.** Innovation, in the digital sector as elsewhere, is a hit-or-miss issue, with human resources and private firms playing key roles within the orchestra.

This is both a question of timing and realistic priorities. To cite one example, **a European (or nationally-based) cloud solution has little chance to succeed now if it targets the broader B2C market.** It is probably the last phase in a process that would first necessitate European hyperscalers able to use these solutions. This is a situation which is the reverse of that of the chip industry, where it makes sense to develop capacity first for 28 to 65 nanometer semiconductors widely used in consumer industries, and to move later to the most advanced formats. The only game changer would be a US change in competition policies (e.g. a mandated break-up of the largest cloud companies that have an excessive hold over the market). This is unlikely to happen. In the absence of a European competence to deal with national security data – a failure that is as consequential as the broad dispersion and division on national lines of European defense industries – **it is the next level of critical data that should be targeted for European cloud solutions, followed by hybrid B2B data storage.**

In the absence of a US antitrust push in the IT sector, **the European Union should make its own competition policy into a priority.** At present, the major hyperscalers and cloud solutions often lock in their customers with complex exit processes and heavy fees for the data they have collected from their customers. Creating a level-playing field requires a regulatory enforcement of fair competition. Data portability is an important requirement for this. The Data Act, now under consideration by the European Union, includes requirements on cloud switching and interoperability.¹⁶⁷ Even after adoption, it will only become effective after an 18 to 24 months delay. As beneficial as this will be to European customers, it remains to be seen if significant alternatives to the majors will come up in time.

Recommendation 2

The EU needs to **broaden its long-term vision beyond the traditional Commission support to first stage innovation mechanisms** in order to increase public and private financial resources, as well as to **create more synergy with industry second stage growth.**

“Far too often, promising European start-ups struggle to raise the capital they need to expand and mature. They are forced either to move abroad to the deep capital markets of the US or sell themselves to larger rivals with deeper pockets”, note Gelsomina Vigliotti and Marjut Falkstedt of the European Investment Fund.¹⁶⁸ **The EU needs to broaden its long-term vision beyond traditional innovation support mechanisms.** The

¹⁶⁷ Tambiama Madiega, “The Data Act”, European Parliamentary Research Service, October 2022, p.7, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733681/EPRS_BRI\(2022\)733681_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733681/EPRS_BRI(2022)733681_EN.pdf)

¹⁶⁸ Gelsomina Vigliotti and Marjut Falkstedt, “A venture capital injection for European technology”, EURACTIV, February 16, 2023, <https://www.euractiv.com/section/economy-jobs/opinion/a-venture-capital-injection-for-european-technology/>

EU's approach to reduce asymmetry between American and European firms has been to advocate digital taxes – relying on place of sale rather than on place of production. Should these taxes be used for direct subsidies towards European digital projects, it could be a useful tool. But that novel approach is now stranded in unending negotiations at the OECD, and is also countered by present and future members of the Digital Economy Partnership Agreement (DEPA), a pragmatic digital and cross-border agreement. Whatever its merits or demerits, one cannot fail to notice that this is also an effort to find a new financial resource, whereas the US digital sector relies on deep pockets that already exist with venture capital for hit and miss innovation, and from cash flow and share valuation to buy promising startups from other continents. **While arguments for new taxes or for antitrust moves restoring fair competition may be legitimate, they cannot replace sound public policy and incentives to encourage innovation and to scale up growth.**

True, while the European tech ecosystem is only a third of the American equivalent, it is catching up in the amount of capital raised. On February 13, 2023, the European Investment Bank Group, alongside contributions from Germany, France, Spain, Italy, and Belgium, launched the **European Tech Champions Initiative**. With its initial 3.75 billion euros, this is only a beginning, one hopes. The initiative aims to boost Europe's high-tech companies in their late-stage development and address the continent's venture capital lag. Pooling public resources from participating Member States and the EIB Group, this fund of funds will invest into large-scale venture capital funds, which will thereafter provide growth financing to European tech champions. Before the current downward trend of valuations, Europe had 13% of the world's unicorns (valued over 1 billion dollars). Clouds and the IoT are an important component.

But innovation requires public-private partnership. In some cases – such as European telecom companies involved in 5G infrastructure – the lack of support has made it more difficult to move away from Chinese suppliers. In other areas, such as clouds, private capital is not sufficient to

allow for scaling – an argument that is often repeated by large hyperscalers against their local competitors. **The EU is changing its approach to industrial policy and subsidies, and this adjustment should be extended to the interaction with private companies.** This has begun with Important Projects of Common European Interest (IPCEIs) for semiconductors, batteries and hydrogen. A similar project has been launched over *Next Generation Cloud Infrastructure and Services (IPCEI-CIS)*. It must ensure that as many industry actors in the field as possible should be considered, and the range should be broadened to algorithms and AI: these are areas where small companies and research laboratories can quickly make a huge difference. Direct support to private companies must in any case go beyond the research phase, with an open door to potential entrants. When it comes down to the market production phase, the relevant public funder also has to avoid over-involvement into the actual execution of the funded project. Where there is large government investment in large-scale European projects (Arianespace, Airbus), the influence of Member State governments is often too large over effective management and investment choices. This contrasts with SpaceX and Blue Origin. These too benefited from key support to innovation, and from public orders, but there is no intervention into management, and competition prevails among them. These differences should not be repeated in the digital sector.

Recommendation 3

The EU should adopt a **pragmatic and inclusive approach in the design of funding and employment policies** to attract startups, research centers, foreign firms and talent. For instance, implementing a “Buy European” policy that is inclusive enough to allow for non-European suppliers in critical or underdeveloped sectors would be an improvement over a “Made in EU” requirement.

There is a fundamental difference between US subsidies for innovation and many European (or Chinese) policies: the former are designed to attract non-US firms, while the latter are often reserved to European companies. In fact the most disturbing aspect of the IRA to Europeans is precisely that it is an open appeal to foreign firms to create new capacities in the United States. By contrast, most of the moves and rhetoric around **European strategic autonomy in the digital sector focus on European actors**, and often in practice within the boundaries of a single Member State. One should also note that while Chinese support for innovation includes political control and in some cases full strategic support (Huawei), it also leaves ample room for a venture capital market and competition between firms. Nor can the European Union ignore that US innovation policies combine public and private actors, subsidies and tenders, private companies and research institutions, and in many cases American and foreign firms. Massive support to R&D and innovation is needed, but neither the European Commission nor Member States should pick the winners or go as far as to entirely subsidize an industry. On the other hand, regulation and their requirements can nudge towards outcomes, and public orders can be all the more important as one increases these requirements for critical data.

A “Buy European” policy that is inclusive enough to allow for non-European suppliers in critical or underdeveloped sectors would in fact be an improvement over a “Made in EU” requirement or, worse, its single Member State equivalent. **The emphasis on rules has been overwhelming and targets the demand side while leaving intact supply side deficiencies. Referees do not win matches.** The “Brussels effect” – or Europe’s ambitious regulatory power and influence – is not enough to compensate for a lack of resources, industry and skills. In all these areas, the United States, often criticized for weaker competition rules, but endowed with large congressional oversight over federal grants and contracts, has been more pragmatic and inclusive.

Another area where Europe has not moved forward with enough speed is the **acquisition of human resources, including through targeted skill**

immigration. Spending for higher education, links between academia and entrepreneurs from job choices by students to cooperative association are weaker in Europe – except in the United Kingdom – than in the United States.¹⁶⁹ Solving this is not a short-term issue. On every one of those counts, France is behind the curve in comparison to its neighbors. Only 20% of its students choose a scientific education, as opposed to 40% in Germany. Only 33% of French youth think that “science brings more good than evil to mankind”.¹⁷⁰ In addition, Europe is far less open than the United States to skilled immigration. It is telling that a perennial topic of friction with India is that of visas for students and software engineers, while the United States has recently made a move to ease H-1B specialty worker visa renewal.¹⁷¹ This is caught up with wider European fears about immigration, but also with policies that combine humanitarian concerns (the refugee and abode issues) with employment closed door policies. Paradoxically, the effective result is that **Europe is in effect more open to low skill immigration than to high skill contributions from regions beyond Europe’s neighborhood such as India or Taiwan.** While America’s IT industry employs many talented immigrants – including from Europe – with higher pay, Europe’s IT sector is largely passed over because of more restrictive or misplaced immigration rules. And it is entirely possible that the United States will adopt even more open rules for STEM (science, technology, engineering and mathematics) student and professional visas. A reform of visa rules was envisaged but dropped from the 2022 U.S. Chips and Science Act, but could well reappear in view of the labor shortage for digital workers and electrical engineers.

¹⁶⁹ Gilles Babinet and Olivier Coste, “Technologies numériques : l’insuffisance du système d’enseignement supérieur et d’innovation”, Institut Montaigne, January 17, 2023, <https://www.institutmontaigne.org/analyses/technologies-numeriques-linsuffisance-du-systeme-denseignement-superieur-et-dinnovation>

¹⁷⁰ François Kraus, Helen Lee Bouygues, and Rudy Reichstadt, “La mésinformation scientifique des jeunes à l’heure des réseaux sociaux”, Fondation Jean Jaurès, January 12, 2023, <https://www.jeanjaurès.org/publication/la-mesinformation-scientifique-des-jeunes-a-lheure-des-reseaux-sociaux/>

¹⁷¹ Andrew Kreighbaum, “State Department Plans Pilot for Domestic Visa Renewal (1)”, *Bloomberg Law*, February 9, 2023, <https://news.bloomberglaw.com/daily-labor-report/state-department-plans-pilot-for-domestic-visa-renewal-this-year>

Recommendation 4

Europe must **improve and leverage its market power and regulatory ability** to achieve more data security. These policies can go a long way **without pursuing radical self-sufficiency, or “going Chinese”**.

We must remind ourselves of how unrealistic and in fact pointless is any shortcut to self-sufficiency involving full data localization in sovereign clouds, a 100% national or European supply chain, and external data flows limited to partners where full adequacy of rules is recognized. Strikingly, there is an **unspoken alliance between digital sovereignists, who are security hawks, and radical advocates of personal data protection, who are privacy doves**. The two will usually clash on their own national ground – since national defense and public order may require encroachments on the sort of personal data protection that is sought by privacy advocates. But on cross-border data flows, the two extremes often meet, as is the case now for opposition to a new adequacy decision by the European Union with the United States.

Once this reservation is made, there is major room for improvement in the autonomy and security of a European data space. It is interesting to look at Chinese policies, because China’s digital space is as or more developed than Europe’s. Behind ideological diktats and the absolute priority given by the Party-state to access any data, including proprietary and personal data whenever it wants and to make use thereof, there have been industry dilemmas that slow down the move to digital self-reliance. One is the dependence on foreign equipment, whether hard or soft. **Chinese companies and customers are as sensitive as any to first mover and winner-take-all advantage**. Moving to untested or less known alternatives is not their first option. It requires a combination of foreign sanctions – for instance on chips and chip design – and political will to fight back. Even one of the staunchest Chinese advocates of digital

autarky recognizes that “independent innovation is not about working on technology behind closed doors, but about persevering in developing technologies ourselves while learning from others”.¹⁷² His solution to this dilemma is exercising China’s market power – by denying access to those foreign companies which implement technology denials against Chinese manufacturers. Although the strategic and political context between Europe and the United States is wholly different, **in terms of bargaining there is a case to be made for leveraging Europe’s market power and regulating ability**.

On another issue, China is an interesting case to study. Its overall digital strategy has huge ambitions, encompassing every sector of the economy and society. And it simultaneously seeks to uphold its cybersecurity. Yet it refrains from spelling out with precision what data belongs to each of the five criticality levels defined by law. There is currently room for initiative in this regard by local authorities and operators, perhaps with later streamlining of the national regulation. Needless to add, all defense related data are beyond the range of the law.

Recommendation 5

The EU must **contain regulatory requirements and avoid promulgating broad and sweeping rules that are either overextended or unrealistic**. Negotiating and legal inflexibility on our principles and values may produce undesirable outcomes, with less demanding standards such as DEPA prevailing outside Europe.

¹⁷² Lu Feng, “Lu Feng: In response to the US tech decoupling, China must be determined to do this (应对美国科技脱钩, 中国要下定决心做这件事)”, *Guancha*, January 17, 2023, http://web.archive.org/web/20230203143424/https://www.guancha.cn/lufeng2/2023_01_17_676210.shtml, translation provided by sinification@substack.com

Europe has created in principle the most favorable environment for data privacy through GDPR but it is now oversold in several respects. As any user can find out daily, this **broadest and top-down approach from a legal angle has left an immense number of loopholes against the exercise of their rights by users**. National data protection authorities often face major challenges since the One-Stop-Shop (OSS) mechanism demands cooperation between the Lead Supervisory Authority and the Concerned Supervisory Authorities (CSAs). In February 2023, a proposal was made for a regulation to streamline cooperation between Data Processing Agreements in cross-border cases, by harmonizing some aspects of the administrative procedure.¹⁷³ The initiative aims to simplify the enforcement of the GDPR and is expected for the second quarter of 2023.

Regulatory and oversight boards at both EU and Member State levels should not only consist of EU and Member State representatives, but should also include at least an advisory tripartite structure with experts and private sector representatives. This is not the case even with the most recent regulatory authorities such as the European Artificial Intelligence Board created by the Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (so-called Artificial Intelligence Act) and amending certain Union legislative acts.¹⁷⁴ From the legal quagmires set up by well-known hyperscalers to the constant evasion by smaller actors – abuse of “legitimate interest” and convoluted UX designs being currently at the top of the pile – GDPR is poorly implemented even for the most privacy conscious user. As one observer drily notes, “the law

¹⁷³ European Commission, “Further specifying procedural rules relating to the enforcement of the General Data Protection Regulation”, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_en

¹⁷⁴ European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts*, COM(2021) 206 final, April 21, 2021, Title 6, Chapter 1, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>

doesn’t make people figure out for themselves whether the food they buy will poison them”.¹⁷⁵ The European, and in many cases the CJEU’s, insistence on individual right of choice is often counterproductive because this does not work in practice. The Commission has traveled a digital learning curve from GDPR to the DSA and DMA. The CJEU has to achieve similar progress. It also has to acknowledge uncertainty and unavoidable risks. If one absolutely wanted to prevent all road accidents, one could ban road traffic. Principles do matter, pre-emptive measures and redress are important, but they must be weighed against the risk of slowing down European innovation and favoring outside competitors.

In public debates, broad assertions regarding “Big Brother”, hegemonic or aggressive foreign actors create a paranoia that is both ineffective against many of the more obvious encroachments, and a general atmosphere that is hostile to data sharing for the best of purposes. **Regulations should not reinforce the aversion of primary data collectors to sharing, whether it is out of profit or for reputational considerations** (a very frequent case for non-profit research). In the health sector, suspicion and protection are everywhere: against the risk that health data be communicated to credit and insurance companies; against communication of data that sits unused for actual research, but that would perhaps be of immense value once used effectively by a pharma company. In Europe’s risk-averse society, a development well symbolized by the popularity of the “precautionary principle”, it is easier to erect barriers than to lower them. Any regulatory authority will gain more public approval from the former choice rather than from the latter.

Europe should therefore resist the temptation to promulgate broad and sweeping rules that seem based on our cherished principles and values, but that are either overextended or unrealistic. Again, a good example is the recent AI regulation proposal from the Commission. Its

¹⁷⁵ Solove, Daniel J., “Murky Consent: An Approach to the Fictions of Consent in Privacy Law”, January 22, 2023, <https://ssrn.com/abstract=4333743>

recital 17 broadly forbids “social scoring of natural persons”, likely on the basis of reports regarding the purported uses of social scoring in China. But the regulation is then forced into multiple contortions in order to allow for AI algorithms and scoring in multiple cases – criminal and judicial proceedings including through cooperation with third parties where agreements exist, credit-worthiness assessed by “small-scale providers for their own use” (Recital 37), “proceedings by tax and customs authorities” (Recital 38). At the same time, the list of safety requirements for high-risk AI systems is literally endless and could be summed up with one phrase: they should be safe. These rules will also apply to data treatment by third parties outside the European Union, starting a new chapter in the attempt by the EU to globalize its digital rules but increasing the possibility that European data remains unused.

Recommendation 6

In Europe, we must **acknowledge the strategic value of a transatlantic cross-border data agreement**. Despite the difficulties encountered through the years, a conciliation towards a renewed agreement following the Schrems rulings is necessary. After all, full convergence on democracy, values, and local rules between systems does not exist.

Another regulatory hurdle is **the potential treatment of the issues following Schrems II voiding transatlantic cooperation under the terms of the CLOUD Act and the EU’s introduction of its e-evidence package**. The Commission has signaled its support for the October 2022 White House executive order regarding signals intelligence, which attempts to resolve a key issue on intelligence collection. It is proposing a new adequacy decision that would replace the failed Privacy Shield and Safe Harbour proposals. The final review is likely to involve the European

Court of Justice and its appraisal of the Data Protection Review Court to be established. With judges appointed by the Attorney General but who cannot be removed except under very narrow exceptions, this is the closest attempt ever by the United States to create an administrative justice, in fact similar to the French system. Yet the lack of appeal to a wholly independent institution such as the US Supreme Court is likely to derail the process.

Indeed, the main criterion for cross-border data flows, rather than an abstract authoritarian/democratic divide, should be the separation of powers and the independent oversight within a regulatory space. **No full convergence on democracy, values and even less on local rules exists between systems**. It is the right to appeal and obtain redress, the requirements for information and transparency, that make the key differences. Tension exists within systems that are broadly speaking democratic. For instance, APEC’s Cross Border Privacy Rules only require self-certification without oversight and verification mechanisms.¹⁷⁶ At the same time, full equivalency is impossible – no state will grant foreign subjects the same rights and immunity from intelligence gathering that its own citizens may obtain. **In fact it is authoritarian systems which can decree or enforce equality – by denying rights to citizens and foreigners alike!**

By contrast, the proposed EU e-evidence package is meant to create a sound legal environment supplementing the long process of Mutual Legal Assistance agreements. The range of e-evidence concerned is comprehensive, including metadata, with checks and balances, including some oversight by the EU Parliament on data exchange requests. But the provision that a “European Production Order and the European Preservation Order should only be issued for specific criminal proceedings

¹⁷⁶ Access Now, “Data Free Flow with Trust and international data spaces: sustainable and successful frameworks require a focus on fundamental rights and data minimisation”, September 6, 2022, <https://www.accessnow.org/cms/assets/uploads/2022/09/Estelle-Masse-G7-speech-6-Sept-2022.pdf>

concerning a concrete criminal offense that has already taken place” (Recital 24)¹⁷⁷ seems to place much of intelligence cooperation outside this framework. The old situation – well-described in Recital 8 – is likely to prevail in those cases: **“all Member States increasingly rely on voluntary direct cooperation channels with service providers where available, applying different national tools, conditions and procedures”**.

Under the present conditions, a “Schrems III” decision voiding the Commission proposal is unfortunately a potential outcome in several years. During that interval, and likely beyond it, transatlantic data flows will continue under limited and complicated contracts, or informally. **Intelligence and police services in Europe will continue to rely on American or Five Eyes sources to complement their own insufficient data collection.** While hold-out authoritarian states are likely to resist any bilateral agreements with the United States or even the data protection requirements of an agreement such as DEPA, many others will simultaneously resist the maximalist demands from the European Union and accept more trade-based cross-border data agreements.

Recommendation 7

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

¹⁷⁷ Council of the EU, “Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings – Analysis of the final compromise text”, Document ST_5448_2023_INIT, January 20, 2023, <https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf>

This is the most sensitive issue in public opinion – sbut often misleading. **The debate should not conflate cybersecurity (safety from hacking) with legal security.** The first is contested between advocates of wide-open supply chains involving the most experienced hardware and software, and those who assert that new entrants and smaller firms can guarantee equivalent levels of security. The choice becomes harder as clouds include not only storage but also data treatment. Legal security, on the other hand, requires a supply chain whose components are not subject to another jurisdiction for requirements of data transfer. “Secure” cloud storage therefore has two different meanings.

Data localization has pros and cons. In terms of cybersecurity, the best provider also has the best ability to crack systems, so that there may not be an advantage in going for delocalized data storage, or with the most proven technical solutions. The cynics among security experts, however, will assert that this is true in any case – **absolute safety does not exist.** In terms of legal security, it is doubtful that suppliers, by creating non-affiliated companies for different jurisdictions, can wholly escape extra-territorial requirements.

One should also consider the flip side of legal security. **A global system where sanctions or data extraction would not be enforceable beyond national borders, but only through agreed replication, will be largely toothless** – except in denying access of non-compliant states, companies or individuals to the market of the country or grouping deciding the sanctions. Verification is also an integral part of sanctions. Is the European Union hostile to the financial sanctions that are allowed under the Office for Foreign Assets Control (OFAC) for the US, or to the 2017 Countering America’s Adversaries Through Sanctions Act (CAATSA)? Certainly, if the decisions for these sanctions are not conditioned by European approval or even consultation. Yet, in the absence of similar tools that would be available to the European Union, **how would Europe by itself implement sanctions against third countries or parties?** It can only do so in cooperation with the United States. Would the European Union and

its Member States benefit from their own extraterritorial leverage if they had the relevant tools at their disposal? Certainly, this would also provide them with choices that would go beyond going with the US sanctions or turning them down – a fruitless endeavor again, since US sanction decisions can be taken without consultation of allies.

Unfortunately, **extraterritorial reach is an issue that goes beyond current European constitutional provisions.** For instance, to match the US Foreign Account Tax Compliance Act (FATCA), and its very long arm due to a broad definition of what constitutes a US nexus, one would need to have a truly sovereign euro currency – whereas Treasury competences currently remain within each Member State.

Focusing on Europe’s own capacity to deploy sanctions and enforce them, including with extraterritorial data leverage, would in fact put the European Union in a better capacity to require consultation and more joint decisions. **A European participation with the United States and others through its own extraterritorial instruments would improve the collective efficiency of data extraction and sanctions.** Reciprocity between systems is one way to treat this inequality, which is mentioned in the White House executive order on signals intelligence.

Recommendation 8

The concept of “**minimization**” must be applied over two particular issues: that of data collection, where it can **reduce the risk of data breaches** in a world where absolute data security is beyond our reach; the other one concerns rule making, as **an overwhelming number of overlapping rules makes implementation harder** for both the regulated and the regulator.

Literally all expertise on data security – whether it is cybersecurity or data privacy – emphasizes that there are no absolute guarantees for preserving data confidentiality and integrity. Backdoors inside hardware components, software code, algorithms, not to mention the hydra of quantum computing defeating cryptography, mean that data security is relative. Data minimization, which provides that personal data must be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”,¹⁷⁸ is a component of data security. Yet mirror sites are also needed, since data clouds are in the end servers which are as vulnerable to incidents as any other physical structure. For international data transfers to be sustainable, data minimization is key. So are data retention time limits. After all, the less data collected, the less data to be secured or moved around. This is also consistent with the need to reduce the energy footprint of data flows.

Minimization should also apply to regulation. It is true that the complexity of ever changing digital issues and the varying requirements across sectors prevent a one-size-fits-all solution – the GDPR has been the farthest one could go in terms of top-down regulation, and it has shown the practical limits of general rules based on principle. But the proliferation of overlapping rules and regulating institutions is a challenge to users, leaving perhaps the largest companies in the best position to navigate this environment with lawyers. **One-stop-shops for consultation on rules and the permanent input from UX specialists is a necessity for public rules to be implemented fully.** An overabundance of goals and requirements increases transaction costs and can be a motive to move cutting edge innovation and data research to less demanding locations. **Rules are a tax on time, and as with taxes, too many rules kill rules.** One sometimes feels that just as the school system is sometimes meant to redress all of mankind’s inequalities, digital regulation is asked to create an ideal world of equal parties. This is unlikely to happen.

¹⁷⁸ The data minimisation principle is expressed in Article 5(1)(c) of the GDPR and Article 4(1)(c) of Regulation (EU) 2018/1725.

Recommendation 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.

A related development would be to increase the liability of hardware, software and platform suppliers to leaks and cybersecurity vulnerabilities. This is particularly an issue in the United States, where the liability is usually limited to a consumer product warranty (e.g. not extending to any wrongful use by a third party). For instance, Apple’s software license agreement’s “disclaimer of warranties” announce that the “use of the Apple software and any services performed by or accessed through the Apple software is at your sole risk and that the entire risk as to satisfactory quality, performance, accuracy and effort is with you” (7.2). But what precedes this point is also crucial since it recognizes consumer rights under local laws: “you may have legal rights in your country of residence which would prohibit the following limitations from applying to you, and where prohibited they will not apply to you” (7.1).¹⁷⁹

In practice, **the lack of strong penalties for insufficient action to prevent security leaks means that there is far less incentive for providers to invest in cybersecurity.** The European and American banking sectors are a case in point. Both GDPR, and in some Member States criminal law inflict severe penalties to protect personal banking data.¹⁸⁰

¹⁷⁹ Apple, iOS AND iPadOS SOFTWARE LICENSE AGREEMENT, https://www.apple.com/legal/sla/docs/iOS16_iPadOS16.pdf

¹⁸⁰ Banque de France, “Secret bancaire”, Updated September 28, 2022, <https://particuliers.banque-france.fr/info-banque-assurance/compte/secret-bancaire>

The European Central Bank and the European Data Protection Board both impose reserve quotas to banks guarding against the consequences of data leaks, currently estimated at 12.5% of overall bank risks on their assets. This incentive is so large as to foster the possibility that in the future, banking data leaks may disappear. By contrast, US liability laws are weak and not uniform – one reason why so many data centers are registered in Delaware. Interestingly, the Information Technology & Innovation Foundation (ITIF), which is usually critical of EU regulations, supports a federal privacy law for the United States and endorses the notion of increased platform liability to consumers for harming their data privacy rights, and advocates the inclusion of class action suits in the law.¹⁸¹ This would go a long way in practice to narrow the transatlantic gap on data uses.

Europe’s proposed Cyber Resilience Act requires providers to inform public authorities of any “known exploitable vulnerability”, to which Germany’s corporate industry body, BDI, would add a requirement for intelligence services and other public bodies to inform manufacturers of the vulnerabilities that they are aware of.¹⁸² The first requirement is also made by China’s Cyberspace Administration: Microsoft is on record¹⁸³ for pointing out that this may in fact increase the capacity of Chinese authorities to exploit these very same vulnerabilities. The second requirement is likely to be turned down by many states as concerns their intelligence services. **This shows how much mutual trust is still the most vital component of data security.**

¹⁸¹ Ashley Johnson, “Equifax Settlement Previews Likely Outcome if Congress Creates a Data Privacy Law Allowing Class Action Lawsuits”, *Information Technology and Innovation Foundation*, Innovation Files, February 17, 2023, <https://itif.org/publications/2023/02/17/equifax-settlement-previews-outcome-if-congress-creates-data-privacy-law-allowing-class-action-lawsuits/>

¹⁸² Stephen Heckler, “Cyber Resilience Act: Introducing cybersecurity requirements for products with digital elements”, *Bundesverband der Deutschen Industrie*, July 12, 2022, pp.6-7, <https://english.bdi.eu/publication/news/cyber-resilience-act>

¹⁸³ Tom Burt, “Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression”, *Microsoft*, November 4, 2022, <https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/>

Recommendation 10

We must **look beyond the sole transatlantic relationship and seek the right international format**. Solutions among like-minded, or reasonably like-minded entities are the next best option to multilateralism. Japan's proposals for its ongoing G7 presidency, which aim to be inclusive but do not push for universality, could be a promising avenue for coordinating international efforts.

None of the above will happen solely behind the closed walls of transatlantic dialogue, however necessary that is. **Third parties and markets matter a lot**. Some of them may have similar economic issues as Europe in nurturing their digital sectors or preserving data security, whether non personal or personal. Others may seek the quickest and most efficient solutions – which might as well be Chinese rather than American in many cases. All, with the exception of India, face the issue of market size and scalability, and even India understands that in spite of market size, it should not cut itself off from international sources of digital innovation.

At the same time, and particularly for cross-border data flows, a truly multilateral solution is out of reach. Authoritarian systems are influential in the UN system, and the WTO has not been retooled to face these issues. **This is not to say that common rules should not be sought at the multilateral system**, in particular to try and stop even more fragmentation. **But these rules will be very limited in scope, non-binding and not verifiable**.

From the above, and from skepticism on transatlantic relations, one might again retreat into cynicism: with added difficulties, personal and non-personal data keeps flowing across the Atlantic since Safe Harbour and Privacy Shield were invalidated. The intelligence world may be prone to believe that since “others do it too”, **there is no rule that will stop**

gentlemen from reading other people's mail, and therefore no reason to seek those rules. And the dynamics of digital and AI innovation make the search for full security very elusive.

Yet **legality matters for a good reason, if and when it is enforceable in court**: it prevents public use of wrongly collected data and sanctions illegal onward use; it allows for redress. This is the flip side of trust. The fragmentation of digital space – or case-by case bartering of data – are deeply impractical. Solutions among like-minded, or reasonably like-minded entities are the next best option. The European insistence on full value convergence and absolute legal certainty risks not being fully attractive to others. There is an even bigger risk that there is token acceptance but little implementation or compliance.

From the recent advocacy of limited, or “murky” consent to data collection,¹⁸⁴ we take the inspiration for **limited agreements that would accept a reasonable risk**. For instance, a limit on the volume of data requests across borders, and a better delimitation of their justification – between Member States also, as we have seen; transparency to users of data treatment algorithms and use of approved intermediaries avoiding conflicts of interest; time limits on the retention of non-intelligence data (it is futile to make this requirement of intel organizations), etc.; legal liability for harm resulting from onward use of data; choices for users between no further use of their personal data or monetization.

But these are piecemeal suggestions of limited value. **Far more important is to start a better coordinated international process, taking in view the dispersed initiatives and proposals that have been made previously**. In this context, the Japanese presidency proposals for their ongoing G7 presidency are currently the most interesting avenue.

¹⁸⁴ Daniel J. Solove, “Murky Consent: An Approach to the Fictions of Consent in Privacy Law”, George Washington University Law School, January 15, 2023, pp. 44-49, <http://dx.doi.org/10.2139/ssrn.4333743>

They seek to be inclusive but do not push for universality, since the basis for cooperation is trust and therefore broadly compatible political and legal systems. On priority areas such as transparency, tackling disinformation, privacy enhancing technologies (PETs), interoperability across the different data governance and user cases, Japan is presently proposing a tripartite institutional arrangement that is not equivalent to yet another international institution. **An international secretariat, perhaps based with the OECD, would work in tandem with a stakeholder panel that importantly should include representatives from business as well as digital experts, and with a government panel representing involved public stakeholders.** The goal is to facilitate the removal of regulatory and non-regulatory barriers, by testing projects such as transparency, data certification and interoperability across systems: a method that is compatible with the regulatory sandboxes currently envisaged by the European Commission. The process seeks to bring together regulators, tech experts and business practitioners.

There is an informal quality to the Japanese proposal which papers over the public-private divide, and in this respect looks more like the back and forth American processes than does the formal European separation between public and private actors. **That the origin of the proposal is Japanese is also interesting because Japan has borne the brunt of American competition in the past and isn't naive.** In the 1980s, it lost the first "chip war" to Intel before US companies decided to abandon the production side of semiconductors. Japan made a number of attempts to "go it alone" with separate standards in IT consumer industries (television, telecom). It is a large and very digitized economy and society, but it is still smaller than a truly unified European digital market could be, and it is therefore more vulnerable to issues of scale in innovation. One should add that it labors against cultural and linguistic differences that are far beyond those that exist across the Atlantic. Japan cannot act alone in this field. Because of past experiences it needs to cooperate with others on economic issues, including digital industries, as much as it does with the United States for strategic reasons.

The Japanese proposal clearly encompasses rules of the road for cross-border data flows. It is not obvious that this would extend to infrastructure and software – although the emphasis on transparency and privacy enhancing technology would indicate so. This is a distinct issue from the reciprocal data adequacy agreement that has already been reached between the EU and Japan. The last, however, forms a good basis for coordinating viewpoints on data transfers. **The OECD as a permanent secretariat – not an international organization with a power of decision – is an anchor that has already an experience in studies and propositions in the digital area.** Apart from its 38 member countries, it cooperates with five "key partners": Brazil, China, India, Indonesia, and South Africa, and has had in the past discussion about accession with Russia.

The exploration of the topic would not have been possible without the help of many friends and colleagues. The authors wish to express their gratitude, in particular, to **Anne Bouverot, Gilles Babinet, Marie-Pierre de Baillencourt, Joseph Dellatte, Mathieu Duchâtel, Jonathan Guiffard,** and **Andrew Grotto,** who have provided stimulating comments at one stage or another.

The policy paper has also benefited from the exchanges and discussions with company representatives and government officials, who have provided useful insights on a wide range of relevant issues.

Finally, the author owes much to the time and assistance provided by a number of colleagues at Institut Montaigne for making this publication possible: **Timoteo Cozzio, Claire Lemoine, Thomas Maddock, Pierre Pinhas,** and the institute's Communications Team.

*Institut Montaigne welcomes thoughts
and ideas on how to address these issues
collectively and put forward recommendations
which serve the public interest.*



ABB France	Omnium	Katalyse	Renault
Abbvie	Conseil supérieur du notariat	Kearney	Rexel
Accenture	Crédit Agricole	Kedge Business School	Ricol Lasteyrie
Accuracy	D'angelin & Co.Ltd	KKR	Rivolier
Adeo	Dassault Systèmes	KPMG S.A.	Roche
ADIT	De Pardiou Brocas	La Banque Postale	Rokos Capital Management
Aéma	Maffei	La Compagnie Fruitière	Roland Berger
Air France - KLM	DIOT SIACI	Linedata Services	Rothschild & Co
Air Liquide	Doctolib	Lloyds Europe	RTE
Airbus	ECL Group	L'Oréal	Safran
Allen & Overy	Edenred	Loxam	Sanofi
Allianz	EDF	LVMH - Moët-Hennessy	SAP France
Amazon	EDHEC Business School	- Louis Vuitton	Schneider Electric
Amber Capital	Egis	M.Charraire	Servier
Amundi	Ekimetrics France	MACSF	SGS
Antidox	Enedis	MAIF	SIER Constructeur
Antin Infrastructure Partners	Engie	Malakoff Humanis	SNCF
Archery Strategy Consulting	EQT	Mazars	SNCF Réseau
Archimed	ESL & Network	Média-Participations	SNEF
Ardian	Ethique & Développement	Mediobanca	Sodexo
Arqus	Eurogroup Consulting	Mercer	SPVIE
Astrazeneca	FGS Global Europe	Meridiam	SUEZ
August Debouzy	Fives	Michelin	Taste
Avril	Getlink	MicroPort CRM	Tecnet Participations
AXA	Gide Loyrette Nouel	Microsoft France	SARL
Baker & Mckenzie	Google	Mitsubishi France	Teneo
Bearingpoint	Groupama	S.A.S	The Boston Consulting Group
Bessé	Groupe Bel	Moelis & Company	Group
BG Group	Groupe M6	Moody's France	Tilder
BNP Paribas	Groupe Orange	Morgan Stanley	Tofane
Bolloré	Hameur Et Cie	Natixis	TotalEnergies
Bona Fidé	Henner	Natural Grass	UBS France
Bouygues	Hitachi Energy France	Nestlé	Unibail-Rodamco
Brousse Vergez	HSBC Continental Europe	OCIRP	Veolia
Brunswick	IBM France	ODDO BHF	Verlingue
Capgemini	IFPASS	Oliver Wyman	VINCI
Capital Group	Inkarn	Ondra Partners	Vivendi
CAREIT	Institut Mérieux	onepoint	Wakam
Carrefour	International SOS	Onet	Wavestone
Casino	Interparfums	Optigestion	Wendel
Chubb	Intuitive Surgical	Orano	White & Case
CIS	Ionis Education Group	Ortec Group	Willis Towers Watson
Cisco Systems France	iQo	PAI Partners	France
Clifford Chance	ISRIP	Pelham Media	Zurich
Club Top 20	Jeantet Associés	Pergamon	
CMA CGM	Jolt Capital	Pergamon	
CNP Assurances	Kantar Public	Prodware	
Cohen Amir-aslani		PwC France & Maghreb	
Compagnie Plastic		Raise	
		RATP	
		RELX Group	

Institut Montaigne
59 rue La Boétie, 75008 Paris
Tél. +33 (0)1 53 89 05 60
institutmontaigne.org/en

Imprimé en France
Dépôt légal : avril 2023
ISSN : 1771-6756

Europe is confronted with a threat and a challenge on cross-border data flows, within a fragmenting digital world. The threat is posed by authoritarian China, seeking to assert state-access to data while maintaining connection to global data flows. The challenge is posed by the digitally predominant US, whose market lead and first-mover advantages constrain the growth of European domestic challengers. In this context, debates around European digital sovereignty have gained ground, particularly as national and European policy-makers balance competing interests of free flow efficiency and protection of their data from other state actors. Multilateral efforts to regulate cross-border data flows have stumbled, facing questions of enforcement, mutual distrust, and systemic differences. From the EU's GDPR, to China's cybersecurity and data protection legislation and India's 'fence-sitting', to multi-state agreements such as DEPA, governments and other actors are increasingly opting for national or at best plurilateral solutions. With case studies of China and India as well as a focus on cloud and infrastructure issues, this policy paper takes stock of a rapidly evolving international context. From the analysis of the various facets of this debate and of existing arrangements, ten lessons for regulating cross-border data flows are drawn.

In all this, what should the EU do? The strength of its common market and renowned "Brussels effect" in exporting regulatory norms are unquestionable assets. But facing this threat and challenge, Europe must go further. The EU's steadfast commitment to data privacy sets it at odds with others, including the US, as well as challenges Europe's objective of maintaining mutual data access with international partners. As such it must step up its domestic capabilities with a common European digital space and mobilize greater funding for innovation. Skilled education, immigration, and competition policies, avoiding overregulation, adopting our own extraterritorial instruments are all more practical than a rush to tech sovereignty. Likewise – whether through transatlantic compromises or proposals such as that of Japan's Data Free Flow with Trust now at the G7 – international cooperation is key. To guarantee open data flows while upholding data security and protection, policymakers must act now, with the risk otherwise of accelerating the fragmentation of the digital arena.

10 €

ISSN : 1771-6756

NAC2304-03