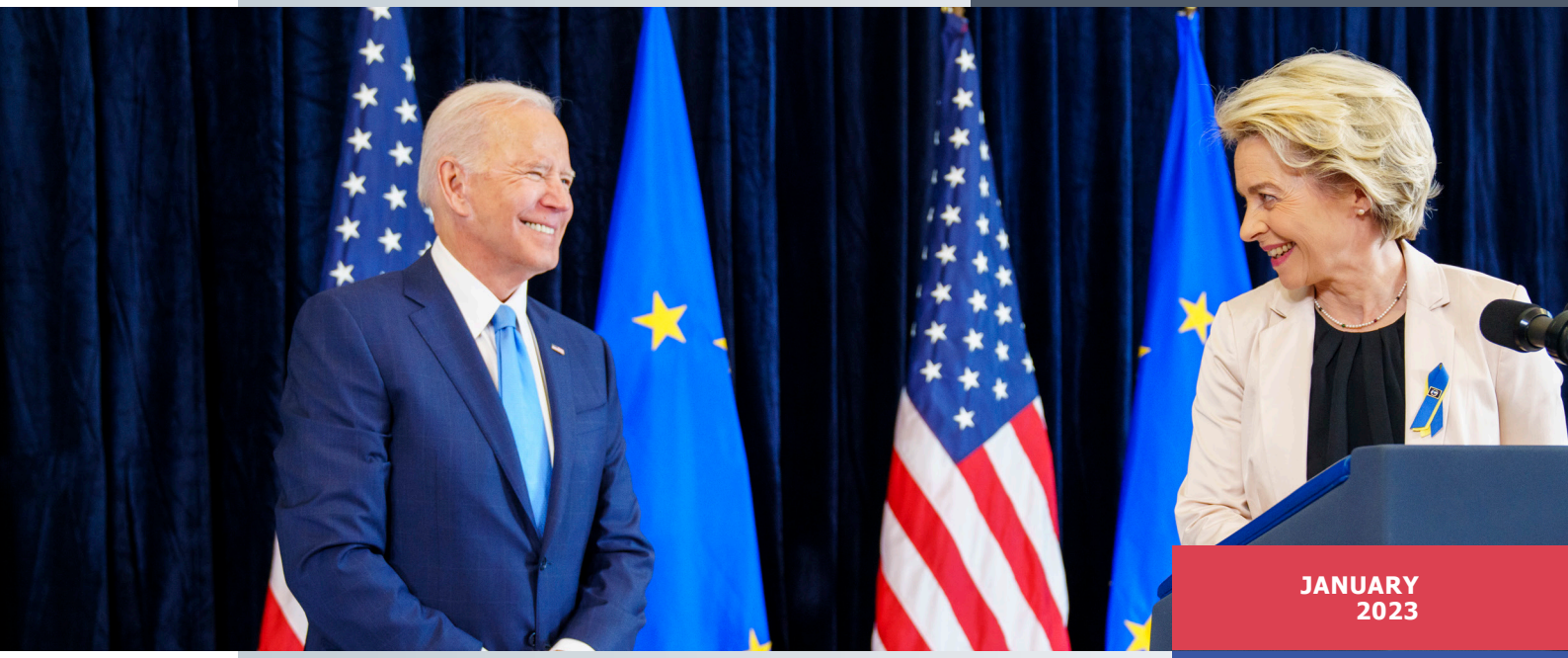
NOTES
DE L'IFRI



JANUARY
2023

Digital Sovereignty: European Policies, American Dilemmas

Mathilde VELLIET

Geopolitics of Technology Program

In partnership with:

POLICY CENTER FOR THE NEW SOUTH
THINK • STIMULATE • BRIDGE

Ifri is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit foundation according to the decree of November 16, 2022. As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience. Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

Policy Center for the New South, formerly OCP Policy Center, is a Moroccan policy-oriented think tank based in Rabat, Morocco, striving to promote knowledge sharing and to contribute to an enriched reflection on key economic and international relations issues. By offering a southern perspective on major regional and global strategic challenges facing developing and emerging countries, the Policy Center for the New South aims to provide a meaningful policy-making contribution through its four research programs: Agriculture, Environment and Food Security, Economic and Social Development, Commodity Economics and Finance, Geopolitics and International Relations.

This study has been carried out within the partnership between the French Institute of International Relations (Ifri) and Policy Center for the New South.

ISBN: 979-10-373-0673-9

Cover: © Official White House Photo by Adam Schultz

How to cite this publication:

Mathilde Velliet, "Digital Sovereignty: European Policies, American Dilemmas", *Notes de l'Ifri*, Ifri, January 2023.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

Email: accueil@ifri.org

Website: Ifri.org

Author

Mathilde Velliet is a Research Fellow within the Geopolitics of Technology program at Ifri since September 2021. Her research focuses on international issues related to new technologies, particularly American and Chinese technology policies as well as U.S.-China relations. She is also a PhD student in American civilization at the University of Paris and the University of Aix-Marseille. Her doctoral thesis focuses on U.S. policies on strategic technologies in response to the China threat under the Obama, Trump, and Biden administration.

She holds a master's degree in English studies from the École Normale Supérieure de Lyon and a master's degree in International Security from Sciences Po Paris. She also conducted research in the United States, at New York University and Boston University.

Her last publications include : "'Open' Telecom Networks (Open RAN): Towards a Reconfiguration of International Competition in 5G?", *Notes de l'Ifri*, October 2022; and "Convince and Coerce: U.S. Interference in Technology Exchanges Between its Allies and China", *Études de l'Ifri*, February 2022.

Résumé

La souveraineté numérique européenne, entendue comme « capacité de l'Europe à agir de façon indépendante dans le monde numérique », a été érigée comme priorité par la Commission d'Ursula von der Leyen. Du fait de la position privilégiée occupée par les entreprises américaines sur le marché européen, les efforts de Bruxelles en matière de souveraineté numérique sont scrutés de près par les décideurs politiques américains. Ces derniers considèrent souvent les initiatives européennes comme « protectionnistes » et ciblant injustement les entreprises américaines.

Toutefois, la vision américaine de la souveraineté numérique européenne a évolué ces dernières années sous l'influence de deux principaux facteurs. D'une part, la prise de conscience des effets et pratiques problématiques des plateformes a fait émerger un consensus sur la nécessité de réformer le secteur du numérique. D'autre part, la compétition technologique avec la Chine a été élevé au rang de priorité.

Cette vision demeure pleine de contradictions, suivant des lignes de fracture entre partis, au sein des partis, entre agences, entre États et gouvernement fédéral, et selon les sujets. La position de Washington sur la lutte contre les pratiques monopolistiques en est un exemple éclairant, caractérisé par un double discours entre volonté de réforme du secteur numérique américain sur le plan intérieur et une diplomatie active pour diluer ces efforts au niveau européen. Cependant, plusieurs acteurs américains – en particulier dans la branche législative – cherchent à tirer les leçons des succès et défaillances des réglementations européennes pour les projets de réformes américains, comme sur la régulation des plateformes ou la protection des données.

Le facteur Chine renforce l'ambiguïté de la position américaine. Il crée de nouvelles opportunités de coopération face à la perception de vulnérabilités communes (sécurité des infrastructures, investissements entrants, etc.) et face aux définitions autocratiques de la souveraineté numérique. Mais il suscite également crispation et incompréhension côté américain envers des réformes européennes ciblant davantage les entreprises américaines que chinoises.

Enfin, si les entreprises américaines et européennes se sont adaptées à l'exigence de souveraineté numérique à travers un éventail de solutions techniques et commerciales, la tentation d'une définition maximaliste de la souveraineté européenne continue de créer d'importants points d'achoppement, en particulier sur le cloud.

Abstract

European digital sovereignty, understood as "Europe's ability to act independently in the digital world", has been made a priority by Ursula von der Leyen's European Commission. Due to the privileged position of American companies in the European market, Brussels' efforts toward digital sovereignty are closely scrutinized by American policymakers. They often view European initiatives as "protectionist" and unfairly targeting U.S. companies.

However, the American vision of European digital sovereignty has evolved in recent years under the influence of two main factors. On the one hand, awareness of the problematic effects and practices of platforms has led to a consensus on the need for reform in the digital sector. On the other hand, technological competition with China has become a priority.

This vision remains fraught with contradictions, along inter-party, intra-party, inter-agency, state-federal, and issue-based fault lines. Washington's position on anti-monopolistic practices is an illuminating example, characterized by a double discourse between a desire to reform the U.S. digital sector domestically and active diplomacy to dilute these efforts at the European level. Nonetheless, several American actors – particularly in the legislative branch – are seeking to learn from the successes and flaws of European regulations for American reform projects, such as on platform regulation or privacy.

The China factor reinforces the ambiguity of the U.S.' position. It creates new opportunities for cooperation in the face of perceived common vulnerabilities (infrastructure security, inbound investments, etc.) and autocratic definitions of digital sovereignty. However, it also raises tension and misunderstanding on the American side towards European reforms that often target American companies more than Chinese ones.

Lastly, while American and European companies have adapted to the need for digital sovereignty through a range of technical and commercial solutions, the temptation of a maximalist definition of European sovereignty continues to create major stumbling blocks, particularly on the cloud.

Table of content

INTRODUCTION 6

As Seen from Washington, the Risk of a Discriminatory "Fortress Europe" 7

Two Major Developments in The United States: "Techlash" and the Chinese Threat 8

AMERICAN VS. EUROPEAN REFORMS: AMERICAN DOUBLESPEAK .. 10

Regulate or Be Regulated 11

A Divided Party and Administration: the Example of Antitrust Reform 12

EUROPEAN REFORMS, MODELS FOR U.S. REGULATION? 15

Competition Policy 15

Platform and Marketplace Regulation 16

Data Protection 16

Lessons Learned from the GDPR 17

Surveillance and Data Transfer 18

THE CHINA FACTOR IN AMERICA'S PERSPECTIVE ON EUROPEAN DIGITAL SOVEREIGNTY 20

Responding to the Chinese Threat: a Matter of European Digital Sovereignty 20

"Be Protectionist against China, not Against Us!" 22

U.S. ADAPTATION AND OPPOSITION: THE CLOUD CASE 23

Solutions for a Cloud "on Europe's Terms"... 23

... With Significant Sticking Points Remaining 24

CONCLUSION 26

Introduction

Though seldom employed in the United States, the term "digital sovereignty" – the definition of which varies – and other related concepts ("technological sovereignty," "network sovereignty," "sovereign Internet")[1] have emerged as keywords in national discourse and strategies around the world. Starting in the late 1990s, this idea was first promoted by China and then Russia as a critique of American digital hegemony (with regard to data, information flows, etc.).[2] Although the first theoretical discussion of digital sovereignty in Europe dates back to 2006,[3] the concept grew in popularity in the 2010s, first in the Member States, in the wake of Edward Snowden's revelations on American surveillance. In European Union (EU) institutions, technological sovereignty has been explicitly cited among the Commission's priorities since the beginning of Ursula von der Leyen's presidency.[4]

The purpose of this note is not to summarize the rich theoretical and political debate surrounding the definition of the concept of digital sovereignty, or the problematic nature of its application both to cyberspace, which has no real territorial borders, and to a non-national unity (the EU).[5] European digital sovereignty is understood here as "Europe's ability to act independently in the digital world".[6] This objective justifies a large number of "protective" and "offensive" policies with a variety of goals: protecting the data of Europeans, securing communication infrastructures, stimulating technological innovation, fighting online disinformation, limiting risks associated with new technologies, combating monopolistic practices in the digital world... Although it differs from the explicitly anti-American

1. J. Thumfart, "The Norm Development of Digital Sovereignty between China, Russia, the EU and the US: From the Late 1990s to the COVID Crisis 2020/21 as Catalytic Event", *Data Protection and Privacy: Enforcing Rights in a Changing World,* Dara Hallinan, Ronald Leenes and Paul De Hert (ed.), Oxford: Hart Publishing, 2022. p.3.
2. *Ibid*, p.9-15; G. Glasze et al., "Contested Spatialities of Digital Sovereignty", *Geopolitics*, 2022.
3. B. Benhamou, Bernard, and L. Sorbier. "Souveraineté et réseaux numériques", *Politique étrangère*, Ifri, vol. 71, No. 3, 2006, pp. 519-530.
4. U. Von der Leyen, "Orientations politiques pour la prochaine Commission européenne 2019-2024", 2020, available at: https://commission.europa.eu; see also Thierry Breton's remarks in "Questions to the Commissioner-Designate Thierry Breton", European Commission, 2019, available at: https://ec.europa.eu.
5. J. Thumfart, "The Norm Development of Digital Sovereignty between China, Russia, the EU and the US", *op. cit.*; G. Glasze et al., "Contested Spatialities of Digital Sovereignty", *op. cit.*; F. Douzet, "Cyberspace – the New Frontier of State Power", in S. Moisio et al. (dir.), *Handbook On The Changing Geographies Of The State: New Spaces of Geopolitics,* Cheltenham Northampton: Edward Elgar, 2020; T. Christakis, "'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest For Strategic Autonomy", *SSRN Journal*, No. 7, December 2020.
6. T. Madiega, "Digital Sovereignty for Europe", *Briefing*, European Parliamentary Research Service, July 2020.

definitions promoted by Russian and Chinese authoritarian regimes, European digital sovereignty has historically been shaped by concerns (in particular from France and Germany) over the economic dominance of large American groups, and U.S. companies' and authorities' access to European data. Considering the predominance of U.S. firms in the European digital market, the European desire to act "independently" inevitably entails focusing on the United States. This focus has been made explicit by numerous (and occasionally provocative) statements by state and European actors, such as Arnaud Montebourg, then French Minister of the Economy, who in 2014 railed against the risk of "Europe and France becoming digital colonies of the United States".[7]

As Seen from Washington, the Risk of a Discriminatory "Fortress Europe"[8]

In this context, U.S. authorities and companies were naturally critical of European efforts to strengthen digital sovereignty. These have been – since their inception and to this day – criticized for being protectionist and discriminating against U.S. firms.[9] For example, while defending Google and Facebook (targeted by Commission investigations), President Obama claimed in 2015 that the EU's response "is sometimes a mask for European protectionism" that "is just designed to carve out some of their commercial interests" because European IT firms "can't compete with ours".[10] European digital sovereignty is thus sometimes interpreted in the United States as a justification for industrial policies seeking to impose barriers to entry into the European market out of commercial interest, in order to penalize certain large U.S. firms and bolster their domestic champions.[11] According to Kenneth Propp, professor of law and senior fellow at the Atlantic Council, "in Washington, there is always a suspicion that European regulations tend toward protectionism".[12] The general perception is that Europe has a tendency to over-regulate, which is detrimental to innovation (both

7. "Interview Exclusive d'Arnaud Montebourg", Collectif David Contre Goliath, May 14, 2014, available at: www.collectif-david-contre-goliath.fr.
8. F. Burwell and K. Propp, "The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?", *Issue Brief*, Atlantic Council, June 2020.
9. F. Burwell and K. Propp, "Digital Sovereignty in Practice: the EU's Push to Shape the New Global Economy", Atlantic Council, October 2022, p.1.
10. M. Ahmed, "Obama Attacks Europe over Technology Protectionism", *Financial Times,* February 16, 2015.
11. See, for example, the positions of industry associations on the GDPR, or on European cloud certification or platform regulation projects: European Commission, "Protection des données – rapport sur le réglement général sur la protection des données", 2020, available at: https://ec.europa.eu ; U.S. Chamber of Commerce, "Comments on the European Commission's Consultation on the Digital Services Act", September 2020, available at: www.uschamber.com; American Chamber of Commerce to the European Union et al., "European Cybersecurity Certification Scheme for Cloud Services", June 14, 2022, available at: www.amchameu.eu.
12. Interview with Kenneth Propp, Washington D.C., November 30, 2022.

American and European).[13] This American perception can be explained in part by the U.S. and EU's contrasting approaches to regulation: the U.S. has traditionally tended to let technology develop and regulate the resulting issues afterwards, while Europe prefers to have a general regulatory framework in place early on.[14] U.S. detractors therefore often criticize European proposals for being overly broad or premature, and highlight the confusion and lack of harmonization caused by their proliferation.[15]

Two Major Developments in the United States: "Techlash" and the Chinese Threat

Since the late 2010s, two major developments have, however, tempered the American narrative on European digital sovereignty.

Firstly, U.S. confidence and optimism concerning technology and its democratic value have clearly deteriorated. Up to the Obama administration, U.S. digital foreign policy, and a relatively laisser-faire domestic regulatory policy, were rooted in the conviction that digitization was tied to democratization. However, in the wake of the failed Arab Springs, foreign interference via digital tools (most notably Russia's in the 2016 U.S. elections), and revelations of large-scale surveillance by platforms[16] and states, this perception has become more critical,[17] with a growing political will to regulate the digital sector more carefully. This varies widely depending on the subject, however (competition, data protection, content moderation, etc.). No consensus has yet emerged on the content of these regulations, and it is a source of division within the Republican and Democratic parties. Although diverse, this desire for reform draws closer to European efforts in this area, from which it sometimes draws inspiration.

Then, under the Trump and Biden administrations, the perception of a Chinese threat grew significantly and propelled "great-power competition" to the forefront of American foreign and domestic policy.[18] Although sovereignty is not a term that is employed in the United States, the identification of new vulnerabilities associated with Chinese technological

13. J. Lewis, in B. Dekker and M. Okano-Hijmans (dir.), *Dealing with China On High-Tech Issues: Views From The US, EU And Like-Minded Countries In A Changing Geopolitical Landscape*, Clingendael Report, December 2020, p. 14.
14. See, for example, L. Movius and N. Krup, "U.S. and EU Privacy Policy: Comparison of Regulatory Approaches", *International Journal of Communication,* No. 3, 2009; B. Smith, in "Les chemins de la puissance européenne", *Revue européenne du droit*, vol. 3, December 2021, p. 144.
15. European Commission, "Protection des données – rapport sur le réglement général sur la protection des données", *op. cit*; M. Scott, "Digital Bridge: Trade and Tech Council stand-off", *Politico*, October 30, 2022, available at: www.politico.eu.
16. S. Zuboff, *L'âge du capitalisme de surveillance,* Zulma, 2020.
17. J. Thumfart, "The Norm Development of Digital Sovereignty between China, Russia, the EU and the US", *op. cit.*; Interview with a U.S. Senate advisor, Washington D.C., November 10, 2022.
18. D. Trump, "National Security Strategy of the United States of America", December 2017, p. 27.

capabilities (e.g., in telecom infrastructure or applications) and the need to "preserve American technological leadership" can be seen in policies that sometimes resemble European efforts to establish digital sovereignty.

These two factors are crucial to understand America's perspective on European digital sovereignty. How can the contradictions this perspective implies be understood? What consequences do these developments, amid new tensions and opportunities for cooperation, have on transatlantic relations?

This paper focuses on the actors and factors that shape the U.S. perspective on European policies in this area. It first examines the reasons for the apparent contradiction between the desire to reform the U.S. digital sector domestically and the active diplomacy to dilute these efforts at the European level. Some U.S. actors, however, are attempting to apply the lessons learned from European regulatory successes and failures to U.S. reform projects. In its third part, this paper examines the importance of China as a factor in the American perspective on European digital sovereignty and its consequences on transatlantic relations. Finally, while American and European private actors have developed solutions to address the need for sovereignty, its maximalist interpretation continues to crystallize a categorical opposition on certain subjects across the Atlantic.

American vs. European Reforms: American Doublespeak

The gradual emergence in recent years of a political consensus on the need to reform the U.S. digital sector has created a seemingly contradictory double discourse on the part of U.S. authorities.

On the domestic front, the Biden administration and part of Congress have shown their willingness to better regulate "Big Tech" and its practices with regard to monopolies, data capture, or content moderation.[19] This objective is in many ways similar to what the EU has been doing in the name of digital sovereignty. In the words of the president of Microsoft on the subject of digital market regulation,

> "If you look closer to the policy proposals today coming from the Biden administration, the legislation coming out of the House Judiciary Committee, and so on, the discussions are remarkably similar. Even if on one side of the Atlantic a company is a gatekeeper and on the other side it is an essential trading partner, what regulators are worried about is the same thing: potential bottlenecks in the digital economy".[20]

However, on the international front, Washington has actively pursued diplomacy to slow down and dilute European efforts to reform the sector, such as the Digital Market Act (DMA) and Digital Services Act (DSA). American misgivings about the DMA – pointing to its discriminatory nature and the risks to innovation and cybersecurity – have been repeatedly expressed: by the White House, by Commerce Secretary Gina Raimondo, by American negotiators in transatlantic talks, and in certain inter-agency documents sent to members of the European Parliament.[21]

This was further supported by some 30 Representatives from both parties in a letter to the Biden Administration issued in February 2022.[22]

---

19. See, for example: The White House, "Readout of White House Listening Session on Tech Platform Accountability", September 8, 2022, available at: www.whitehouse.gov.
20. B. Smith, in "Les chemins de la puissance européenne", *op. cit.*, p. 144.
21. J. Espinoza, "US Warns EU against Anti-American Tech Policy", *Financial Times*, June 15, 2021; M. McGill and A. Gold, "The Biden Administration's Tightrope Act on Tech", *Axios*, December 9, 2021; S. Stolton, "US Pushes to Change EU's Digital Gatekeeper Rules", *Politico*, January 31, 2022.
22. S. DelBene et al., "Letter on the EU's Digital Markets Act", February 23, 2022, available at: https://delbene.house.gov.

This contradiction can be explained both by a kind of rivalry to be in charge of digital regulation and by the divisions existing within the Democratic Party and even the Biden administration.

Regulate or Be Regulated

The first factor explaining this contradiction is the – historically entrenched – American reluctance to see U.S. companies subjected to external (in this case European) regulation, in an interesting echo to the concept of sovereignty.

For some, this reluctance reflects a form of skepticism toward the EU's political legitimacy. Jim Lewis, a prominent researcher at the Center for Strategic and International Studies (CSIS), captures this in one question: "Who appointed Brussels to be the global regulator? [...] Brussels is not elected. So it lacks legitimacy in a way. And Brussels has no oversight on national security, which is an ongoing problem".[23] Brussels can also easily be suspected of advancing protectionist and anti-American regulations. Some American elected officials (especially Republicans), who are quite hostile to "Big Tech" and in favor of more binding regulations (for instance against monopolistic practices), are nonetheless opposed to European regulations in this area, in part out of suspicion towards the EU.[24] An interview with President Trump in 2019 illustrates this clearly: on the issue of the EU Commission's fines imposed on Google and Facebook, Donald Trump says that the European negotiator "hates the United States" and that "they think there's a monopoly, but I'm not sure that they think that, they just figure this is easy money". However, he goes on to admit that "there is something going on in terms of monopoly" and that considering the money collected through these fines, the United States "should do what [the EU is] doing!"[25] Beyond this assessment's contradictions, it appears the former president's analysis of the monopolistic practices of tech companies falls close to that of the EU, yet he objects to European regulation because he believes that regulation and financial penalties should be left to U.S. authorities.

This aversion to seeing U.S. companies subjected to European regulation has grown in recent years with the perception that the U.S. has missed the opportunity to be the leader in digital regulation. While Europe proved surprisingly capable of asserting itself as a political and normative actor by adopting complex reforms relatively quickly, the failure of American projects paralyzed by institutional deadlock (and the influence of private interest groups) stands in stark contrast, and is a cause for concern.

23. Interview with Jim Lewis, vice president and director of the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS), Washington D.C., November 14, 2022.
24. Interview with Aurelien Portuese, Ph.D., director of the Schumpeter Project on Competition Policy at the Information Technology & Innovation Foundation (ITIF), Washington D.C., December 1, 2022. See, for example, Republican Senators Josh Hawley and Orrin Hatch (Senator until 2019, who passed away last April).
25. Donald Trump, on "Squawk Box", *CNBC*, June 10, 2019, available at: www.cnbc.com.

Especially after a Trump administration that did little to engage with Europe on these issues, the United States has been slow to respond to European plans and now finds itself having to implement an increasing number of regulations that it did not have a hand in formulating. The frustration associated with this lack of American regulatory leadership explains – at least in part – certain actors' reservations about European reforms, even when they approve of their terms.

A Divided Party and Administration: the Example of Antitrust Reform

Beyond this form of regulatory rivalry, the U.S. authorities' doublespeak can also be explained by the disagreements that divide the Democratic Party (as well as the Republican Party) and even the current administration.

The parties are divided internally on many of the issues associated with digital sovereignty ambitions in Europe (antitrust, online content moderation, data, etc.), and reforms are backed by surprising bipartisan coalitions. For example, reform proposals to restrict U.S. agencies' access to data and surveillance are supported by both progressives and Freedom Caucus libertarians.[26] On content moderation, the possibility of removing or narrowing the scope of Section 230 of the Communications Decency Act (which grants providers immunity from liability for content posted by users) has been supported – for different reasons – by members of the Biden administration and elected officials from both parties.[27]

Likewise, combating monopolistic practices – especially by large digital platforms – is of great interest to certain senators, whether progressive (e.g., Elisabeth Warren), center-left (e.g., Amy Klobuchar), or very conservative (e.g., Mike Lee, Josh Hawley, Ted Cruz).[28] This issue divides both parties, generally opposing radical elected officials (Republicans and Democrats who are very hostile to "Big Tech", often for very different reasons) and so-called pro-business representatives (such as Democrats in California and Washington State and some moderate Republicans).

These intra-party differences are reflected in the congressional analysis of European reforms. Certain Democratic representatives (like Suzan DelBene, Stacey Plaskett, or Bradley Schneider) have opposed several

26. See this paper's "Surveillance and Data Transfer" section.
27. M. Reardon, "Democrats and Republicans Agree that Section 230 is Flawed", *CNET*, June 21, 2020, available at: www.cnet.com; M. Perault, "After Dobbs, Democrats and Republicans Switch Places on Speech Policy", *Lawfare*, July 28, 2022, available at: www.lawfareblog.com.
28. B. Brody, "Republican Tech Skeptics Are Flirting With Progressives' Choice For Antitrust Chief", *Protocol*, April 20, 2021; E. Warren, "At Hearing, Warren Pushes for Stronger Antitrust Laws to Protect Economy, Consumers, Workers, and Data Privacy", December 7, 2021, available at: www.warren.senate.gov; L. Green, "Antitrust: Hawley And Klobuchar On The Big Tech Battles To Come", *The Guardian*, May 2, 2021.

congressional antitrust bills[29] and the European DMA, and "support[ed] the administration's recent engagement to encourage the European Union to revise [it]".[30] Other Democrats, like Senators Warren and Klobuchar, actively support both.[31] In addition to their enthusiastic depiction of the DMA, Elizabeth Warren's letters to Commerce Secretary Gina Raimondo denounce the contradiction between the Commerce Department's critical stance on the DMA and the reform agenda announced by the Biden administration.[32]

Within the Biden administration, attitudes toward the DMA have been mixed. While the Commerce Department (supported by major tech companies and business lobbies such as the U.S. Chamber of Commerce[33]) has sought to have the DMA revised, other agencies such as the Federal Trade Commission (FTC) and the Justice Department have shown it more support. In a speech in Brussels, FTC Chairwoman Lina Khan called the DMA "a significant proposal to promote fair access to markets controlled by digital gatekeepers" (and did not mention that the targeted gatekeepers would be mainly American).[34] Assistant Attorney General Jonathan Kanter, in charge of the Justice Department's Antitrust Division, also underscored the alignment between European and U.S. reforms, and that he "look[s] forward to working closely with EVP Vestager and our friends at the European Commission as they implement the Digital Markets Act".[35]

Rather than an aberrant contradiction, the divergence in U.S. authorities' positions is part of the normal bureaucratic game, in which agencies pursue different and sometimes antithetical missions. As spearheads of antitrust reform under the Biden administration with close interactions with their European counterparts, the FTC and the Department of Justice were naturally better informed and more supportive of the DMA than the Department of Commerce, whose role is to promote and preserve the activities of American businesses.

29. "New Democrat Coalition Leadership Members Urge Leadership and House Judiciary to Hold Legislative Hearings on Upcoming Antitrust Legislation", New Democrat Coalition, June 12, 2021, available at: https://newdemocratcoalition.house.gov.
30. S. DelBene et al., "Letter on the EU's Digital Markets Act", *op. cit.*
31. A. Klobuchar, *Antitrust: Taking on Monopoly Power from the Gilded Age to the Digital Age*, Knopf, 2021; E. Warren, "Letter to The Honorable Gina Raimondo", December 14, 2021; E. Warren, "Letter to The Honorable Gina Raimondo", March 4, 2022.
32. See, for example, G. Raimondo, "U.S.-EU Partnerships: Transatlantic Goals and Priorities", U.S. Chamber of Commerce, December 8, 2021, available at: www.uschamber.com.
33. L. Nylen and S. Stolton, "U.S. Slow to Respond to EU's Landmark Tech Regulation", *Politico*, March 25, 2022; C. Goujard, "Big Tech Accused of Shady Lobbying in EU Parliament", *Politico*, October 14, 2022. It should be noted, however, that the chairman of Microsoft Brad Smith has publicly supported the DMA: B. Smith, in "Les chemins de la puissance européenne", *op. cit.*, p. 141.
34. L. Khan, "Remarks of Chair Lina M. Khan", Charles River Associates Conference, Brussels, March 31, 2022, available at: www.ftc.gov.
35. J. Kanter, "Solving the Global Problem of Platform Monopolization", 49th Annual Conference on International Antitrust Law and Policy, Fordham Competition Law Institute, New York, September 16, 2022, available at: www.justice.gov; J. Kanter, "Competition & Regulation in Disrupted Times", Charles Rivers Associates Conference, Brussels, March 31, 2022, available at: www.crai.com.

Beyond the DMA, bureaucratic disputes and the lack of an effective inter-agency process for international digital policy account for some of the inconsistencies in the U.S.'s position.[36] This adds to the reluctance of a section of the political establishment to see Silicon Valley subjected to external regulation. These two elements help explain the apparent contradictions in the positions of the executive branch and Congress on European digital sovereignty, despite a sometimes similar desire for reform.

36. Interview with Frances Burwell, distinguished fellow at the Atlantic Council and senior director at McLarty Associates, Washington D.C., November 30, 2022.

European Reforms, Models for U.S. Regulation?

Among the supporters of this desire for reform in the American digital sector, some draw inspiration and lessons from what has been done on the Old Continent in recent years in the name of European digital sovereignty. However, te points of interest identified and the potential for implementation into the U.S. system vary depending on the subject matter.

Competition Policy

To address monopolistic practices, some actors affirm their willingness to draw inspiration from Europe. Law professor Tim Wu, brought in by President Biden as special assistant for competition and technology policy,[37] wrote in 2018:

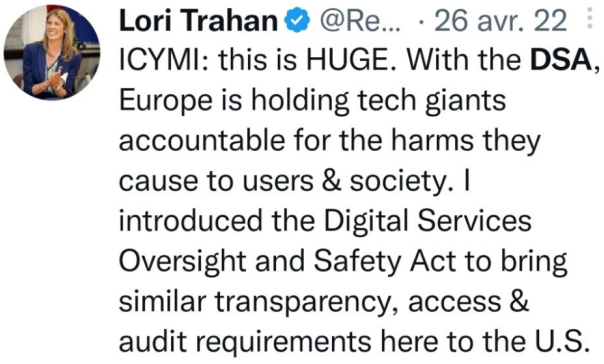
> "It is here, among other places, that America can borrow from Europe [...]. Europe now leads in the scrutiny of "big tech," including [Google and Apple]. European antitrust is far from perfect, but its leadership and willingness to bring big cases when competition is clearly under threat should serve as a model for American enforcers and for the rest of the world."[38]

This interest in the European model has been reflected in legal texts: the American Innovation and Choice Online Act proposed by Senator Klobuchar incorporates many elements of the DMA.[39] The bill takes inspiration in particular from the DMA's quantitative threshold system, an asymmetrical form of regulation that only targets the largest actors.[40] Given the private sector's opposition and congressional disagreements, the bill's adoption seems highly uncertain, however, and antitrust developments may instead be determined by case law and litigation brought by the FTC.

37. In office for two years, Mr. Wu left his position in the Biden administration on January 4, 2023.
38. T. Wu, *The Curse of Bigness: Antitrust in the New Gilded Age*, Columbia Global Reports, 2018, p. 131.
39. U.S. Congress, *S. 2992 - American Innovation and Choice Online Act,* introduced October 18, 2021, available at: www.congress.gov.
40. Interview with Aurélien Portuese, Washington, D.C., December 1, 2022; S. Heather, "Striking Similarities: Comparing Europe's Digital Markets Act to the American Innovation and Choice Online Act", U.S. Chamber of Commerce, June 17, 2022, available at: www.uschamber.com.

Platform and Marketplace Regulation

The second part of the European legislative package on digital services – the Digital Services Act (DSA) – has generated less opposition from the U.S. than the DMA. The DSA's focus on transparency is well-received in the United States, and some of its features (e.g., verification of third-party vendors or mandatory auditing of risk management systems by platforms) seem to have piqued the interest of political actors in Washington. Some analysts argue that the Digital Services Oversight and Safety Act[41] introduced in the House in February 2022 was even drafted as a true "American translation of the DSA".[42] Lori Trahan, the Democratic Representative who introduced the bill, embraces this similarity, as evidenced by her reaction to the DSA's adoption in April 2022:



Source: twitter.com

While some aspects of this bill could be inserted into other legislation being debated in Congress (such as the American Data Privacy and Protection Act) or into FTC regulations, its adoption as such seems very unlikely, in a context of strong partisan tensions on content moderation issues.[43]

Data Protection

Another central topic in transatlantic discussions on digital technology is the issue of access to data (both by private platforms and national security agencies) and privacy protection, which is now the subject of significant debate in the United States. These debates draw on regulations already adopted abroad, in particular the General Data Protection Regulation (GDPR) that has been in place in the EU since 2018 and is considered a pioneering measure in this area.

41. U.S. Congress, *H.R.6796 - Digital Services Oversight and Safety Act of 2022*, introduced February 18, 2022, available at: www.congress.gov.
42. Interview with Nathalie Maréchal, policy director at Ranking Digital Rights, Washington D.C., December 2, 2022.
43. To simplify, Democrats are concerned about disinformation and the proliferation of hateful content online while Republicans object to moderation by platforms perceived to disadvantage conservatives (or even censor them).

Lessons Learned from the GDPR

In the absence of a general federal framework, several states – like California, Colorado, Connecticut, Virginia, or Utah – have adopted their own data protection legislation in recent years.[44] Lessons learned from the GDPR were therefore first translated into U.S. laws at the state level, in particular in the California Consumer Privacy Act (CCPA) passed in 2018 and effective since 2020.

The debate in Washington over the last few months on the proposed federal data protection scheme[45] has drawn on the European (and Californian) experiences. According to Kevin Diamond, deputy chief of staff to a Democratic Representative heavily invested in consumer rights and privacy issues, the GDPR has shifted the discussion on several fronts.[46] The GDPR introduced repeated requests for consent for data collection on every new web page, a burdensome requirement. In response, U.S. lawmakers are considering, for example, a model of minimum guarantees for certain basic rights – a major, bipartisan development. Also, while individuals' right to sue businesses for data breaches ("private right of action") was portrayed by some at the GDPR's inception as paving the way to an avalanche of litigation, this ultimately did not materialize, emboldening U.S. politicians who supported it. Finally, federal lawmakers have heard the private sector's grievances about the complexity of dealing with national regulators in all 27 member states – within the general framework of the GDPR – who each have their own philosophies and perspectives. This feedback drew the attention of members of Congress to the risks associated with a federal text with too weak a preemption clause, especially in a context where several states have adopted (or will adopt) their own data protection laws.[47] This explains the American private sector's strong support for a federal data protection law, which would be far more reliable and advantageous than a patchwork of state-specific laws.

More generally, certain ideas have grown in acceptance over the past four years of the GDPR's implementation, prompting U.S. businesses to call for an equivalent across the Atlantic. The GPDR's very existence (but also China's data governance regime) is regularly touted as evidence that Washington is falling behind on this issue.

---

44. A. Desai, "US State Privacy Legislation Tracker, International Association of Privacy Professionals, October 7, 2022, available at: https://iapp.org.
45. Mainly the *American Data Privacy and Protection Act* (ADPPA, H.R. 8152), introduced June 21, 2022, available at: www.congress.gov.
46. Interview with Kevin Diamond, Deputy Chief of Staff in charge of technology and digital affairs for Representative Lisa Rochester, Washington, D.C., November 28, 2022.
47. Preemption is the power of the federal government to nullify or supersede a state law in favor of a federal law. This is the main point of contention in current talks over the ADPPA, Californian Democrats refusing to back a federal law that would preempt their CCPA. L. Zabierek et al., "Preemption in Federal Data Security and Privacy Legislation", Belfer Center for Science and International Affairs, Harvard Kennedy School, June 14, 2022, available at: www.belfercenter.org; J. Duball, "State views on proposed ADPPA preemption come into focus", International Association of Privacy Professionals, September 27, 2022, available at: https://iapp.org.

Surveillance and Data Transfer

To a lesser extent, European concerns about U.S. agencies' surveillance of their citizens – a key issue in early debates on European digital sovereignty – have also had some resonance in Washington.

The majority of elected officials in the U.S. have strongly criticized the decisions of the Court of Justice of the European Union (CJEU), annulling transatlantic data transfer agreements. However, some have responded not by trying to reassure the EU that there are no surveillance programs but by condemning them and calling for their revision. For example, Democratic Senator Ron Wyden stated in 2015:

> "By striking down the Safe Harbor Agreement, the European Union Court of Justice today called for open season against American businesses. This misguided decision amounts to nothing less than protectionism against America's global data processing services and digital goods. [...] Yet, U.S. politicians who allowed the National Security Agency to secretly enact a digital dragnet of millions of phone and email records also bear responsibility. [...] [B]y helping the European Courts to strike [the Safe Harbor agreement] down, short-sighted politicians have seriously damaged American businesses. Congress needs to start taking the next steps on surveillance reform now [...]."[48]

In 2015, as now, members of both parties[49] in favor of surveillance reform include in their arguments the issue of data transfers with Europe, and European restrictions imposed in the name of digital sovereignty (and privacy).[50]

It should be noted, however, that a large number of American officials and businesses tend to point out, in the face of European criticism, the (real but limited) progress made by the American system in this area in recent years.[51] The European idea that the American regime provides less protection against surveillance by national security agencies is thus portrayed as a misunderstanding.

48. R. Wyden, "Wyden Blasts EU 'Safe Harbor' Ruling", October 6, 2015, available at: www.wyden.senate.gov.

49. One example of bipartisan cooperation on this issue is the amendment proposed in 2020 by Democratic Senator Wyden and Republican Senator Daines during debates on Section 215 of the *PATRIOT Act*, or the *Fourth Amendment is Not For Sale Act* proposed in April 2021 by Senator Wyden and Republican Rand Paul. E. Goitein, "Surprising Senate Vote Signals New Hope for Surveillance Reform", Brennan Center for Justice, May 16, 2020, available at: www.brennancenter.org; R. Wyden, "Wyden, Paul and Bipartisan Members of Congress Introduce The Fourth Amendment Is Not For Sale Act", April 21, 2021, available at: www.wyden.senate.gov.

50. On this topic, see also: T. Wetzling, L. Sarkesian and C. Dietrich, "Solving the Transatlantic Data Dilemma: Surveillance Reforms to Break the International Gridlock", Stiftung Neue Verantwortung, December 2021.

51. See for example C. Chin, "The EU-U.S. Data Privacy Framework: More Steps Needed to Repair Trust in Data Flows", CSIS, October 24, 2022.

Particularly in an American context dominated by competition with China, European misgivings surrounding data transfers may resonate even more strongly with American concerns… but are seen as picking the wrong target. As one congressional aide put it, "I feel like the concerns the EU and some privacy advocates have about our surveillance system are similar to the concerns I and others have about downloading TikTok".[52] The popularity on both sides of the Atlantic of major Chinese digital platforms (like ByteDance, which owns TikTok), which have been accused of transferring citizens' data to the authorities, gives new weight to concerns about foreign governments' access to the data of millions of citizens. The United States itself has adopted several restrictions in recent months to address this risk. These include President Trump's Executive Order 13942 "Addressing the Threat Posed by TikTok," revoked by President Biden's Executive Order 14034 "Protecting Americans' Sensitive Data from Foreign Adversaries," or the bipartisan bill passed by Congress in December 2022 banning TikTok on all government-owned devices.

This comparison reveals an increasingly important factor in America's perspective on digital sovereignty: China.

52. Interview with an advisor in the House of Representatives, Washington D.C., November 2022.

The China Factor in America's Perspective on European Digital Sovereignty

Since the Trump administration, the American political class (both executive and legislative) has ratcheted up competition with China, considered the United States' main threat, as a high priority. This analysis has major implications for U.S. digital and technology policies, including with respect to its European ally.

The rise of China's technological might leads Washington to recognize new vulnerabilities and justifies implementing reforms similar to certain European digital sovereignty aspirations. The issue of TikTok and data protection is a case in point, as are the debates on both sides of the Atlantic about misinformation and over-reliance on foreign suppliers in certain critical sectors. However, the focus on "great power competition" also makes U.S. businesses' competitiveness (including, or even especially, in digital and technology) a national security concern. This argument, which the private sector has widely promoted, emphasizes the risk that regulation (whether American or European) could slow down innovation – and thus penalize American competitive leadership.[53] The China factor thus overlaps with other previously mentioned criteria in the constitution of bipartisan groups, whether pro-industry, pro-growth, anti-China or against European regulations.

Responding to the Chinese Threat: a Matter of European Digital Sovereignty

Washington looks very favorably on European digital sovereignty measures that are primarily (though implicitly) aimed at China and resemble U.S. policies.

The desire to protect European high-tech companies from certain acquisitions is an integral part of European digital sovereignty ambitions.[54] Concerned about the sharp increase in European company takeovers by investors from China, Hong Kong, and Macau, the European Union adopted

53. This argument was, for example, advanced by Mark Zuckerberg and Sheryl Sandberg, the founder and COO, respectively, of Facebook (now Meta), and Eric Schmidt, former CEO of Google. K. Wagner, "Mark Zuckerberg Says Breaking Up Facebook Would Pave The Way For China's Tech Companies To Dominate", *Vox*, July 18, 2018, and N. Tiku, "Big Tech: Breaking Us Up Will Only Help China", *Wired*, May 23, 2019.
54. T. Madiega, "Digital sovereignty for Europe", *op. cit.*

new regulations to tighten oversight over inbound foreign investments.[55] These efforts resemble what has happened in the United States since 2018, when the committee in charge of screening inbound foreign investment was strengthened,[56] and can be seen as "an opportunity to further align the U.S.-EU partnership".[57]

More recently, the European Commission has planned in its 2023 work program to "examine whether additional tools are necessary in respect of outbound strategic investments controls".[58] This sentence is aimed in particular at investments in strategic Chinese sectors, and seems informed by the debate that has stirred in Congress and the White House in recent months on this subject.[59] This process – in the EU and in the Member States – is therefore clearly backed by Washington. Democratic Senator Bob Casey, co-author of a bipartisan outbound investment controls bill, for example, said he was "encouraged to see Germany considering the kind of outbound investment screening I've been urging here in America with my National Critical Capabilities Defense Act".[60]

In their diplomatic relations with their allies, when stressing the risks posed by China, U.S. authorities have occasionally framed the issue in terms of sovereignty themselves. Mike Pompeo, U.S. Secretary of State under Donald Trump, undertook an aggressive campaign to convince Europe (among others) to exclude Chinese suppliers deemed to be a risk,[61] stressing the importance of this decision for national sovereignty.[62]

Where European digital sovereignty is understood as "Europe's ability to act independently" of China, the United States supports and may even promote it, which presents opportunities for transatlantic cooperation. These are bolstered by the United States and the EU's desire to promote a technological agenda that reflects their shared values

55. See for example the regulation in effect since October 20: "2017/0224 (COD) Screening of Foreign Direct Investments into the European Union", Legislative Observatory, European Parliament, 2023, available at https://oeil.secure.europarl.europa.eu. It should be noted, however, that final decisions concerning investment controls are the responsibility of the member states.
56. U.S. Congress, *Foreign Investment Risk Review Modernization Act of 2018*, passed on August 13, 2018.
57. S. Erickson, "Recent Developments in EU Foreign Investment Screening", CSIS, April 19, 2021.
58. European Commission, "Commission Work Programme 2023: A Union Standing Firm and United", COM (2022) 548, Strasbourg, October 18, 2022, p. 8.
59. S. Aarup, "China Beware! Europe Eyes Closer Control Over How Firms Invest Abroad", *Politico*, January 3, 2023; U.S. Senate, "Examining Outbound Investment", Hearing before the U.S. Senate Committee on Banking, Housing and Urban Affairs, September 29, 2022, available at: www.banking.senate.gov.
60. B. Casey, tweet from November 23, 2022, available at: https ://twitter.com.
61. M. Velliet, "Convince and Coerce: U.S. Interference in Technology Exchanges Between its Allies and China", *Étude de l'Ifri,* February 2022, available at: www.ifri.org.
62. For example in Slovenia or the UK: S. Lau, "US Secretary of State Mike Pompeo Secures Slovenia Support for 'Clean Network' Campaign against Chinese Technology", *South China Morning Post*, August 14, 2020; C. Skopeliti, "UK Sovereignty in Jeopardy if Huawei Used for 5G, US Warns", *The Guardian,* January 27, 2020.

(democracy, human rights, open internet, etc.),[63] as a counter to the more centralizing and autocratic approach to digital sovereignty favored by Russia and China.[64]

"Be Protectionist Against China, not Against Us!"

However, on other issues more relevant to U.S. businesses, Washington's heightened perception of a Chinese threat reinforces the sense of injustice that characterizes the U.S. response to European initiatives. Many U.S. public and private actors find it difficult to understand why they would burden U.S. businesses with additional regulations, while Chinese companies (e.g., Alibaba, ByteDance, WeChat), which present more security concerns, are not. As one Congressional aide puts it, the question in Washington "is less about everything being non-protectionist, but more about 'who are we trying to protect ourselves *from*?' [...] If you [Europeans] are going to be protectionist, be protectionist against China, not against us!".[65] This American position combines two criticisms: the EU's laxity toward China and the clear anti-Americanism of European digital sovereignty. For instance, that the DMA's definition of "gatekeepers" could potentially only cover the Big Five (Google, Apple, Facebook, Amazon, Microsoft) has been sharply criticized by the United States, despite the justification that their position in the European market far outweighs that of Chinese companies.[66]

The China factor thus accentuates the ambiguity of the U.S.'s stance on European digital sovereignty and its impact on industrial policy. As one American researcher and former official puts it,

> "the US has mixed feelings about [innovation policy] development in the EU: welcoming it as a counterweight to China, which is a national security rationale; but objecting to it if it is seen as disadvantaging US companies, which is a competitiveness concern."[67]

Perhaps the most striking example of how U.S. public and private sectors have expressed opposition to – and adapted to – the perceived disadvantages of European restrictions is the case of cloud computing.

63. European Commission, "Le Conseil du commerce et des technologies UE-États-Unis relève des défis communs et fait face aux crises mondiales", December 5, 2022, available at: https://ec.europa.eu.
64. J. Thumfart, "The Norm Development of Digital Sovereignty between China, Russia, the EU and the US", *op. cit.*
65. Interview with an advisor in the House of Representatives, Washington D.C., November 2022.
66. J. Espinoza, "US Warns EU against Anti-American Tech Policy", *op. cit.*; J. Espinoza, "EU Should Focus on Top 5 Tech Companies, Says Leading MEP", *Financial Times,* May 31, 2021.
67. W. Reinsch, in B. Dekker and M. Okano-Hijmans (dir.), *Dealing with China on High-Tech Issues, op. cit.,* p. 7.

U.S. Adaptation and Opposition: the Cloud Case

Given the EU's concerns about strategic dependencies and U.S. authorities' access to European data, the fact that 80 percent of Old-World data is hosted by non-European cloud providers is seen as an economic, political and cybersecurity issue.[68] To address this issue and ensure Europe's "data sovereignty" for personal and non-personal data, EU institutions have drafted new regulations in recent years. These regulations – like the GDPR, the Data Act, the Data Governance Act, or the EU Cybersecurity Act – contain measures both to liberalize Europe's data market, in order to foster its development, and to limit data transfers outside the EU. The restrictive measures are explicitly justified by the risks posed by U.S. and Chinese laws, whose extraterritorial reach can force certain cloud service providers to grant their authorities access to European data.[69]

Solutions for a Cloud "on Europe's Terms"…

In response to this new sovereignty objective in national and European regulatory requirements, private American and European actors have developed a wide range of technical, commercial and organizational solutions. There is in fact a certain convergence of interests between the two: American cloud service providers want to remain in the European market, and it is not in the interest of European companies to lose access to the cutting-edge services of hyperscalers. Several solutions have therefore been proposed to benefit from the performance offered by the leading American cloud services (Google Cloud, Microsoft Azure, Amazon's AWS) while protecting European data from extraterritorial laws.

Different data encryption techniques have been put forward, including some which allow customers to store their data in the cloud without the service

68. A. Pannier, "The Changing Landscape of European Cloud Computing Gaia-X, the French National Strategy, and EU Plans", *Briefing de l'Ifri*, Ifri, July 22, 2021.
69. The European Commission's impact assessment report on the *Data Act* specifically cites U.S. Presidential Executive Order 12333, the *Foreign Intelligence Surveillance Act* (FISA), the U.S. CLOUD Act, and China's 2017 National Intelligence Law. European Commission, "Impact Assessment Report Accompanying the Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data", Brussels, February 23, 2022, p. 21.

provider having access to it. These encryption solutions are part of the "sovereign control" offered by U.S. companies as part of their commitments to European digital sovereignty, such as "Microsoft Cloud for Sovereignty"[70] or Google's "Cloud on Europe's Terms".[71]

Other approaches involve combining cloud providers (a "hybrid cloud" combining public and private clouds, or a "multi-cloud" with multiple public cloud providers) to provide different levels of security and data protection. Some of these offers, namely in France, rely on partnerships between American and French companies. One example is the creation of Bleu, announced in 2021: a joint venture controlled by French shareholders that will use cloud computing services provided by Microsoft, with data hosted by Orange and Capgemini locally in France.[72] Google and Thalès presented a similar cloud solution, S3NS, in June 2022.[73] Bleu and S3NS were both designed to qualify for the SecNumCloud label issued by the French National Agency for Information Systems Security (ANSSI), which would entitle them to the "trusted cloud" designation.

… With Significant Sticking Points Remaining

However, this French certification and its European counterpart are facing strong opposition from the U.S. private and public sectors (notably the Department of Commerce and Treasury).

Firstly, officials and analysts in the United States see SecNumCloud as a way to force the development of joint ventures, likening the certification to predatory practices by China.[74] Moreover, U.S. stakeholders expressed concern in early 2022 over the lack of an initial definition (also pointed out by the Commission) of "sensitive data", as well as a list of which public agencies would require the label. The United States fears that France may adopt a very broad definition of what qualifies as "sensitive" (well beyond military data, for example), and that it may extend the SecNumCloud certification requirement beyond the public sector to public companies or even the entire private sector.[75]

70. C. Sanders, "Microsoft Cloud For Sovereignty: The Most Flexible And Comprehensive Solution For Digital Sovereignty", Official Microsoft Blog, July 19, 2022, available at: https://blogs.microsoft.com.

71. A. Fox-Martin, "Advancing Digital Sovereignty On Europe's Terms", Google Cloud, October 13, 2022, available at: https://cloud.google.com.

72. A. Vitard, "Bleu, le "cloud de confiance" d'Orange, Microsoft et Capgemini sera opérationnel en 2024", *L'Usine Digitale*, June 22, 2022.

73. A. Vitard, "Thales lance S3NS, son offre de "cloud de confiance" avec Google", *L'Usine Digitale*, June 30, 2022.

74. Interviews with researchers, officials and companies, Washington, November 2022; N. Cory, ""Sovereignty Requirements" in French —and Potentially EU— Cybersecurity Regulations", ITIF, December 10, 2021.

75. This fear is fueled by French authorities' ambiguous political statements on the issue. French Minister Bruno Le Maire said last September, for instance, "if our *businesses* holding exceptionally

U.S. concerns also extend to the European Union Cybersecurity Certification Scheme on Cloud Services (EUCS) being developed by the EU Cybersecurity Agency, which may follow the lines of the French criteria. France is indeed heavily involved in the development of the EUCS, and SecNumCloud 3.2 (which "sets out criteria for protection against extra-European laws") "serves as a reference in the development of this future [EU] certification's 'high' rating".[76] France, Germany, Italy, and Spain support an EUCS design that would contain a requirement for immunity from non-European laws: only cloud providers located in Europe and not subject to control by foreign entities would be certifiable.[77] Other member states (e.g., the Netherlands, Sweden, Ireland, Greece, Poland) question the need for a sovereignty criterion, which is also much decried by the United States.[78] The fact that the EUCS was discussed during U.S. Trade Representative Katherine Tai's call with EU Trade Commissioner Valdis Dombrovskis in September 2022 speaks to its importance at the top levels of the Biden administration.[79]

Though far from being universally supported in Europe, the maximalist conception of digital sovereignty – which would only entrust Europeans' data to European cloud providers totally independent from non-European laws – thus remains a point of contention.

sensitive data do not voluntarily embrace this [SecNumCloud] offer to secure their data, I cannot rule out that, at some point, we may need to resort to a *mandatory* standard to protect our industrial sovereignty". B. Le Maire, "Discours sur la stratégie nationale pour le Cloud", Strasbourg, September 12, 2022.

76. "L'ANSSI actualise le référentiel SecNumCloud", ANSSI, March 8, 2022.

77. A. Vitard, "Divergences autour des exigences de souveraineté dans le schéma européen de certification du cloud", *L'Usine Digitale*, June 20, 2022; K. Propp, "European Cybersecurity Regulation Takes a Sovereign Turn", European Law Blog, September 12, 2022, available at: https://europeanlawblog.eu.

78. American Chamber of Commerce to the EU et al., "European Cybersecurity Certification Scheme for Cloud Services", *op. cit.*; L. Cerulus, "Big Tech Cries Foul over EU Cloud-Security Label", *Politico*, June 14, 2022.

79. K. Tai, "Readout of Ambassador Katherine Tai's Call with European Commission Executive Vice President Valdis Dombrovskis", Office of the U.S. Trade Representative, September 1, 2022, available at: https://ustr.gov.

Conclusion

The dual evolution of the American analysis on the need to reform the digital sector and prevail in its technological competition against China has therefore transformed the United States' perspective on European digital sovereignty. This perspective is still fraught with contradictions, along party lines, within parties, between agencies, between states and the federal government, and across issues. It generates new opportunities for cooperation (against large platforms with abusive practices, or against autocratic definitions of digital sovereignty), mutual enrichment of legal and regulatory frameworks, but also real tensions.

Nearly ten years after the term first appeared in official policy language, the definition of European digital sovereignty and its policy implications are still poorly understood across the Atlantic. This is due in part to some degree of reluctance from certain affected U.S. firms, and a lack of understanding and involvement on the subject in Congress. However, this is also a direct consequence of the persistent vagueness (partly due to disagreements among member states) about what digital sovereignty means for the EU. Whether this is a failure of communication or deliberate political ambiguity, certain statements by European political figures, with hints of anti-Americanism, continue to feed the suspicions of American public and private actors about the EU's objectives.[80]

This persistent lack of clarity makes it all the more necessary to hold bilateral talks, for example within the framework of the Trade and Technology Council, as well as within European bodies and with American businesses, in order to address the contradictory demands arising from the digital sovereignty objective.[81]

Despite these contradictions and tensions, the current U.S. administration's Europhile stance and call for bipartisan unity "against Big Tech abuses"[82] represents a window of opportunity for transatlantic rapprochement on these issues – one that may not last.

---

80. The most frequently cited in Washington (late 2022) is that of European MP Andreas Schwab, rapporteur for the DMA. See J. Espinoza, "EU Should Focus on Top 5 Tech Companies, Says Leading MEP", *Financial Times*, May 31, 2021. See also B. Le Maire, "Discours sur la stratégie nationale pour le Cloud", Strasbourg, September 12, 2022.

81. For example, issues surrounding privacy and competition (and the European authorities associated with their protection) sometimes lead to conflicting positions on the need for companies to share their data.

82. J. Biden, "Unite Against Big Tech Abuses", *Wall Street Journal,* January 12, 2023.

27 rue de la Procession 75740 Paris Cedex 15 – France

Ifri.org