



HAL
open science

Souveraineté numérique : politiques européennes, dilemmes américains

Mathilde Velliet

► **To cite this version:**

Mathilde Velliet. Souveraineté numérique : politiques européennes, dilemmes américains. Notes de l'Ifri, 2023. hal-03968950

HAL Id: hal-03968950

<https://hal.science/hal-03968950>

Submitted on 14 Feb 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

**NOTES
DE L'IFRI**



**JANVIER
2023**

Souveraineté numérique : politiques européennes, dilemmes américains

4ifri
depuis
1979

Programme
Géopolitique des
technologies

Mathilde VELLIET

En partenariat avec:



L'**Ifri** est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une fondation reconnue d'utilité publique par décret du 16 novembre 2022. Elle n'est soumise à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux. L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

Le **Policy Center for the New South**, anciennement OCP Policy Center, est un *think tank* marocain basé à Rabat, Maroc, qui a pour mission la promotion du partage de connaissances et la contribution à une réflexion enrichie sur les questions économiques et les relations internationales. À travers une perspective du Sud sur les questions critiques et les grands enjeux stratégiques régionaux et mondiaux auxquels sont confrontés les pays en développement et émergents, Policy Center for the New South offre une réelle valeur ajoutée et vise à contribuer significativement à la prise de décision stratégique à travers ses quatre programmes de recherche : agriculture, environnement et sécurité alimentaire, économie et développement social, économie et finance des matières premières, géopolitique et relations internationales.

Les opinions exprimées dans ce texte n'engagent que la responsabilité de l'auteur.

Cette note a été réalisée dans le cadre du partenariat entre l'Institut français des relations internationales (Ifri) et le Policy Center for the New South.

ISBN : 979-10-373-0664-7

© Tous droits réservés, Ifri, 2023

Couverture : © Official White House Photo by Adam Schultz

Comment citer cette publication :

Mathilde Velliet, « Souveraineté numérique : politiques européennes, dilemmes américains », *Notes de l'Ifri*, Ifri, janvier 2023.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

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

E-mail : accueil@ifri.org

Site internet : ifri.org

Auteure

Mathilde Velliet est chercheuse au sein du programme Géopolitique des technologies, qu'elle a rejoint en septembre 2021. Ses travaux portent sur les enjeux internationaux liés aux nouvelles technologies, en particulier les politiques technologiques américaines et chinoises et les relations sino-américaines. Elle poursuit un doctorat en civilisation américaine à l'Université de Paris : ses recherches analysent la fabrique des politiques américaines de protection des technologies stratégiques sous les administrations Obama et Trump.

Mathilde Velliet est diplômée d'un master en Études Anglophones de l'École Normale Supérieure de Lyon et d'un master en Sécurité Internationale de Sciences Po Paris, et a effectué deux séjours de recherche aux États-Unis, à l'université de New York puis à l'université de Boston.

Elle a récemment publié pour l'Ifri : « Les réseaux télécoms “ouverts” (Open RAN). Vers une reconfiguration de la compétition internationale dans la 5G ? » (*Notes de l'Ifri*, octobre 2022) et « Convaincre et contraindre : les interférences américaines dans les échanges technologiques entre leurs alliés et la Chine » (*Études de l'Ifri*, février 2022).

Remerciements

L'auteure remercie Rubén Pépin pour son aide à la recherche.

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 élevée 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 towards 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.

Sommaire

| | |
|---|-----------|
| INTRODUCTION | 6 |
| Vu de Washington, une tendance à « l'Europe forteresse » discriminatoire..... | 7 |
| Deux évolutions majeures : « techlash » et menace chinoise | 8 |
| RÉFORMES AMÉRICAINES VS. EUROPEÉNNES : LE DOUBLE DISCOURS AMÉRICAIN | 10 |
| Réguler ou être régulé | 11 |
| Un parti et une administration divisés : l'exemple des réformes antitrust | 12 |
| LES RÉFORMES EUROPÉENNES, MODÈLES POUR LA RÉGULATION AMÉRICAIN ? | 15 |
| Politique de concurrence | 15 |
| Régulation des plateformes et <i>marketplaces</i>..... | 16 |
| Protection des données | 16 |
| <i>Tirer les leçons du RGPD.....</i> | <i>17</i> |
| <i>Surveillance et transferts de données</i> | <i>18</i> |
| LE FACTEUR CHINE DANS LA VISION AMÉRICAIN DE LA SOUVERAINETÉ NUMÉRIQUE EUROPÉENNE..... | 20 |
| Répondre à la menace chinoise : un enjeu de souveraineté numérique européenne..... | 20 |
| « Soyez protectionnistes contre la Chine, pas contre nous ! » | 22 |
| ADAPTATION ET OPPOSITION AMÉRICAIN : L'EXEMPLE DU CLOUD | 24 |
| Des solutions pour un cloud « aux conditions de l'Europe »... .. | 24 |
| ... Avec encore d'importants points d'achoppement | 25 |
| CONCLUSION | 28 |

Introduction

Très peu usités aux États-Unis, le terme de « souveraineté numérique » – dont la définition est à géographie variable – et ses autres proches concepts (« souveraineté technologique », « souveraineté des réseaux », « internet souverain »)¹ sont devenus des mots-clés dans les discours et stratégies nationales à travers le monde. À partir de la fin des années 1990, cette notion est promue d’abord par la Chine puis par la Russie comme une critique de l’hégémonie numérique américaine (en matière de données, de flux d’information, etc.)². Si la première discussion théorique sur la souveraineté numérique en Europe date de 2006³, c’est surtout au cours des années 2010 que le concept gagne en popularité, d’abord dans les États membres, dans la lignée des révélations d’Edward Snowden sur la surveillance américaine. Dans les institutions européennes, dès les débuts de la présidence d’Ursula Von der Leyen, la souveraineté technologique est explicitement citée parmi les priorités de la nouvelle Commission⁴.

L’objectif de cette note n’est pas de résumer le riche débat théorique et politique autour de la définition de la notion de souveraineté numérique, ou du caractère problématique de son application à la fois à un cyberspace sans réelles frontières territoriales et à une unité non-nationale (l’Union européenne (UE))⁵. La souveraineté numérique européenne est comprise ici comme « la capacité de l’Europe à agir de façon indépendante dans le monde numérique »⁶. Cet objectif justifie un grand nombre de politiques « protectrices » et « offensives » aux objectifs variés : protéger les données des Européens, sécuriser les infrastructures de communication, stimuler

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, et L. Sorbier. « Souveraineté et réseaux numériques », *Politique étrangère*, Ifri, vol. 71, n° 3, 2006, pp. 519-530.

4. U. Von der Leyen, « Orientations politiques pour la prochaines Commission européenne 2019-2024 », 2020, disponible sur : <https://commission.europa.eu> ; voir aussi les propos de Thierry Breton, dans « Questions to the Commissioner-Designate Thierry Breton », European Commission, 2019, disponible sur : <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. Moisis 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*, n° 7, décembre 2020.

6. T. Madiega, « Digital Sovereignty for Europe », *Briefing*, European Parliamentary Research Service, juillet 2020.

l'innovation technologique, lutter contre la désinformation en ligne, limiter les risques liés aux nouvelles technologies, lutter contre les pratiques monopolistiques dans le numérique... Bien que différent des définitions explicitement anti-américaines promues par les régimes autoritaires russe et chinois, la souveraineté numérique européenne s'est historiquement construite à partir de préoccupations (en particulier françaises et allemandes) quant à la domination économique des grands groupes américains et à l'accès d'entreprises et autorités américaines aux données des Européens. À la lumière de la prédominance des entreprises américaines sur le marché numérique européen, la volonté européenne de pouvoir agir « de façon indépendante » implique inévitablement de tourner son regard vers les États-Unis. Cette direction a été explicitée par les nombreuses déclarations (parfois provocatrices) d'acteurs étatiques et européens, comme Arnaud Montebourg, alors ministre français de l'Économie, qui en 2014 s'insurgeait contre le risque que « l'Europe et la France deviennent les colonies numériques des États-Unis⁷ ».

Vu de Washington, une tendance à « l'Europe forteresse⁸ » discriminatoire

Dans ce contexte, les autorités et entreprises américaines ont assez logiquement été critiques des efforts européens de renforcement de la souveraineté numérique. Ceux-ci sont – depuis leurs débuts et encore aujourd'hui – accusés d'être protectionnistes et discriminatoires envers les entreprises américaines⁹. Par exemple, défendant Google et Facebook (visés par des enquêtes de la Commission), le président Obama affirmait en 2015 que la réponse de l'UE « masquait parfois le protectionnisme européen » qui « n'a pour but que de préserver certains de leurs intérêts commerciaux », car les entreprises européennes du numérique « ne peuvent rivaliser avec les nôtres¹⁰ ». La souveraineté numérique européenne est ainsi parfois interprétée aux États-Unis comme la justification d'une politique industrielle visant à imposer des barrières à l'entrée du marché européen par intérêt commercial, pour pénaliser certaines grandes entreprises américaines et renforcer des champions nationaux¹¹. Selon Kenneth Propp, professeur de

7. « Interview Exclusive d'Arnaud Montebourg », Collectif David Contre Goliath, 14 mai 2014, disponible sur : www.collectif-david-contre-goliath.fr.

8. F. Burwell et K. Propp, « The European Union and the Search for Digital Sovereignty: Building “Fortress Europe” or Preparing for a New World? », *Issue Brief*, Atlantic Council, juin 2020.

9. F. Burwell et K. Propp, « Digital Sovereignty in Practice: the EU's Push to Shape the New Global Economy », Atlantic Council, octobre 2022, p.1.

10. M. Ahmed, « Obama attacks Europe over Technology Protectionism », *Financial Times*, 16 février 2015.

11. Entre autres exemples, voir les positions des associations industrielles sur le RGDP, ou sur les projets européens de certification cloud ou de régulation des plateformes : Commission européenne, « Protection des données – rapport sur le règlement général sur la protection des données », 2020, disponible sur : <https://ec.europa.eu> ; U.S. Chamber of Commerce, « Comments on the European Commission's Consultation on the Digital Services Act », septembre 2020, disponible sur :

droit et chercheur à l'Atlantic Council, « à Washington, la suspicion est toujours que les réglementations européennes tendent vers le protectionnisme¹² ». En outre, l'Europe est perçue comme ayant une tendance excessive à la régulation, ce qui nuit à l'innovation (américaine comme européenne)¹³. Cette perception américaine s'explique notamment par la différence d'approche en matière de régulation entre les États-Unis et l'UE : les États-Unis ont traditionnellement tendance à laisser la technologie se développer et à réguler *a posteriori* les problèmes spécifiques qui en découlent, tandis que l'Europe préfère disposer d'un cadre réglementaire général assez tôt¹⁴. Les critiques américaines pointent donc souvent le caractère excessivement large ou prématuré des propositions européennes, ainsi que l'incertitude et le manque d'harmonisation provoqués par leur multiplication¹⁵.

Deux évolutions majeures aux États-Unis : « techlash » et menace chinoise

Depuis la fin des années 2010, deux évolutions majeures ont cependant nuancé le discours américain sur la souveraineté numérique européenne.

Tout d'abord, la confiance et l'optimisme américains dans les technologies et leurs bienfaits démocratiques se sont nettement dégradés. Jusqu'à l'administration Obama, la conviction d'un lien entre numérisation et démocratisation fondait la politique extérieure numérique américaine et autorisait une politique intérieure de relatif laisser-faire réglementaire. Cependant, dans la lignée de l'échec des Printemps arabes, des ingérences étrangères grâce aux outils numériques (en particulier celle de la Russie dans les élections américaines de 2016), et des révélations sur la surveillance à grande échelle mise en place par les plateformes¹⁶ et les États, cette perception s'est faite plus critique¹⁷. Elle s'est accompagnée d'une volonté politique croissante de mieux réglementer le secteur du numérique.

www.uschamber.com ; American Chamber of Commerce to the European Union et. al., « European Cybersecurity Certification Scheme for Cloud Services », 14 juin 2022, disponible sur www.amchameu.eu.

12. Entretien avec Kenneth Propp, Washington D.C., 30 novembre 2022.

13. J. Lewis, in B. Dekker et 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, décembre 2020, p. 14.

14. Voir par exemple L. Movius et N. Krup, « U.S. and EU Privacy Policy: Comparison of Regulatory Approaches », *International Journal of Communication*, n° 3, 2009 ; B. Smith, dans « Les chemins de la puissance européenne », *Revue européenne du droit*, vol. 3, décembre 2021, p. 144.

15. Commission européenne, « Protection des données – rapport sur le règlement général sur la protection des données », *op. cit.* ; M. Scott, « Digital Bridge: Trade and Tech Council stand-off », *Politico*, 30 octobre 2022, disponible sur 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.* ; Entretien avec une conseillère au Sénat américain, Washington D.C., 10 novembre 2022.

Celle-ci varie toutefois fortement selon les sujets (concurrence, protection des données, modération des contenus...). Elle ne s'est pas traduite par un consensus sur le contenu de ces régulations et divise les partis républicain et démocrate en leur sein. Bien que plurielle, cette volonté de réforme se rapproche des efforts européens en la matière, dont elle tire parfois des éléments d'inspiration.

Ensuite, sous les administrations Trump et Biden, la perception d'une menace chinoise a considérablement augmenté et a propulsé la « compétition entre grandes puissances » au rang de priorité de la politique extérieure et intérieure américaine¹⁸. Sans que le terme de souveraineté ne soit employé aux États-Unis, l'identification de nouvelles vulnérabilités liées à la puissance technologique chinoise (dans les infrastructures télécoms ou les applications par exemple) et la nécessité de « préserver le leadership technologique américain » se déclinent en politiques parfois proches des efforts européens visant la souveraineté numérique.

Ces deux facteurs sont décisifs pour comprendre la vision américaine de la souveraineté numérique européenne. Comment expliquer les contradictions qui sous-tendent cette vision ? Quelles conséquences ont ces évolutions sur la relation transatlantique, entre nouvelles tensions et opportunités de coopération ?

La présente note se concentre sur les acteurs et facteurs qui déterminent la vision américaine des politiques européennes en la matière. Elle analyse d'abord les raisons de l'apparente contradiction entre la volonté de réforme du secteur numérique américain sur le plan intérieur et la diplomatie active pour diluer ces efforts au niveau européen. Certains acteurs américains cherchent toutefois à tirer les leçons des succès et défailances des réglementations européennes pour les projets de réformes américains. En troisième partie, cette note détaille l'importance du facteur Chine dans la vision américaine de la souveraineté numérique européenne et ses conséquences sur la relation transatlantique. Enfin, si les acteurs privés américains et européens ont développé des solutions pour répondre à l'exigence de souveraineté, la conception maximaliste de celle-ci continue de cristalliser une totale opposition outre-Atlantique sur certains sujets.

18. D. Trump, « National Security Strategy of the United States of America », décembre 2017, p. 27.

Réformes américaines vs. européennes : le double discours américain

La formation progressive ces dernières années d'un consensus politique sur la nécessité de réformer le secteur numérique américain a créé un double discours des autorités américaines, en apparence contradictoire.

Sur le plan intérieur, l'administration Biden et une partie du Congrès ont affiché leur volonté de mieux réguler la « *Big Tech* » et ses pratiques en matière de monopoles, de captation des données, ou de modération des contenus¹⁹. Cette ambition se rapproche à bien des égards de ce qui est fait par l'UE au nom de la souveraineté numérique. Comme le résume le président de Microsoft au sujet de la régulation des marchés numériques,

« si vous regardez de plus près les propositions politiques de l'administration Biden, la législation qui émane de la *U.S. House Committee on the Judiciary*, et ainsi de suite, les discussions sont remarquablement similaires. Même si, d'un côté de l'Atlantique, une est un contrôleur d'accès au marché et, de l'autre, un partenaire commercial essentiel, ce qui inquiète les régulateurs est la même chose : les goulets d'étranglement potentiels dans l'économie numérique²⁰. »

Cependant, sur le plan extérieur, Washington a déployé une diplomatie cherchant activement à freiner et diluer les efforts européens de réforme du secteur, comme les règlements sur les marchés et les services numériques (*Digital Market Act* (DMA) et *Digital Services Act* (DSA)). Les réticences américaines vis-à-vis du DMA – qui soulignent son caractère discriminatoire et les risques pour l'innovation et en matière de cybersécurité – ont ainsi été exprimées à maintes reprises : par la Maison Blanche, la Secrétaire au Commerce Gina Raimondo, les négociateurs américains dans les discussions transatlantiques, ou encore dans certains documents interagences envoyés aux membres du Parlement européen²¹.

19. Voir par exemple : The White House, « Readout of White House Listening Session on Tech Platform Accountability », 8 septembre 2022, disponible sur www.whitehouse.gov.

20. B. Smith, dans « Les chemins de la puissance européenne », *op. cit.*, p. 144.

21. J. Espinoza, « US Warns EU against Anti-American Tech Policy », *Financial Times*, 15 juin 2021 ; M. McGill et A. Gold, « The Biden Administration's Tightrope Act on Tech », *Axios*, 9 décembre 2021 ; S. Stolton, « US Pushes to Change EU's Digital Gatekeeper Rules », *Politico*, 31 janvier 2022.

Cette démarche a en outre été soutenue par une trentaine de Représentants des deux partis dans une lettre à l'administration Biden publiée en février 2022²².

Cette contradiction s'explique à la fois par une forme de rivalité pour être le régulateur du numérique et par les divisions qui existent au sein du parti démocrate et même de l'administration Biden.

Réguler ou être régulé

Le premier facteur expliquant cette contradiction est la réticence américaine – historiquement ancrée – de voir les entreprises américaines soumises à une régulation extérieure (en l'occurrence européenne), dans un écho intéressant au concept de souveraineté.

Cette méfiance reflète pour certains une forme de scepticisme quant à la légitimité politique de l'UE. Jim Lewis, influent chercheur au *Center for Strategic and International Studies* (CSIS), l'illustre en une question : « Qui a nommé Bruxelles régulateur mondial ? [...] Bruxelles n'est pas élu. Donc il manque de légitimité d'une certaine manière. Et Bruxelles n'a pas de contrôle sur la sécurité nationale, ce qui est un problème constant²³. » Bruxelles est en outre facilement suspecté de proposer des régulations protectionnistes et anti-américaines. Certains élus américains (notamment républicains), qui sont assez hostiles à la « *Big Tech* » et favorables à une régulation plus contraignante – par exemple en matière de lutte contre les pratiques monopolistiques, sont pourtant opposés aux règlements européens en la matière, en partie par suspicion envers l'UE²⁴. Une interview du président Trump en 2019 l'illustre clairement : sur la question des amendes infligées par la Commission à Google et Facebook, Donald Trump affirme que le négociateur européen « déteste les États-Unis » et que celui-ci « ne pense pas qu'il y a vraiment un monopole, il pense juste que c'est de l'argent facile ». Il poursuit cependant en confessant qu'« il y a quelque chose qui se passe en termes de monopole » et qu'au vu de l'argent récolté par ces amendes, les États-Unis « devraient faire ce que [l'UE] fait²⁵ » ! Au-delà de l'analyse contradictoire, il apparaît donc que l'ancien président partage une analyse proche de celle de l'UE sur les pratiques monopolistiques des entreprises de la tech, mais s'oppose à la régulation européenne car il souhaite que l'élaboration des règles et les pénalités financières reviennent aux autorités américaines.

22. S. DelBene et. al., « Letter on the EU's Digital Markets Act », 23 février 2022, disponible sur : <https://delbene.house.gov>.

23. Entretien avec Jim Lewis, vice-président et directeur du programme Strategic Technologies au Center for Strategic and International Studies (CSIS), Washington D.C., 14 novembre 2022.

24. Entretien avec Aurélien Portuese, docteur en droit et directeur du Schumpeter Project on Competition Policy à l'Information Technology & Innovation Foundation (ITIF), Washington D.C., 1^{er} décembre 2022. Voir par exemple les sénateurs républicains Josh Hawley et Orrin Hatch (sénateur jusque 2019, décédé en avril dernier).

25. Donald Trump, dans « Squawk Box », *CNBC*, 10 juin 2019, disponible sur www.cnbcm.com.

Cette réticence à voir les entreprises américaines soumises à la régulation européenne s'est accrue ces dernières années avec l'impression d'avoir laissé passer l'opportunité d'être le chef de file de la réglementation du numérique. Face à une Europe qui a surpris par sa capacité à s'affirmer comme acteur politique et normatif en adoptant des réformes complexes relativement rapidement, l'échec des projets américains paralysés par le blocage des institutions politiques (et l'influence des groupes d'intérêts privés) contraste et inquiète. En particulier après une administration Trump peu investie dans les négociations avec l'Europe sur ces sujets, les États-Unis ont mis du temps à réagir aux projets européens et font face à l'obligation d'appliquer un nombre croissant de règles qu'ils n'ont pas contribué à élaborer. La frustration liée à cette absence de leadership régulateur américain explique – au moins en partie – la réserve de certains acteurs quant aux réformes européennes, même lorsqu'ils en approuvent le contenu.

Un parti et une administration divisés : l'exemple des réformes antitrust

Outre cette forme de rivalité régulateur, le double discours des autorités américaines s'explique par les divergences qui morcellent le parti démocrate (tout comme le parti républicain), et même l'administration en place.

Sur bon nombre de sujets associés en Europe à l'ambition de souveraineté numérique (*antitrust*, modération des contenus en ligne, données, etc.), les partis sont divisés en leur sein et les réformes portées par d'étonnantes coalitions bipartisanes. Les tentatives de réformes pour réduire l'accès aux données et la surveillance par les agences américaines sont par exemple soutenues à la fois par des progressistes et des libertariens du Freedom Caucus²⁶. Sur la modération des contenus, la possibilité de supprimer ou réduire la portée de la Section 230 du *Communications Decency Act* (qui reconnaît l'absence de responsabilité des hébergeurs quant aux contenus mis en ligne par les utilisateurs) a été défendue – pour des raisons différentes – par des membres de l'administration Biden et des élus des deux partis²⁷.

De même, la lutte contre les pratiques monopolistiques – surtout des grandes plateformes numériques – suscite un fort intérêt chez les sénateurs progressistes (comme Elisabeth Warren), de centre gauche (comme Amy Klobuchar), mais aussi chez les très conservateurs (Mike Lee, Josh Hawley, Ted Cruz)²⁸. Cette question divise les deux partis, opposant en général les

26. Voir la section « Surveillance et transferts de données » de la présente note.

27. M. Reardon, « Democrats and Republicans Agree that Section 230 is Flawed », *CNET*, 21 juin 2020, disponible sur : www.cnet.com ; M. Perault, « After Dobbs, Democrats and Republicans Switch Places on Speech Policy », *Lawfare*, 28 juillet 2022, disponible sur : www.lawfareblog.com.

28. B. Brody, « Republican Tech Skeptics Are Flirting With Progressives' Choice For Antitrust Chief », *Protocol*, 20 avril 2021 ; E. Warren, « At Hearing, Warren Pushes for Stronger Antitrust Laws to Protect Economy, Consumers, Workers, and Data Privacy », 7 décembre 2021, disponible

élus radicaux (républicains et démocrates très hostiles à la « Big Tech », souvent pour des raisons très différentes) aux élus dits *pro-business* (comme les démocrates californiens et de l'État de Washington ou certains républicains modérés).

Ces divergences intrapartisanes se déclinent dans l'analyse des réformes européennes par le Congrès. Certains représentants démocrates (comme Suzan DelBene, Stacey Plaskett, ou Bradley Schneider) se sont opposés à plusieurs projets de loi *antitrust* du Congrès²⁹ et au DMA européen, et « soutienn[ent] l'engagement récent de l'administration pour encourager l'Union européenne à [le] réviser³⁰ ». D'autres Démocrates, comme les sénatrices Warren et Klobuchar, soutiennent les deux³¹. Outre leur description enthousiaste du DMA, les lettres d'Elizabeth Warren à la Secrétaire au Commerce Gina Raimondo dénoncent la contradiction entre la position critique du département du Commerce sur le DMA et l'agenda réformateur annoncé par l'administration Biden³².

Au sein de l'administration Biden, les positions sur le DMA se sont avérées contrastées. Si le département du Commerce (soutenu par les grandes entreprises de la tech et lobbys commerciaux comme la *U.S. Chamber of Commerce*³³) s'est efforcé de faire réviser le DMA, d'autres agences comme la Commission fédérale du commerce (*Federal Trade Commission* (FTC)) et le département de la Justice s'y sont montrés plus favorables. Dans un discours à Bruxelles, la présidente de la FTC, Lina Khan, qualifie ainsi le DMA de « proposition importante pour promouvoir l'accès équitable aux marchés contrôlés par les *gatekeepers* numériques » (sans évoquer que les *gatekeepers* visés seront principalement américains)³⁴. Le procureur général assistant Jonathan Kanter, en charge de la division *antitrust* du département de la Justice, a également souligné l'alignement entre les réformes européennes et américaines et sa « motivation à travailler

sur : www.warren.senate.gov ; L. Green, « Antitrust: Hawley And Klobuchar On The Big Tech Battles To Come », *The Guardian*, 2 mai 2021.

29. « New Democrat Coalition Leadership Members Urge Leadership and House Judiciary to Hold Legislative Hearings on Upcoming Antitrust Legislation », New Democrat Coalition, 12 juin 2021, disponible sur : <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 », 14 décembre 2021 ; E. Warren, « Letter to The Honorable Gina Raimondo », 4 mars 2022.

32. Voir par exemple G. Raimondo, « U.S.-EU Partnerships: Transatlantic Goals and Priorities », U.S. Chamber of Commerce, 8 décembre 2021, disponible sur : www.uschamber.com.

33. L. Nylen et S. Stolton, « U.S. Slow To Respond To EU's Landmark Tech Regulation », *Politico*, 25 mars 2022 ; C. Goujard, « Big Tech Accused of Shady Lobbying in EU Parliament », *Politico*, 14 octobre 2022. Notons toutefois que le président de Microsoft Brad Smith a publiquement soutenu le 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, Bruxelles, 31 mars 2022, disponible sur : www.ftc.gov.

étroitement avec la Vice-Présidente Vestager et nos amis de la Commission européenne dans le cadre de la mise en œuvre du *Digital Markets Act*³⁵ ».

Moins qu'un aberrant contresens, les divergences dans la position des autorités américaines relèvent du jeu bureaucratique normal, dans lequel les agences ont des missions différentes et parfois antithétiques. Fers de lance des réformes *antitrust* sous l'administration Biden aux interactions étroites avec leurs homologues européens, la FTC et le département de la Justice étaient naturellement mieux informés et plus favorables au DMA que le département du Commerce, dont le rôle est de promouvoir et préserver les activités des entreprises américaines.

Au-delà du DMA, les différends bureaucratiques et l'absence d'un processus interagence effectif pour l'élaboration d'une politique étrangère sur les sujets numériques expliquent certains manques de cohérence dans la position américaine³⁶. Ce facteur s'ajoute à la réticence d'une partie de la classe politique de voir la Silicon Valley soumise à une régulation extérieure. Ces deux éléments contribuent à expliciter les apparentes contradictions de la position de l'exécutif et du Congrès sur la souveraineté numérique européenne, en dépit d'une volonté de réforme parfois semblable.

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, 16 septembre 2022, disponible sur : www.justice.gov ; J. Kanter, « Competition & Regulation in Disrupted Times », Charles Rivers Associates Conference, Bruxelles, 31 mars 2022, disponible sur : www.crai.com.

36. Entretien avec Frances Burwell, chercheuse à l'Atlantic Council et directrice à McLarty Associates, Washington D.C., 30 novembre 2022.

Les réformes européennes, modèles pour la régulation américaine ?

Parmi les partisans de cette ambition de réforme du secteur numérique américain, plusieurs cherchent à s'inspirer et tirer les leçons de ce qui a été fait sur le Vieux Continent ces dernières années au nom de la souveraineté numérique européenne. Les points d'intérêts relevés et la possibilité de les transposer dans le système américain varient toutefois selon les sujets traités.

Politique de concurrence

Sur la lutte contre les pratiques monopolistiques, certains acteurs assument leur volonté de s'inspirer du modèle européen. Le professeur de droit Tim Wu, recruté par le président Biden comme assistant spécial pour la compétition et la politique technologique³⁷, écrivait ainsi en 2018 :

« C'est sur ce sujet, entre autres, que l'Amérique peut emprunter à l'Europe [...]. L'Europe est aujourd'hui en tête dans l'examen de la "Big Tech", y compris [Google et Apple]. L'*antitrust* européen est loin d'être parfait, mais son leadership et sa volonté de porter des affaires importantes devant la justice lorsque la concurrence est clairement menacée devraient servir de modèle aux autorités américaines et au reste du monde³⁸. »

Cet intérêt pour le modèle européen s'est notamment traduit dans les textes juridiques : le projet de loi *American Innovation and Choice Online Act* proposé par la sénatrice Klobuchar reprend ainsi de nombreux éléments du DMA³⁹. Il s'inspire en particulier du fonctionnement par seuil quantitatif du DMA, proposant une régulation asymétrique qui ne vise que les plus gros acteurs⁴⁰. Au vu de l'opposition du secteur privé et des désaccords au Congrès, l'adoption de ce projet semble toutefois très

37. En poste depuis deux ans, M. Wu a quitté son poste au sein de l'administration Biden le 4 janvier 2023.

38. T. Wu, *Curse of the 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*, présenté le 18 octobre 2021, disponible sur : www.congress.gov.

40. Entretien avec Aurélien Portuese, Washington D.C., 1^{er} décembre 2022 ; S. Heather, « Striking Similarities: Comparing Europe's Digital Markets Act to the American Innovation and Choice Online Act », U.S. Chamber of Commerce, 17 juin 2022, disponible sur : www.uschamber.com.

incertaine, et les évolutions en matière d'*antitrust* pourraient plutôt être déterminées par la jurisprudence et les contentieux portés par la FTC.

Réglementation des plateformes et marketplaces

Le second volet du paquet législatif européen sur les services numériques – le *Digital Services Act* (DSA) – a suscité moins d'opposition côté américain que le DMA. L'objectif de transparence au cœur du DSA résonne aux États-Unis et certains points (comme la vérification des vendeurs tiers ou l'audit obligatoire pour les plateformes des systèmes de gestion des risques) semblent avoir suscité l'intérêt des acteurs politiques à Washington. Selon certains analystes, le projet de loi *Digital Services Oversight and Safety Act*⁴¹ proposé à la Chambre en février 2022 a même été conçu comme une véritable « traduction américaine du DSA⁴² ». Lori Trahan, la Représentante démocrate qui a présenté ce texte, assume cette proximité entre les deux, comme l'illustre sa réaction lors du passage du DSA en avril 2022 :



Lori Trahan  @Re... · 26 avr. 22 ·
ICYMI: this is HUGE. With the **DSA**, Europe is holding tech giants accountable for the harms they cause to users & society. I introduced the Digital Services Oversight and Safety Act to bring similar transparency, access & audit requirements here to the U.S.

Source : twitter.com

Si certains aspects de ce projet seront peut-être intégrés à d'autres textes législatifs débattus au Congrès (comme l'*American Data Privacy and Protection Act*) ou à des réglementations de la FTC, son adoption en tant que tel semble très peu probable, dans un contexte de fortes tensions partisanes sur les sujets de modération des contenus⁴³.

Protection des données

Autre sujet central des discussions transatlantiques sur le numérique, la question de l'accès aux données (à la fois par les plateformes privées et par les agences de sécurité nationale) et de la protection de la vie privée fait

41. U.S. Congress, *H.R.6796 - Digital Services Oversight and Safety Act of 2022*, présenté le 18 février 2022, disponible sur : www.congress.gov.

42. Entretien avec Nathalie Maréchal, directrice politique à Ranking Digital Rights, Washington D.C., 2 décembre 2022.

43. En simplifiant, les démocrates s'inquiètent de la désinformation et prolifération des contenus haineux en ligne tandis que les républicains protestent contre une modération par les plateformes perçue comme désavantageant les conservateurs (voire les censurant).

aujourd'hui l'objet d'importants débats aux États-Unis. Ceux-ci se nourrissent notamment des réglementations déjà adoptées à l'étranger, en particulier le Règlement général sur la protection des données (RGPD) mis en place par l'UE depuis 2018 et considéré comme pionnier en la matière.

Tirer les leçons du RGPD

En l'absence d'un régime fédéral général, plusieurs États – comme la Californie, le Colorado, le Connecticut, la Virginie ou l'Utah – ont adopté ces dernières années leur propre législation sur la protection des données personnelles⁴⁴. Le premier niveau où l'expérience du RGPD a pu se traduire dans des lois américaines est donc l'échelle étatique, en particulier dans le cas du *California Consumer Privacy Act* (CCPA) adopté en 2018 et effectif depuis 2020.

Le débat de ces derniers mois à Washington sur le projet de régime fédéral de protection des données⁴⁵ a tiré les leçons des expériences européennes (et californiennes). Selon Kevin Diamond, directeur adjoint de cabinet d'une Représentante démocrate très investie sur les questions de droits des consommateurs et de vie privée, l'expérience du RGPD a fait évoluer la discussion sur plusieurs points⁴⁶. La répétition de la demande de consentement à la collecte de données à chaque nouvelle page web introduite par le RGPD étant jugée fastidieuse, les législateurs américains privilégient par exemple un modèle de garantie minimum de certains droits de base – une évolution majeure et bipartisane. Par ailleurs, alors que la possibilité pour les individus de poursuivre une entreprise en justice en cas de violation des données (« droit privé d'action ») était dépeint par certains au début du RGPD comme la porte ouverte à une avalanche de contentieux, celle-ci ne s'est finalement pas produite, enhardissant les politiciens américains qui y sont favorables. Enfin, les législateurs fédéraux ont entendu les doléances du secteur privé soulignant leur difficulté à discuter avec les régulateurs nationaux de chacun des 27 États membres – en deçà du cadre général du RGPD – qui ont chacun leur philosophie et perspectives. Ce retour d'expérience a attiré l'attention des membres du Congrès sur les risques liés à un texte fédéral avec une clause de préemption trop faible, surtout dans un contexte où plusieurs États ont adopté (ou vont adopter) leur propre loi sur la protection des données⁴⁷.

44. A. Desai, « US State Privacy Legislation Tracker », International Association of Privacy Professionals, 7 octobre 2022, accessible sur : <https://iapp.org>.

45. Principalement autour du projet de loi *American Data Privacy and Protection Act* (ADPPA, H.R. 8152), présenté le 21 juin 2022, disponible sur : www.congress.gov.

46. Entretien avec Kevin Diamond, chef de cabinet adjoint en charge des sujets technologiques et numériques de la Représentante Lisa Rochester, Washington D.C., 28 novembre 2022.

47. La préemption est la capacité du gouvernement fédéral à annuler ou remplacer une loi étatique en faveur d'une loi fédérale. C'est le principal point d'achoppement des discussions actuelles autour de l'ADPPA, les démocrates californiens refusant de soutenir une loi fédérale qui préempterait leur

Ce point explique le soutien marqué du secteur privé américain pour une loi fédérale de protection des données, qui serait bien plus fiable et avantageuse qu'un puzzle de lois étatiques différentes.

Plus largement, la mise en place du RGPD ces quatre dernières années a facilité l'acceptation de certaines idées et incité les entreprises américaines à appeler de leurs vœux un équivalent outre-Atlantique. L'existence même du RGPD (mais également du régime chinois de gouvernance des données) est régulièrement brandie comme preuve d'un retard de Washington sur la question.

Surveillance et transferts de données

Dans une moindre mesure, les critiques européennes de la surveillance des citoyens exercées par les agences américaines – élément majeur des premiers débats sur la souveraineté numérique européenne – ont également eu un certain écho à Washington.

La majorité des élus américains ont vivement critiqué les décisions de la Cour européenne de Justice (CJUE) annulant les accords transatlantiques de transferts de données. Cependant, certains y répondent non pas en tentant de rassurer l'UE sur l'absence de programmes de surveillance, mais en condamnant ces derniers et en appelant à les réformer. Par exemple, le sénateur démocrate Ron Wyden déclarait en 2015 :

« En annulant le Safe Harbor Agreement, la Cour de justice de l'Union européenne a ouvert la chasse aux entreprises américaines. Cette décision malencontreuse n'est rien d'autre que du protectionnisme à l'encontre des services mondiaux de traitement des données et des biens numériques de l'Amérique. [...] Cependant, *les politiciens américains* qui ont permis à l'Agence nationale de sécurité de mettre secrètement en place un filet numérique de millions d'enregistrements téléphoniques et de courriels *portent également une responsabilité*. [...] *En aidant les tribunaux européens à annuler [le Safe Harbor Agreement], les politiciens à courte vue ont gravement porté atteinte aux entreprises américaines*. Le Congrès doit commencer à prendre les prochaines mesures sur la réforme de la surveillance dès maintenant [...]»⁴⁸. »

le CCPA. L. Zabierek et. al., « Preemption in Federal Data Security and Privacy Legislation », Belfer Center for Science and International Affairs, Harvard Kennedy School, 14 juin 2022, disponible sur : www.belfercenter.org ; J. Duball, « State views on proposed ADPPA preemption come into focus », International Association of Privacy Professionals, 27 septembre 2022, disponible sur : <https://iapp.org>.

48. R. Wyden, « Wyden Blasts EU 'Safe Harbor' Ruling », 6 octobre 2015, disponible sur : www.wyden.senate.gov.

En 2015 comme aujourd'hui, des membres des deux partis⁴⁹ favorables à une réforme du régime de surveillance intègrent à leur argumentaire la question des transferts de données avec l'Europe, et des restrictions européennes imposées au nom de la souveraineté numérique (et de la protection de la vie privée)⁵⁰.

Il convient toutefois de souligner qu'une grande partie des officiels et entreprises américaines tendent plutôt à rappeler, face aux critiques européennes, les progrès (réels mais limités) du système américain en la matière depuis quelques années⁵¹. L'idée européenne selon laquelle le régime américain serait moins protecteur vis-à-vis de la surveillance opérée par les agences de sécurité nationale serait ainsi erronée.

Surtout, dans un contexte américain dominé par la compétition avec la Chine, les réticences européennes en matière de transferts de données résonnent sans doute davantage avec les préoccupations américaines... mais sont perçues comme se trompant de cible. Comme le résume un conseiller au Congrès, « j'ai l'impression que les inquiétudes de l'UE et de certains défenseurs de la vie privée concernant notre régime de surveillance sont similaires aux inquiétudes que j'ai, ou que d'autres ont, concernant le téléchargement de TikTok⁵² ». La popularité des deux côtés de l'Atlantique des grandes plateformes chinoises du numérique (comme ByteDance, qui détient TikTok), accusées de transférer les données des citoyens aux autorités, donne un nouvel écho aux préoccupations associées à la capacité d'un gouvernement étranger d'accéder aux données de millions de citoyens. Les États-Unis eux-mêmes ont adopté ces derniers mois plusieurs restrictions pour limiter ce risque. Citons par exemple le décret n°13942 du président Trump pour « faire face à la menace posée par TikTok », révoqué par le décret n° 14034 du président Biden pour « protéger les données sensibles des Américains face aux adversaires étrangers », ou encore le projet de loi bipartisan adopté par le Congrès en décembre 2022 interdisant l'installation de TikTok sur tous les appareils appartenant au gouvernement.

Cette comparaison révèle un facteur d'importance croissante dans la vision américaine de la souveraineté numérique : la Chine.

49. Comme exemple de coopération bipartisane sur le sujet, citons l'amendement proposé en 2020 par le sénateur démocrate Wyden et le sénateur républicain Daines lors des débats sur la section 215 du *PATRIOT Act*, ou le projet de loi *The Fourth Amendment is Not For Sale Act* proposé en avril 2021 par le sénateur Wyden et le républicain Rand Paul. E. Goitein, « Surprising Senate Vote Signals New Hope for Surveillance Reform », Brennan Center for Justice, 16 mai 2020, disponible sur : www.brennancenter.org ; R. Wyden, « Wyden, Paul and Bipartisan Members of Congress Introduce The Fourth Amendment Is Not For Sale Act », 21 avril 2021, disponible sur : www.wyden.senate.gov.

50. Sur le sujet, voir également : T. Wetzling, L. Sarkesian et C. Dietrich, « Solving the Transatlantic Data Dilemma: Surveillance Reforms to Break the International Gridlock », Stiftung Neue Verantwortung, décembre 2021.

51. Voir par exemple C. Chin, « The EU-U.S. Data Privacy Framework: More Steps Needed to Repair Trust in Data Flows », CSIS, 24 octobre 2022.

52. Entretien avec un conseiller à la Chambre des Représentants, Washington D.C., novembre 2022.

Le facteur Chine dans la vision américaine de la souveraineté numérique européenne

Depuis l'administration Trump, la classe politique américaine (exécutive comme législative) a élevé la compétition avec la Chine, considérée comme la principale menace pour les États-Unis, au rang de haute priorité. Cette analyse a d'importantes répercussions sur les politiques numériques et technologiques américaines, y compris vis-à-vis de son allié européen.

La montée en puissance technologique de la Chine conduit Washington à percevoir de nouvelles vulnérabilités, et justifie la mise en place de réformes proches de certaines ambitions européennes de souveraineté numérique. La question de TikTok et de la protection des données en est une illustration, tout comme les débats des deux côtés de l'Atlantique sur la désinformation ou la dépendance excessive à l'étranger dans certains secteurs critiques. Cependant, la priorité accordée à la « compétition entre grandes puissances » fait également de la compétitivité des entreprises américaines (y compris, voire surtout, dans le numérique et les technologies) un enjeu de sécurité nationale. Largement relayé par le secteur privé, cet argument souligne le risque que la régulation (qu'elle soit américaine ou européenne) freine l'innovation – et donc pénalise le leadership américain dans la compétition⁵³. Le facteur Chine recoupe ainsi d'autres critères déjà mentionnés dans la constitution de groupes bipartisans, par exemple pro-industrie, pro-croissance, anti-Chine et contre les régulations européennes.

Répondre à la menace chinoise : un enjeu pour la souveraineté numérique européenne

Washington voit d'un très bon œil les mesures de souveraineté numérique européenne qui visent principalement (bien qu'implicitement) la Chine et se rapprochent des politiques américaines.

53. Cet argument a par exemple été défendu par Mark Zuckerberg et Sheryl Sandberg, respectivement fondateur et directrice des opérations de Facebook (aujourd'hui Meta), et Eric Schmidt, ancien P.-D.G. de Google. K. Wagner, « Mark Zuckerberg Says Breaking Up Facebook Would Pave The Way For China's Tech Companies To Dominate », *Vox*, 18 juillet 2018 et N. Tiku, « Big Tech: Breaking Us Up Will Only Help China », *Wired*, 23 mai 2019.

La volonté de protéger les entreprises européennes de haute technologie de certains rachats fait partie intégrante de l'ambition de souveraineté numérique européenne⁵⁴. S'inquiétant de la forte augmentation des prises de contrôle d'entreprises européennes par des investisseurs venant de Chine, Hong Kong et Macao, l'Union européenne a adopté de nouvelles réglementations pour renforcer les contrôles sur les investissements étrangers entrants⁵⁵. Ces efforts se rapprochent de ce qui a été fait aux États-Unis depuis 2018, année du renforcement des pouvoirs du comité en charge de l'examen des investissements entrants⁵⁶, et peuvent être considérés comme « une opportunité pour aligner davantage le partenariat USA-UE⁵⁷ ».

Plus récemment, la Commission européenne a prévu dans son programme de travail 2023 d'« examiner si des outils supplémentaires sont nécessaires pour le contrôle des investissements stratégiques sortants⁵⁸ ». Cette phrase vise particulièrement les investissements en direction des secteurs stratégiques chinois, et semble inspirée par le débat sur cette question qui agite le Congrès et la Maison Blanche depuis quelques mois⁵⁹. Cette réflexion – au niveau de l'UE et des États membres – bénéficie donc clairement du soutien de Washington. Le sénateur démocrate Bob Casey, coauteur d'un projet de loi bipartisan sur le contrôle des investissements sortants, s'est par exemple déclaré « encouragé par le fait que l'Allemagne envisage le type d'examen des investissements sortants que je préconise ici aux États-Unis avec mon *National Critical Capabilities Defense Act*⁶⁰ ».

Dans le cadre de leur diplomatie auprès de leurs alliés soulignant les risques posés par la Chine, les autorités américaines ont parfois elles-mêmes défini les enjeux en termes de souveraineté. Mike Pompeo, secrétaire d'État américain sous Donald Trump, a ainsi déployé une intense campagne auprès (notamment) des Européens afin de les convaincre d'exclure les fournisseurs

54. T. Madiega, « Digital sovereignty for Europe », *op. cit.*

55. Voir par exemple la réglementation effective depuis octobre 2020 : « 2017/0224 (COD) Screening of Foreign Direct Investments into the European Union », Legislative Observatory, European Parliament, 2023, disponible sur : <https://oeil.secure.europarl.europa.eu>. Notons cependant que les décisions finales sur le contrôle des investissements relèvent des États membres.

56. U.S. Congress, *Foreign Investment Risk Review Modernization Act of 2018*, adopté le 13 août 2018.

57. S. Erickson, « Recent Developments in EU Foreign Investment Screening », CSIS, 19 avril 2021.

58. Commission européenne, « Commission Work Programme 2023: A Union Standing Firm and United », COM (2022) 548, Strasbourg, 18 octobre 2022, p. 8.

59. S. Aarup, « China Beware! Europe Eyes Closer Control Over How Firms Invest Abroad », *Politico*, 3 janvier 2023 ; U.S. Senate, « Examining Outbound Investment », Hearing before the U.S. Senate Committee on Banking, Housing and Urban Affairs, 29 septembre 2022, disponible sur : www.banking.senate.gov.

60. B. Casey, tweet du 23 novembre 2022, disponible sur : <https://twitter.com>.

chinois jugés à risque⁶¹, en soulignant l'importance de cette décision pour la souveraineté nationale⁶².

Lorsque la souveraineté numérique européenne est pensée comme « capacité de l'Europe à agir de façon indépendante » *de la Chine*, les États-Unis la soutiennent voire la mettent en avant, ce qui crée des opportunités pour la coopération transatlantique. Celles-ci sont renforcées par la volonté des États-Unis et de l'UE de promouvoir une approche de la technologie reflétant leurs valeurs communes (démocratie, droits de l'Homme, internet ouvert, etc.)⁶³, pour faire face à l'approche plus centralisatrice et autocratique de la souveraineté numérique favorisée par la Russie et la Chine⁶⁴.

« Soyez protectionnistes contre la Chine, pas contre nous ! »

Cependant, sur d'autres sujets ciblant davantage les entreprises américaines, la perception accrue d'une menace chinoise à Washington renforce le sentiment d'injustice qui caractérise la réaction américaine aux initiatives européennes. Beaucoup d'acteurs publics et privés américains ont du mal à comprendre pourquoi celles-ci imposent des réglementations supplémentaires aux entreprises américaines mais pas aux entreprises chinoises (comme Alibaba, ByteDance, WeChat), pourtant plus problématiques sur le plan sécuritaire. Comme le résume un conseiller du Congrès, la question à Washington « c'est moins que tout doit être non-protectionniste, mais plutôt "de *qui* cherchons-nous à nous protéger ?" [...] Si vous [les Européens] voulez être protectionnistes, soyez protectionnistes contre la Chine, pas contre nous !⁶⁵ ». Deux reproches sont combinés dans cet argumentaire américain : le laxisme de l'UE face à la Chine et l'anti-américanisme patent de la souveraineté numérique européenne. La définition dans le DMA de « *gatekeepers* » qui pourraient n'inclure que les GAFAM a par exemple suscité une vive opposition côté américain, en dépit des justifications liées à leur taille sur le marché européen, bien supérieure à celle des entreprises chinoises⁶⁶.

61. M. Velliet, « Convaincre et contraindre : les interférences américaines dans les échanges technologiques entre leurs alliés et la Chine », *Étude de l'Ifri*, février 2022, disponible sur : www.ifri.org.

62. Par exemple en Slovénie ou au Royaume-Uni : S. Lau, « US Secretary of State Mike Pompeo Secures Slovenia Support for 'Clean Network' Campaign against Chinese Technology », *South China Morning Post*, 14 août 2020 ; C. Skopeliti, « UK Sovereignty in Jeopardy if Huawei Used for 5G, US Warns », *The Guardian*, 27 janvier 2020.

63. Commission européenne, « Le Conseil du commerce et des technologies UE-États-Unis relève des défis communs et fait face aux crises mondiales », 5 décembre 2022, disponible sur : <https://ec.europa.eu>.

64. J. Thumfart, « The Norm Development of Digital Sovereignty between China, Russia, the EU and the US », *op. cit.*

65. Entretien avec un conseiller à la Chambre des Représentants, Washington D.C., novembre 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*, 31 mai 2021.

Le facteur Chine accentue donc l'ambiguïté de la position américaine sur la souveraineté numérique européenne et ses déclinaisons en matière de politique industrielle. Comme le résume un chercheur et ancien officiel américain,

« les États-Unis ont des sentiments mitigés à l'égard du développement [de la politique d'innovation] dans l'UE : ils s'en félicitent en tant que contreponds à la Chine, pour des raisons de sécurité nationale, mais s'y opposent s'ils considèrent qu'elle désavantage des entreprises américaines, pour des raisons de compétitivité⁶⁷. »

L'exemple le plus parlant d'un domaine dans lequel les secteurs publics et privés américains ont manifesté leur opposition – tout en s'adaptant – aux restrictions européennes perçues comme désavantageuses est sans doute le cas du cloud.

67. W. Reinsch, in B. Dekker et M. Okano-Hijmans (dir.), *Dealing With China On High-Tech Issues*, op. cit., p. 7.

Adaptation et opposition américaine : l'exemple du cloud

Dans la lignée des préoccupations de l'UE sur les dépendances stratégiques et l'accès des autorités américaines aux données des Européens, le fait que 80 % des données du Vieux Continent soient hébergées par des fournisseurs cloud non-européens est considéré comme un problème économique, politique et de cybersécurité⁶⁸. Pour y répondre et garantir à l'Europe une « souveraineté des données » personnelles et non-personnelles, les institutions européennes ont élaboré de nouvelles réglementations ces dernières années. Celles-ci – comme le RGPD, la loi sur les données (*Data Act*), la loi sur la gouvernance des données (*Data Governance Act*), ou la loi sur la cybersécurité de l'UE – comprennent à la fois des mesures libéralisatrices pour faciliter le développement d'un marché européen de la donnée et des mesures limitant les transferts de données hors de l'UE. Ces mesures restrictives sont explicitement justifiées par les risques posés par les lois américaines et chinoises dont la portée extraterritoriale permet de contraindre certains fournisseurs de services cloud à accorder à leurs autorités l'accès aux données européennes⁶⁹.

Des solutions pour un cloud « aux conditions de l'Europe »...

Répondant aux déclinaisons réglementaires nationales et européennes de cette nouvelle exigence de souveraineté, les acteurs privés américains et européens ont développé tout un éventail de solutions techniques, commerciales et organisationnelles. Il existe en effet entre les deux une certaine convergence d'intérêts : les fournisseurs américains de services cloud souhaitent conserver un accès au marché européen et il n'est pas dans l'intérêt des entreprises européennes de ne plus pouvoir utiliser les services de pointe des *hyperscalers*. Plusieurs solutions ont donc été proposées pour tirer parti des

68. A. Pannier, « The Changing Landscape of European Cloud Computing Gaia-X, the French National Strategy, and EU Plans », *Briefing de l'Ifri*, Ifri, 22 juillet 2021.

69. Le rapport de la Commission européenne sur l'analyse d'impact du *Data Act* cite en particulier le décret présidentiel américain 12333, le *Foreign Intelligence Surveillance Act (FISA)*, le US CLOUD Act, et la loi chinoise de 2017 sur le renseignement national. Commission européenne, « Impact Assessment Report Accompanying the Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data », Bruxelles, 23 février 2022, p. 21.

performances des services cloud des leaders américains (Google Cloud, Microsoft Azure, AWS d'Amazon) tout en protégeant les données européennes face aux lois extraterritoriales.

Différentes techniques de chiffrement des données sont ainsi mises en avant, notamment celles permettant au client de stocker ses données dans le cloud sans que le fournisseur de services n'y ait accès. Ces solutions de chiffrement font partie des « contrôles souverains » proposés par les entreprises américaines dans le cadre de leurs engagements pour la souveraineté numérique européenne, tels que « *Microsoft Cloud for Sovereignty*⁷⁰ » ou « *Cloud on Europe's Terms* » de Google⁷¹.

Des propositions complémentaires consistent à panacher les fournisseurs cloud (« cloud hybride » combinant cloud public et privé, ou « multi-cloud » avec plusieurs fournisseurs de cloud public), de façon à fournir différents niveaux de sécurité et de protection des données. Certaines de ces offres, notamment en France, reposent sur la création de partenariats entre des entreprises américaines et françaises. Un exemple est la création annoncée en 2021 de Bleu, une joint-venture détenue par des actionnaires français qui proposera les services de cloud computing de Microsoft mais en hébergeant les données par Orange et Capgemini sur le territoire français⁷². Sur le même modèle, Google et Thalès ont présenté leur offre cloud S3ENS en juin 2022⁷³. Bleu et S3NS ont tous les deux été créés dans le but d'obtenir le label SecNumCloud délivré par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui leur permettrait d'être qualifiés de « cloud de confiance ».

... Avec encore d'importants points d'achoppement

Le développement de cette certification française et de son équivalent européen fait toutefois l'objet d'une très nette opposition de la part du secteur privé et public américain (notamment le département du Commerce et du Trésor).

70. C. Sanders, « Microsoft Cloud For Sovereignty: The Most Flexible And Comprehensive Solution For Digital Sovereignty », Official Microsoft Blog, 19 juillet 2022, disponible sur : <https://blogs.microsoft.com>.

71. A. Fox-Martin, « Advancing Digital Sovereignty On Europe's Terms », Google Cloud, 13 octobre 2022, disponible sur : <https://cloud.google.com>.

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

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

Tout d'abord, officiels comme analystes américains, considèrent que SecNumCloud est une façon de forcer la création de joint-ventures, comparant la certification aux pratiques prédatrices chinoises⁷⁴. En outre, les acteurs américains se sont inquiétés dès début 2022 de l'absence de définition initiale (également pointée par la Commission) à la fois des « données sensibles » et des agences publiques pour qui le label serait requis. Les États-Unis redoutent que la France n'ait une vision très large de ce qui est « sensible » (bien au-delà des données militaires par exemple), et qu'elle étende l'obligation d'être certifié SecNumCloud au-delà du secteur public : aux entreprises publiques, voire à tout le secteur privé⁷⁵.

De fait, les inquiétudes américaines concernent aussi le schéma de certification européen relatif aux prestataires de cloud (*European Union Cybersecurity Certification Scheme on Cloud Services, EUCS*) en cours d'élaboration par l'Agence de l'UE pour la Cybersécurité, susceptible d'intégrer les critères français. La France est en effet fortement impliquée dans le développement de l'EUCS, et le SecNumCloud 3.2 (qui « explicite des critères de protection vis-à-vis des lois extra-européennes ») « sert de référence dans les travaux sur le niveau “élevé” de cette future certification⁷⁶ ». La France, l'Allemagne, l'Italie et l'Espagne soutiennent ainsi une version de l'EUCS comprenant une exigence d'immunité contre les lois non-européennes : seuls les fournisseurs cloud situés en Europe et non-contrôlés par des entités extérieures seraient certifiables⁷⁷. D'autres États membres (Pays-Bas, Suède, Irlande, Grèce, Pologne notamment) remettent en question la nécessité d'un critère de souveraineté, également très décrié par les Américains⁷⁸. Le fait que l'EUCS ait été discuté lors de l'appel de la Représentante au Commerce américaine Katherine Tai avec le Commissaire européen au Commerce Valdis Dombrovskis en septembre 2022 témoigne de l'importance qui y est accordée à haut niveau par l'administration Biden⁷⁹.

74. Entretiens avec des chercheurs, officiels et entreprises, Washington, novembre 2022 ; N. Cory, « “Sovereignty Requirements” in French—and Potentially EU—Cybersecurity Regulations », ITIF, 10 décembre 2021.

75. Cette inquiétude est alimentée par les déclarations politiques ambiguës des autorités françaises sur la question. Le ministre français Bruno Le Maire déclarait par exemple en septembre dernier : « si jamais nos *entreprises* qui ont des données extraordinairement sensibles ne se saisissent pas librement de cette offre [SecNumCloud] de sécurisation de leurs données, je ne peux pas exclure que, à un moment ou à un autre, nous en venions à une norme *obligatoire* pour protéger notre souveraineté industrielle ». B. Le Maire, « Discours sur la stratégie nationale pour le Cloud », Strasbourg, 12 septembre 2022.

76. « L'ANSSI actualise le référentiel SecNumCloud », ANSSI, 8 mars 2022.

77. A. Vitard, « Divergences autour des exigences de souveraineté dans le schéma européen de certification du cloud », *L'Usine Digitale*, 20 juin 2022 ; K. Propp, « European Cybersecurity Regulation Takes a Sovereign Turn », European Law Blog, 12 septembre 2022, disponible sur : <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*, 14 juin 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, 1^{er} septembre 2022, disponible sur : <https://ustr.gov>.

Si elle est loin de faire l'unanimité en Europe, la conception maximaliste de la souveraineté numérique – qui voudrait, pour le cloud, ne confier les données des Européens qu'à des fournisseurs européens totalement indépendants des lois non-européennes – continue donc d'être un point d'achoppement.

Conclusion

La double évolution de l'analyse américaine sur la nécessité de réformer le secteur du numérique et de gagner la compétition technologique contre la Chine a donc transformé la vision qu'ont les États-Unis de la souveraineté numérique européenne. 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. Elle crée à la fois de nouvelles opportunités de coopération (face à des grandes plateformes aux pratiques jugées abusives ou face aux définitions autocratiques de la souveraineté numérique), un enrichissement mutuel des approches juridiques et réglementaires, et de vives tensions.

Près de dix ans après l'apparition du terme dans la rhétorique officielle, la définition de la souveraineté numérique européenne et ses déclinaisons politiques restent mal comprises outre-Atlantique. Cela s'explique d'une part par un degré de mauvaise volonté de la part de certaines entreprises américaines ciblées, et le manque de connaissance et d'engagement du Congrès sur le sujet. Cependant, cette incompréhension est aussi une conséquence directe du flou maintenu (en partie à cause des divergences entre États membres) autour de la signification *pour l'UE* de la souveraineté numérique. Erreurs de communication ou ambiguïté politique volontaire, certaines déclarations de figures politiques européennes, teintées d'anti-américanisme, continuent d'alimenter les soupçons des acteurs publics et privés américains quant aux objectifs de l'UE⁸⁰.

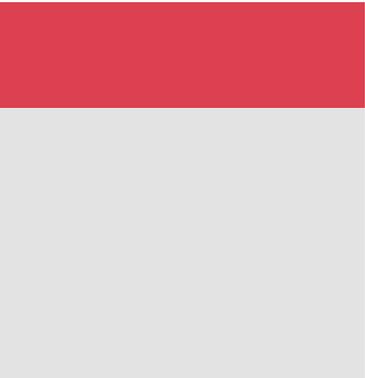
Ces incompréhensions persistantes rendent d'autant plus nécessaires les discussions bilatérales, par exemple dans le cadre du Conseil pour le Commerce et les Technologies, mais aussi au sein des différentes autorités européennes ainsi qu'avec les entreprises américaines, pour répondre aux injonctions contradictoires générées par l'exigence de souveraineté numérique⁸¹.

En dépit des contradictions et tensions, la présence d'une administration américaine europhile et appelant à l'union bipartisane « contre les abus de la *Big Tech*⁸² » représente une fenêtre d'opportunité pour un rapprochement transatlantique sur ces sujets – qui pourrait ne pas durer.

80. La plus fréquemment citée à Washington (fin 2022) est celle du député européen Andreas Schwab, rapporteur pour le DMA. Voir J. Espinoza, « EU should focus on top 5 tech companies, says leading MEP », *Financial Times*, 31 mai 2021. Voir aussi B. Le Maire, « Discours sur la stratégie nationale pour le Cloud », Strasbourg, 12 septembre 2022.

81. Par exemple, les exigences autour de la vie privée et de la concurrence (et les autorités européennes associées à leur protection) défendent des positions parfois différentes sur l'importance pour les entreprises de partager leurs données.

82. J. Biden, « Unite Against Big Tech Abuses », *Wall Street Journal*, 12 janvier 2023.



27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org