ÉTUDES
DE L'IFRI

CENTRE GÉOPOLITIQUE DES TECHNOLOGIES

MARS
2026

(Extra)territorialité des données : quelle souveraineté pour l'Europe ?

Emma BADAOUI
Anne-Thida NORODOM

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.

ISBN : 979-10-373-1192-4

Comment citer cette publication :
Emma Badaoui et Anne-Thida Norodom, « (Extra)territorialité des données : quelle souveraineté pour l'Europe ? », *Études de l'Ifri*, Ifri, mars 2026.

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

Autrices

Emma Badaoui est doctorante en droit public à l'Institut de recherche stratégique de l'École militaire (IRSEM) et à l'Université de Bretagne occidentale. Elle étudie les phénomènes de manipulation algorithmique de la cognition sur les réseaux sociaux et les moyens juridiques de les encadrer. Elle est diplômée d'un master en droit de l'intelligence artificielle (IA) de l'Institut catholique de Paris. Lauréate du prix Data Ring pour son mémoire sur la souveraineté à l'épreuve des réseaux sociaux et la stratégie cognitive chinoise à travers TikTok, elle s'est spécialisée dans les enjeux juridiques, géopolitiques et réglementaires liés à l'IA.

Anne-Thida Norodom est professeur de droit public à l'Université Paris Cité. Le droit international des activités numériques constitue aujourd'hui son domaine de spécialisation. L'analyse juridique du cyberespace et de l'intelligence artificielle lui a permis de dispenser des cours et séminaires, notamment à l'Académie de droit international de La Haye, de publier des articles et diriger quatre ouvrages : le premier sorti en 2014, pour la Société française pour le droit international, co-dirigé avec Philippe Lagrange sur *Internet et le droit international* ; en 2016 avec Lilian Richieri Hanania sur « La diversité culturelle à l'ère numérique » ; en 2019 avec Maryline Grange sur les *Cyberattaques et droit international*, ouvrage récompensé par deux prix, de la European Cyberweek 2019 et du Forum international de la cybersécurité 2020. Son dernier ouvrage, co-dirigé avec Adam Abdou Hassan, est intitulé *Droit du numérique en Afrique. Enjeux internationaux* et a été publié en 2023.

Résumé

L'expansion de l'extraterritorialité aux données numériques traduit l'émergence de nouveaux rapports de pouvoir autour du contrôle des flux de données mondiaux. Dans ce contexte, la localisation des données s'est imposée progressivement comme un instrument stratégique mobilisé par différents États à des fins de contrôle politique et idéologique, de protection des intérêts industriels et de la sécurité nationale, ou encore de soutien à l'innovation et à la protection des données. En Europe, la prééminence de fournisseurs de services *cloud* américains, soumis à des législations extraterritoriales, telles que le *CLOUD Act* ou le *Foreign Intelligence Surveillance Act* (FISA), révèle les limites d'une stratégie européenne uniquement fondée sur la localisation des données. Face à l'étendue de ses dépendances dans les domaines numérique et technologique (*cloud*, logiciels, semi-conducteurs, 5G) et des vulnérabilités qui en résultent, l'Union européenne (UE) gagnerait à mettre pleinement en œuvre une politique de souveraineté sur les données. Aussi, plusieurs orientations pourraient être envisagées : garantir la continuité des services numériques, assurer la résilience des infrastructures critiques ou encore mettre en œuvre une politique de diversification des partenariats technologiques de l'Europe avec des acteurs partageant les mêmes valeurs. Une telle stratégie permettrait de combiner à la fois des objectifs de compétitivité économique et de souveraineté en matière de données, propice à l'innovation technologique, en particulier dans le domaine de l'intelligence artificielle (IA).

Abstract

The expansion of the extraterritorial reach of laws governing digital data highlights the rise of new power dynamics surrounding control over global data flows. In this context, data localization is gradually emerging as a strategic tool employed by various states for purposes of political and ideological control, the protection of industrial interests and national security, or to support innovation and data protection. In Europe, the preeminence of American cloud service providers is subject to extraterritorial legislations such as the CLOUD Act or Foreign Intelligence Surveillance Act (FISA), highlighting the limits of a European strategy based solely on data localization. Given the extent of its dependencies in the digital and technological sectors (cloud computing, software, semiconductors, 5G) and the resulting vulnerabilities, the European Union (EU) would benefit from fully implementing a data sovereignty policy. Several approaches could therefore be considered: ensuring the continuity of digital services, ensuring the resilience of critical infrastructure or implementing a policy to diversify Europe's technological partnerships with actors that share the same values. Such a strategy would make it possible to combine the goals of economic competitiveness and data sovereignty, thereby fostering technological innovation, particularly in the field of artificial intelligence (AI).

Sommaire

Introduction

L'hypothèse, auparavant tenue pour improbable et cantonnée à un imaginaire dystopique, selon laquelle quelques grandes entreprises technologiques mondiales pourraient à terme, restreindre ou suspendre l'accès à leurs services n'appartient plus au registre de la fiction. En 2025, à la suite de sanctions imposées par l'administration Trump à la Cour pénale internationale (CPI), plusieurs juges et procureurs ont vu leur accès à des services numériques essentiels suspendu, s'agissant aussi bien des systèmes de paiement internationaux (Visa, Mastercard), de plateformes de services numériques (Apple Pay, Amazon, Netflix, etc.) ou encore d'outils logiciels fournis par Microsoft. L'institution a donc été poussée à envisager le remplacement de solutions technologiques américaines par des alternatives européennes comme OpenDesk[1].

La frontière entre menace et réalité apparaît désormais de plus en plus ténue, en particulier pour l'Europe, alors que les relations transatlantiques sont mises à rude épreuve par des divergences qui, pour l'heure, semblent irréconciliables. La réglementation des services numériques américains par l'Union européenne (UE), jugée excessivement contraignante par Donald Trump, a exacerbé des tensions politiques et économiques préexistantes et mis en lumière la dépendance technologique toujours plus grande de l'UE aux entreprises technologiques américaines. Le secteur de la *tech* pourrait également faire l'objet de restrictions à l'exportation, en particulier les puces électroniques de Nvidia, une ressource stratégique hautement convoitée dans la course au leadership en intelligence artificielle (IA)[2].

La concentration des infrastructures, des données et des capacités d'innovation entre les mains d'acteurs privés extra-européens contraint l'UE à repenser ses ambitions en matière de souveraineté numérique. Aussi, le 18 novembre 2025, se tenait à Berlin le Sommet franco-allemand sur la souveraineté numérique européenne. Face aux dépendances technologiques structurelles du continent, la France et l'Allemagne, principaux moteurs d'innovation technologique en Europe, y ont présenté des mesures en faveur de la construction d'infrastructures et de solutions innovantes à l'échelle régionale. Les domaines stratégiques visés concernent particulièrement la souveraineté des données et l'IA de pointe, afin de stimuler la compétitivité européenne et renforcer la souveraineté numérique du continent.

1. M. Aellig, « La Cour pénale internationale abandonne Microsoft pour une solution européenne, après les tensions répétées avec l'administration Trump », France Info, 31 octobre 2025.
2. R. Bacqué, D. Leloup et A. Piquard, *Nos nouveaux maîtres*, Paris, Albin Michel, 2026, p. 215.

L'imbrication entre données et innovation en IA est parfaitement résumée par l'idée selon laquelle « pour être *AI-ready*, il faut d'abord être *data-ready*[3] ». Les données sont la matière brute de l'information, elles se présentent comme des faits (chiffres, mots, observations) de différentes natures (personnelle ou non personnelle, sensible, stratégique) et de différentes formes : donnée quantitative (valeur mesurable), qualitative (descriptive et non mesurable), structurée (organisée en base de données), non structurée (sans format défini), métadonnée (c'est-à-dire les données sur des données, comme par exemple l'heure, la date et la localisation d'une photographie), ou encore *Big Data* (grands jeux de données).

Considérées comme l'or noir du XXIe siècle[4], les données cheminent invariablement au travers d'un maillage réticulaire complexe et interconnecté d'infrastructures numériques composé de *data centers*, de *clouds*, de câbles sous-marins et dans une moindre mesure des systèmes satellitaires. Leur volume pourrait avoisiner les 400 zettaoctets d'ici 2028, soit plusieurs fois le volume total de données échangées sur Internet aujourd'hui[5]. Les flux de données ont été qualifiés de « flux stratégiques » par la *Revue nationale stratégique française* de 2025. Ils sont désormais appréhendés comme des actifs critiques à part entière pour l'innovation technologique, notamment en IA, qui doivent être maîtrisés et sécurisés. La maîtrise des données renvoie à la capacité de savoir et de décider dans quel pays elles sont stockées et traitées, tandis que leur sécurisation vise à en garantir la confidentialité, l'intégrité et la disponibilité face aux accès ou altérations non autorisés.

Par ailleurs, les fournisseurs et les utilisateurs peuvent dépendre de souverainetés différentes et la localisation des données afférentes est souvent complexe à déterminer[6] : elles peuvent être dupliquées ou scindées dans plusieurs territoires ; elles n'ont pas de nationalité ; elles peuvent être sensibles, privées ou concerner des intérêts fondamentaux de la nation justifiant une protection particulière. À titre d'illustration, les données d'une entreprise française qui utilise des services *cloud* fournis par une société américaine peuvent être stockées en Europe, d'autres aux États-Unis, et des copies de sauvegarde en Asie. Dans ce cas, les données peuvent exister simultanément dans plusieurs juridictions et échapper à une compétence étatique exclusive.

3. Propos d'un responsable de Huawei en marge du forum Innovative Data Infrastructure en avril 2025. Lire S. Leblal, « Huawei accélère son stockage pour l'IA », *Le Monde informatique*, 30 avril 2025.
4. « The World's Most Valuable Resource Is No Longer Oil, But Data », *The Economist*, 6 mai 2017.
5. « Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2023, with forecasts from 2024 to 2028 », Statista, mai 2024. En informatique, 1 zettaoctet équivaut à 10^{21} octets, soit 200 millions de films en haute définition ; 400 zettaoctets équivaudraient à 80 000 milliards de films en haute définition.
6. C. Bômont, « Maîtriser le *cloud* computing pour assurer sa souveraineté », *in* A. Cattaruzza, D. Danet et S. Taillat (dir.), *La Cyberdéfense. Politique de l'espace numérique,* Paris, Armand Colin, 2023, p. 135.

Cette problématique de localisation des données est particulièrement prégnante dans le contexte du recours massif au *cloud*. Le *cloud computing*, ou informatique en nuage, permet de sécuriser l'accès, stocker et traiter de larges volumes de données, mais également d'utiliser de la puissance de calcul de manière décentralisée au moyen de serveurs distants et interconnectés[7]. L'architecture distribuée du *cloud* repose précisément sur la répartition géographique des données à travers de multiples centres de données situés dans diverses juridictions, ce qui rend particulièrement ardue, voire illusoire, la maîtrise de leur localisation physique et, par conséquent, du cadre juridique applicable. Plusieurs États peuvent dès lors revendiquer, à de multiples titres, l'exercice de leurs compétences sur ces données, les exposant à des revendications concurrentes de souveraineté et à l'application de législations extraterritoriales susceptibles d'en compromettre la protection ou d'en détourner l'usage.

L'avènement du cyberespace, qui par nature transcende les frontières étatiques, a ainsi contraint le droit à redéfinir le concept westphalien de souveraineté fondé sur la territorialité. La dilution des repères territoriaux traditionnels oblige en effet les États à repenser les modalités d'exercice de leurs prérogatives. Ce renouveau conceptuel trouve son expression dans l'avènement d'une « souveraineté numérique ». Celle-ci a été définie par le Sénat français en 2019 comme la capacité de l'État à agir dans le cyberespace, impliquant à la fois la maîtrise des réseaux, des communications électroniques et des données. À l'échelle communautaire, la souveraineté numérique recouvre en apparence la même définition[8]. L'emploi de cette expression par l'UE renvoie en réalité davantage à un projet politique adossé au concept d'« autonomie stratégique », pour faire face à la domination américaine dans le domaine numérique. Les ambitions de souveraineté numérique européenne ont été renouvelées et rehaussées par la Commission depuis le retour de Donald Trump à la présidence des États-Unis en janvier 2025.

Bien que les prémices d'une réflexion sur la souveraineté numérique aient émergé dès les années 1990 en Russie, en Chine et en Iran[9], la dynamique globale de maîtrise des données tend à se renforcer partout dans le monde particulièrement depuis les révélations d'Edward Snowden en 2013 sur la surveillance de masse des télécommunications menée par la National Security Agency (NSA)[10]. Elle s'incarne notamment par des exigences juridiques de localisation de celles-ci. Ce changement de paradigme marque une rupture avec le principe de libre-échange des données qui a longtemps

7. « Cloud computing », Commission nationale de l'informatique et des libertés (CNIL).
8. La souveraineté numérique européenne est définie comme « la capacité de l'Europe à agir de manière indépendante dans le monde numérique » ; T. Madiega, « Digital Sovereignty for Europe », European Parliamentary Research Service, juillet 2020.
9. J. Nocetti, « La souveraineté numérique, un instrument de politique étrangère », in *Enjeux numériques. La souveraineté numérique : dix ans de débats, et après ?*, Annales des Mines, septembre 2023.
10. A. Cattaruzza, *Géopolitique des données numériques*, Paris, Le Cavalier Bleu, 2019, p. 49.

prévalu avec Internet dans les États occidentaux et témoigne par ailleurs de la conviction croissante que la sécurisation des flux de données constitue une condition *sine qua non* de la souveraineté numérique. Cette tendance se traduit concrètement par l'adoption de législations imposant la localisation des serveurs sur leur territoire à partir du moment où les données qui y sont stockées concernent leurs citoyens (Russie) ou encadrant strictement le transfert de données personnelles vers des pays tiers (UE).

En Europe, la politique publique en matière de données s'est d'abord matérialisée par un volet « protection », avec l'adoption en 2016 du Règlement général sur la protection des données à caractère personnel (RGPD), conçu comme un moyen de responsabiliser les acteurs économiques et assurer la protection des droits fondamentaux. Cette approche s'est progressivement doublée d'un volet résolument tourné vers l'innovation et la compétitivité. Elle s'est donc dotée d'une nouvelle « Stratégie pour une union des données » en novembre 2025, dont le troisième pilier est dédié à la préservation de la souveraineté de l'Union en matière de données. L'UE entend désormais faire de la donnée un levier stratégique dans la compétition mondiale pour l'IA, notamment à travers la construction d'un marché unique de la donnée destiné à soutenir les acteurs européens de l'IA. Cet espace économique et juridique vise à garantir au sein de l'UE la libre circulation des données entre États membres, tout en conservant un haut niveau de protection des droits fondamentaux et de concurrence, au moyen d'un cadre réglementaire harmonisé encadrant la collecte, l'accès, le partage et la réutilisation des données personnelles et non personnelles.

Pour autant, parler de localisation des données ou d'extraterritorialité dans un monde numérique ubiquitaire n'a pas véritablement de sens juridique : appliquer des logiques exclusivement territoriales à un espace qui n'a pas de territoire semble intrinsèquement paradoxal. L'application du droit repose par ailleurs sur d'autres critères de rattachement que le seul territoire, tels que la localisation des personnes concernées par les données, la nationalité, ou encore le lieu d'établissement des fournisseurs de services. Territorialiser le numérique reviendrait à projeter sur un espace délocalisé des concepts forgés pour régir des réalités matérielles et géographiques. Cette inadéquation structurelle explique les tensions normatives actuelles : dans un monde où les frontières techniques s'effacent, les frontières juridiques peinent à conserver leur sens et leur effectivité. La stratégie européenne en matière de souveraineté sur les données est-elle alors suffisante pour faire advenir une souveraineté numérique manifeste et participer à l'effort d'innovation technologique du continent ?

Cette étude analyse d'abord les mécanismes d'extraterritorialité juridique pesant sur les données et l'expansion corrélative des stratégies de souveraineté sur les données dans un effort plus global de souveraineté numérique, avant d'interroger les obstacles structurels et industriels qui compromettent la construction d'une autonomie stratégique numérique européenne.

L'expansion de l'extraterritorialité aux données numériques

Au niveau national, la souveraineté signifie que les personnes, physiques et morales, sont assujetties à la puissance de l'État, tandis que dans l'ordre international, le principe de souveraineté consacre le pouvoir d'un État à se gouverner sans ingérence extérieure. En d'autres termes, « aucun État ne peut être subordonné à un autre État[11] ». Ceci renvoie donc au principe d'égalité souveraine au fondement de l'Organisation des Nations unies (ONU)[12] qui reconnaît la souveraineté nationale comme un pilier fondamental des relations internationales. En vertu du principe de souveraineté, l'État dispose par ailleurs d'une compétence exclusive sur son territoire et, par conséquent, ne peut intervenir sur le territoire d'un autre État. Un État peut exercer ses compétences de trois manières :

- par rattachement territorial, lorsque la personne ou le bien se trouve sur son territoire ;
- par rattachement personnel, lorsqu'il agit à l'égard de ses citoyens ou d'engins nationaux (navire, aéronef), même hors de son territoire ;
- par rattachement matériel, lorsqu'il intervient pour protéger ses intérêts fondamentaux (lutte contre le terrorisme) ou ceux de la communauté internationale, ce qui relève alors de la « compétence universelle ».

En droit international, le critère de rattachement territorial est privilégié. Or, les caractéristiques du numérique (virtualité, vélocité et ubiquité) ont profondément bouleversé la logique territoriale sur laquelle est fondée la souveraineté de l'État. L'extraterritorialité s'entend comme l'application d'une norme en dehors du territoire de l'État qui l'a émise[13]. Appliquée aux données, l'extraterritorialité progresse aujourd'hui à double titre. D'une part, les États développent des cadres juridiques de plus en plus complexes et explicitement extraterritoriaux, capables d'imposer à leurs entreprises des obligations d'accès ou de transmission de données même lorsqu'elles sont stockées à l'étranger. D'autre part, la domination mondiale des infrastructures *cloud* par les *hyperscalers* américains (Microsoft, Google,

11. R. Rivier, *Droit international public*, Paris, Presses universitaires de France, 4e éd., 2023, p. 291.
12. Article 2, paragraphe 1 de la Charte des Nations unies.
13. B. Stern, « Une tentative d'élucidation du concept d'application extraterritoriale », *Revue québécoise de droit international*, vol. 3, 1986, p. 49-78, p. 51. L'auteur précise que l'application d'une norme est une « opération complexe – dont la première étape est l'édiction même de la norme ».

Amazon) accroît mécaniquement la vulnérabilité des données européennes : hébergées par des infrastructures contrôlées par des acteurs soumis au droit américain, elles deviennent davantage exposées aux lois extraterritoriales étrangères, en dépit des protections prévues par le droit européen.

Les préoccupations d'ordre juridique liées à l'extraterritorialité de certaines législations étrangères sur les données européennes ont été expressément soulignées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) dans son rapport sur le *cloud computing*[14]. Elles ont été réitérées par le président Emmanuel Macron et le chancelier allemand Friedrich Merz lors du Sommet franco-allemand pour la souveraineté numérique en novembre 2025, invitant à se prémunir des risques relatifs aux lois extraterritoriales sur les données. De fait, certaines puissances ont fait de l'exercice extraterritorial de leurs compétences sur les données un outil de *lawfare* (guerre du droit) au service d'intérêts nationaux. C'est particulièrement le cas des États-Unis.

L'extraterritorialité du droit américain comme instrument de pouvoir sur les flux de données mondiaux

Les États-Unis ont développé une véritable « politique juridique extérieure[15] ». La pratique extraterritoriale américaine, d'abord cantonnée à la lutte anticorruption et au blanchiment d'argent, s'est peu à peu déployée pour englober l'information et la donnée. Les attentats du 11 septembre 2001 ont conduit à l'adoption du *Patriot Act*. La loi accorde à l'administration et aux agences américaines la possibilité d'obtenir toute information stockée par un service informatique en nuage américain, dès lors qu'un accord de coopération judiciaire a été conclu. Quelques années plus tard, en 2008, le Congrès a adopté la section 702 du *Foreign Intelligence Surveillance Act* (FISA) – renouvelée pour la dernière fois en avril 2024. Le texte amendé autorise les agences de renseignement à collecter les données de communications électroniques de personnes non américaines situées à l'étranger, dès lors qu'elles sont détenues par des entreprises américaines, et ce sans mandat.

Enfin, cet arsenal législatif à portée extraterritoriale est renforcé en 2018 par l'entrée en vigueur du *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act). Il confère aux autorités américaines, dans le cadre d'enquêtes pénales, le droit de contraindre les prestataires de services *cloud* immatriculés aux États-Unis à leur transmettre les données de communications électroniques de personnes ou entreprises américaines ou

14. « Cloud computing : état de la menace informatique », ANSSI, 19 février 2025.
15. M. Leblanc-Wohrer, « Le droit, arme économique et géopolitique des États-Unis », *Politique étrangère*, vol. 84, n° 4, Ifri, décembre 2019. L'expression est empruntée à Guy de Lacharrière dans son ouvrage *La Politique juridique extérieure*, Bruxelles, Bruylant, 2023.

étrangères, y compris dans le cas où ces données seraient hébergées hors du sol américain[16]. Cette loi a été adoptée en réponse à l'emblématique affaire Microsoft Ireland[17] en 2018 qui a conduit à la modification du droit américain et indirectement à celle du droit européen. Dans cette affaire, l'administration américaine (État d'origine de la norme) obligeait Microsoft (entreprise américaine) à lui fournir des données, dans le cadre d'une enquête pénale liée à un trafic de stupéfiants, sur le fondement du *Store Communication Act* (SCA) de 1986[18]. L'entreprise multinationale avait alors refusé d'exécuter cette requête pour deux motifs. Tout d'abord les données étaient stockées en Irlande. Ensuite, le stockage desdites données dans un autre État obligeait les États-Unis à passer par l'accord de coopération judiciaire et pénale conclu avec l'Irlande, un *Mutual Legal Assistance Treaty* (MLAT), pour exiger la fourniture des données. Or, le recours à un tel accord implique une procédure longue et contraignante de coopération judiciaire entre États, que les États-Unis souhaitaient contourner : Microsoft étant une entreprise américaine, selon Washington peu importait le lieu de stockage de leurs données. Portée devant la Cour suprême des États-Unis, l'affaire Microsoft s'est conclue par l'adoption du *CLOUD Act* qui a mis fin à la procédure judiciaire.

Bien qu'elle ait mis un terme à l'affaire opposant l'administration américaine à la société Microsoft, cette loi, amplement commentée[19], soulève plusieurs questions sur la dimension extraterritoriale de la compétence du juge pénal américain. S'il exerce légitimement sa compétence à l'égard du comportement litigieux faisant l'objet des poursuites sur le territoire américain (le trafic de stupéfiants), la preuve de l'infraction repose toutefois sur des données stockées en dehors dudit territoire par une entreprise américaine. Dès lors, deux positions s'affrontent. Pour l'administration américaine, l'ordonnance de communication des données adressée à Microsoft se limitait à prendre en compte des éléments extérieurs à son territoire (la localisation irlandaise des données) pour en tirer des conséquences sur son propre territoire. Sa compétence restait ainsi justifiée par la nationalité de Microsoft et l'ordonnance n'était donc pas à proprement parler extraterritoriale. Aux yeux de Microsoft, en revanche, les autorités américaines entendaient produire des effets juridiques extraterritoriaux, puisqu'il s'agissait de saisir des données stockées en Irlande[20].

16. La dimension extraterritoriale du *CLOUD Act* serait toutefois à nuancer selon certains juristes. Lire R. Bismuth, « Every Cloud Has a Silver Lining. Une analyse contextualisée de l'extraterritorialité du Cloud Act », *La Semaine juridique. Entreprise et affaires*, n° 40, 2018, p. 35-47.
17. *United States v. Microsoft Corp.*, 584 US (per curiam), Cour suprême des États-Unis, 17 avril 2018.
18. Le *Stored Communication Act* encadre l'accès des autorités publiques aux communications électroniques et aux données stockées par les fournisseurs de services numériques.
19. Voir, par exemple, P. Jacob, « Quand les nuages ne s'arrêtent pas aux frontières. Remarques sur l'application du droit dans l'espace numérique à la lumière du Cloud Act », *Cahiers de droit de l'entreprise*, n° 4, 2018, dossier 28 ; R. Bismuth, « Every Cloud Has a Silver Lining », *op. cit.*
20. Pour le détail de ces deux positions, voir *United States v. Microsoft Corp.*, *op. cit.*

En droit international un État peut généralement adopter des règles ayant des effets à l'étranger (pouvoir normatif). En revanche, il ne peut exercer directement un pouvoir de contrainte sur le territoire d'un autre État sans son consentement (pouvoir d'exécution). Dès lors, l'ordonnance du juge peut être interprétée de deux manières. Il peut s'agir de l'exercice d'un pouvoir normatif adressé aux fournisseurs de services, ou d'un pouvoir d'exécution, puisqu'elle conduit à la saisie des données. Cependant, en raison de la spécificité des données numériques, l'ordonnance du juge américain – issue de l'exercice de son pouvoir d'exécution – ne requiert pas l'intrusion d'un agent étranger sur le territoire de l'État sur lequel se situent les données. Une violation de l'intégrité territoriale (systèmes d'information et données numériques) de l'État de stockage des données peut-elle alors être établie ?

En pratique, les avis des États sont, à l'heure actuelle, divisés. Alors que la France considère que toute intrusion dans ses systèmes d'information constitue une violation de sa souveraineté[21], cette qualification n'est pas entièrement partagée par le Royaume-Uni[22]. Les droits nationaux[23] comme régionaux[24] autorisent l'accès à des données situées à l'étranger avec des interactions, voire des concurrences, de plus en plus fortes entre elles. Il est dès lors indispensable de réfléchir aux mécanismes de coordination entre ces dispositifs normatifs.

Face à la portée extraterritoriale des lois américaines sur les données, l'UE a choisi de répondre par la voie normative. Elle s'est progressivement dotée de règles communes visant à protéger les données personnelles et à encadrer les transferts de données à l'étranger, limitant l'exposition de celles-ci à des juridictions étrangères. Cette stratégie s'est notamment matérialisée par l'adoption du RGPD.

21. « Droit international appliqué aux opérations dans le cyberespace », Ministère des armées, 2019, p. 6.
22. Tout en reconnaissant le caractère fondamental du principe de souveraineté, le Royaume-Uni considère qu'il n'existe pas de règle spécifique au cyberespace permettant d'affirmer la violation de la souveraineté territoriale en cas d'intrusion dans les réseaux informatiques d'un autre État sans son consentement : Attorney General Jeremy Wright, *Cyber and International Law in the 21st Century*, discours du 23 mai 2018. Cette position a été confirmée par la suite : « Application of International Law to State's Conduct in Cyberspace: UK Statement », *Policy Paper*, United Kingdom, Foreign, Commonwealth & Development Office, juin 2021, § 9.
23. Parmi quelques exemples, en sus du *CLOUD Act* précité, voir pour le Brésil : LAW NO. 12,965, 2014 (Art. 11), et Poder360, « Justiça pode pedir dados de big techs no exterior, diz STF » ; les Pays-Bas : Wetboek van Strafvordering, 1921 (Art. 126ND, 126NG(2)) ; la Lituanie : European Judicial Network, Fiches Belges on Electronic Evidence ; ou encore l'Inde : The Code of Criminal Procedure, 1973 (Chapter VII) (India).
24. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), article 3 ; Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale, article 2.

La riposte extraterritoriale européenne par le RGPD

Les révélations d'Edward Snowden en 2013 sur les programmes de surveillance de la NSA ont ravivé en Europe les préoccupations relatives à la surveillance de masse et ont contribué à accélérer l'adoption d'un cadre juridique plus strict relatif à la protection des données personnelles[25]. Le RGPD adopté en 2016 et entré en vigueur en 2018 est venu encadrer la collecte, le traitement et le stockage des données personnelles dès lors que le traitement des données concerne des citoyens européens ou qu'il a lieu sur le territoire de l'UE.

Considéré comme une innovation juridique majeure, le RGPD a, pendant un temps (aujourd'hui révolu), incarné l'affirmation d'une hégémonie normative européenne, souvent décrite par l'expression d'« effet Bruxelles », popularisée par Anu Bradford[26]. Sa portée est également extraterritoriale : le règlement s'applique non seulement aux organisations établies dans l'UE, mais aussi à toute entreprise située hors de l'UE dès lors qu'elle traite les données de toute personne (y compris non-citoyenne de l'Union) localisée sur le territoire européen. Ainsi, même les géants américains du numérique sont soumis au RGPD lorsqu'ils collectent et traitent des données d'utilisateurs européens. Ces exigences réglementaires s'appliquent également dans le cadre du transfert de données personnelles hors de l'UE. Tout transfert de données vers un pays tiers est conditionné par l'existence d'un niveau de protection adéquat formalisé par la Commission européenne dans le cadre d'une « décision d'adéquation[27] », ou par des garanties contractuelles telles que les « clauses contractuelles types » ou les « règles d'entreprise contraignantes » (BCR). Les transferts de données qui font l'objet d'une décision d'adéquation sont autorisés après examen de l'état de droit prévalant dans le pays tiers et en vertu de l'existence d'autorités de contrôle indépendantes de protection des données.

Entre les États-Unis et l'UE, plusieurs décisions d'adéquation se sont succédé. La première décision d'adéquation, connue sous le nom de *Safe Harbour*, adoptée en 2000, a été invalidée par la Cour de Justice de l'Union européenne (CJUE) en octobre 2015 dans un premier arrêt *Schrems*. En 2016, une seconde décision d'adéquation, le *Privacy Shield*, a été adoptée puis de nouveau invalidée quatre ans plus tard par la Cour, après examen de la législation américaine en matière d'accès aux données par les services de renseignements américains. Une dernière décision d'adéquation a finalement été approuvée en juillet 2023, le *Data Privacy Framework* (DPF)

25. A. Cattaruzza, « Une territorialisation par le droit », *in Géopolitique des données numériques*, Paris, Le Cavalier Bleu, 2019, p. 102.
26. A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford, Oxford University Press, 2020.
27. Décision de la Commission européenne qui atteste du niveau adéquat de protection des données personnelles par un pays tiers et autorise le transfert des données dans ledit pays.

en dépit des controverses entourant l'accord[28]. Celui-ci résulte de la signature en octobre 2022 par l'ancien président Joe Biden d'un décret présidentiel prévoyant des mesures de « renforcement des garanties applicables aux activités de renseignement d'origine électromagnétique des États-Unis ». Il est complété par un règlement du procureur général encadrant la création et le fonctionnement de la Cour chargée du contrôle de la protection des données (DRPC), placée sous la supervision du Conseil de surveillance de la vie privée et des libertés civiles (PCLOB). Cet organe est chargé de prendre en compte les préoccupations liées à la vie privée et aux libertés civiles aux États-Unis lors de l'élaboration des lois et politiques en lien avec le terrorisme depuis 2004.

Le retour de Donald Trump à la Maison-Blanche a réactivé les inquiétudes autour des transferts de données personnelles entre l'UE et les États-Unis. Le licenciement de la quasi-totalité des membres du PCLOB (dont trois membres démocrates sur les cinq que compte le conseil) en février 2025 a conduit à son démantèlement, fragilisant ainsi l'équilibre déjà précaire sur lequel repose le cadre transatlantique de protection des données. Le DPF de 2023 soulignait pourtant le rôle primordial du PCLOB pour garantir la conformité des pratiques des agences de renseignement américaines aux standards de protection des données de l'UE[29]. La suspension inopinée des activités de ces organismes pourrait remettre en cause la capacité des États-Unis à garantir un contrôle indépendant sur l'accès des agences de renseignement aux données étrangères. Pour l'Europe, une telle évolution ravive l'éventualité d'une invalidation du DPF et pourrait remettre en question la sécurité juridique des transferts de données transatlantiques. De fait, les flux de données pourraient à nouveau se retrouver dans une zone grise avec des transferts autorisés en pratique mais juridiquement contestés, suggérant un risque de multiplication des contentieux voire de perturbation des services numériques.

Au-delà des enjeux liés à l'extraterritorialité du droit américain, l'Europe est également confrontée à la domination structurelle des grandes entreprises technologiques sur les infrastructures et services numériques, en particulier dans le domaine du *cloud*. Cette concentration du marché renforce les dépendances technologiques européennes et contrevient aux ambitions stratégiques du continent en matière de souveraineté sur les données.

28. Le *Data Privacy Framework* demeure controversé en dépit de son adoption, considéré par certains comme une « copie de *Privacy Shield* ». Lire J. Cheminat, « Le Data Privacy Framework entériné et déjà contesté », *Le Monde informatique*, 10 juillet 2023.
29. S. L. Perez, « What the PCLOB Firings Mean for the EU-US Data Privacy Framework », Center for Democracy and Technology, 14 février 2025.

L'exterritorialité sur les données favorisées par la mainmise des Big Tech sur le *cloud*

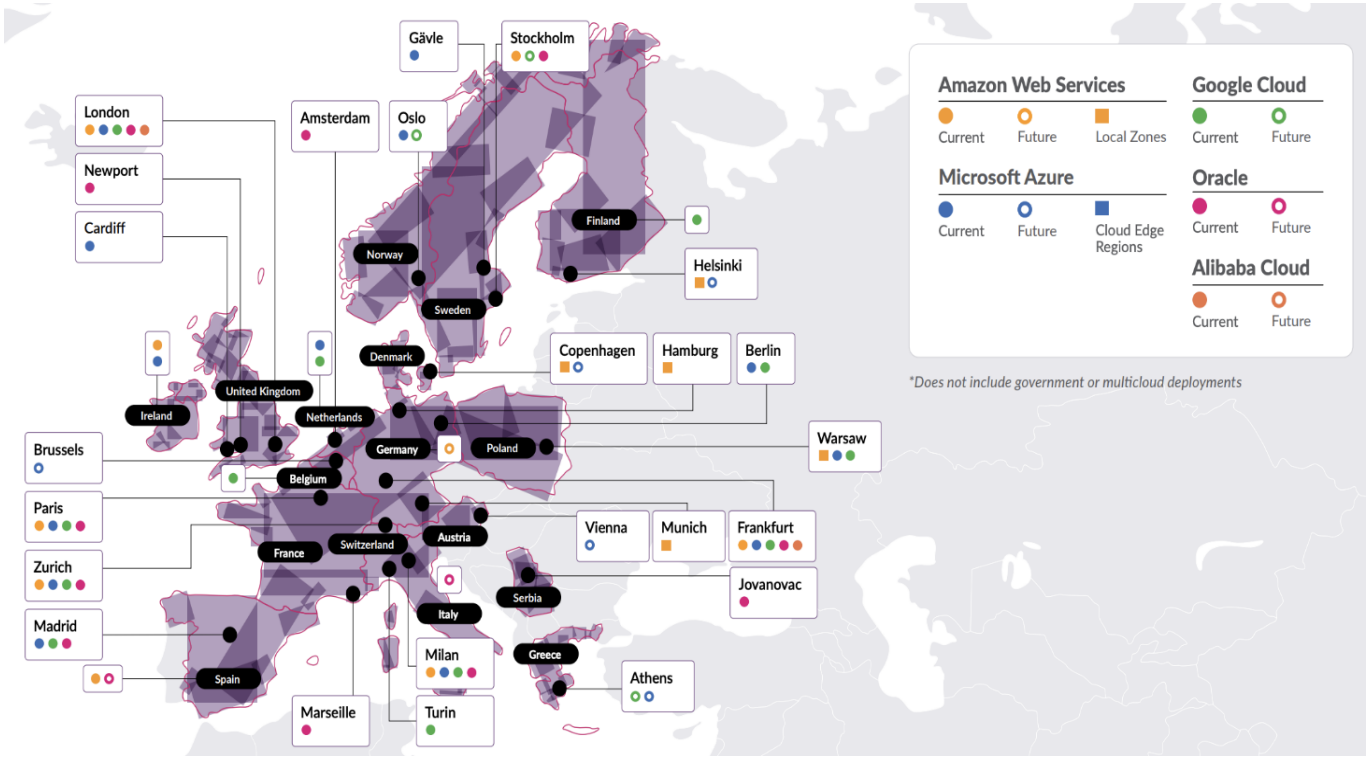
Le *cloud computing* est une technologie névralgique du numérique, principalement construite au moyen de réseaux de *data center*s. Elle est définie par le géographe Amaël Cattaruzza comme un « mode d'organisation des systèmes d'information et de communication » qui s'est soustrait du seul champ technique pour investir celui du politique et du stratégique[30]. Cette évolution tend à suggérer que l'extraterritorialité du droit américain s'est avérée, en pratique, plus efficace que celle du droit de l'UE. Cela s'explique par la nationalité (américaine) des fournisseurs de services. De fait, s'ajoute au problème d'application extraterritoriale de la norme, celui de la domination des États-Unis sur le *cloud* d'infrastructure et de service[31], facilitant la justification de l'exercice de leurs compétences au titre du rattachement territorial (lieu d'activité de la société) ou personnel (la nationalité des entreprises).

La domination mondiale des acteurs américains dans le cloud

Les *hyperscalers* sont des fournisseurs de services *cloud* à grande échelle. Le marché du *cloud* est largement dominé par les *hyperscalers* américains Google Cloud, Microsoft Azure et Amazon Web Services, qui engrangent près de 63 % des parts du marché mondial, contre seulement 6 % pour les entreprises chinoises Alibaba Cloud (4 %) et Huawei (2 %)[32]. Cette concentration inédite des parts de marché du *cloud* par une poignée d'acteurs privés étrangers soulève naturellement des enjeux de souveraineté face à la dépendance des administrations et des entreprises aux services numériques de sociétés extra-européennes. En 2025, seules 15 % des parts du marché européen étaient détenues par des fournisseurs régionaux (contre 29 % en 2017) tandis que les trois géants américains en possédaient plus de 70 %[33].

30. A. Cattaruzza et C. Bômont, « Le *cloud computing* : de l'objet technique à l'enjeu géopolitique. Le cas de la France », *Hérodote*, n° 177-178, 2020, p. 149-163.
31. « Cloud Market Jumped to $330 billion in 2024 – GenAI Is Now Driving Half of the Growth », Synergy Research Group, 6 février 2025.
32. Le marché des services informatiques en nuage est très largement dominé par les *hyperscalers* américains Amazon AWS (28 % des parts du marché mondial), Microsoft Azure (21 %) et Google Cloud (14 %). Lire F. Richter, « Big Three Hold Dominant Lead in Accelerating Cloud Market », Statista, 9 février 2026.
33. « European Cloud Providers' Local Market Share Now Holds Steady at 15 % », Synergy Research Group, 24 juillet 2025 ; « EuroStack – A European Alternative for Digital Sovereignty », Bertelsmann Stiftung, février 2025.

Présence européenne des principaux fournisseurs de services *cloud*



Source : « EMEA Hyperscale Deployment Map », DC Byte, mars 2025.

Leur positionnement oligopolistique leur permet de maîtriser l'ensemble de la chaîne de valeur technologique : des infrastructures physiques (*data centers*) à l'accès à la puissance de calcul (*cloud*). Désormais, 1 189 des plus grands centres de données au monde, dits « *hyperscale* », sont opérés par les *hyperscalers*, soit 44 % de la capacité mondiale de l'ensemble des centres de données[34]. Par ailleurs, la forte pénétration des géants du numérique sur le marché du *cloud* entraîne certains obstacles structurels à la migration vers d'autres fournisseurs de services informatiques en nuage. De nombreuses organisations se retrouvent ainsi aux prises avec des effets de verrouillage (*vendor lock-in*) en raison de licences propriétaires, de frais d'extraction et de réarchitecturation prohibitifs qui rendent le transfert vers un autre fournisseur techniquement complexe et financièrement coûteux[35].

34. « The World's Total Data Center Capacity Is Shifting Rapidly to Hyperscale Operators », Synergy Research Group, 24 juin 2025.
35. H. Le Picard, « Startups européennes et IA générative dépassent la domination des Big Tech », *Études de l'Ifri*, Ifri, avril 2025 ; M. Ashare, « UK Regulators Sound The Alarm On *Cloud* Vendor Lock-In », CIO Dive, 31 mai 2024.

La montée en puissance d'acteurs chinois sur le marché mondial du cloud

La confiance accordée aux fournisseurs de services *cloud* repose à la fois sur des critères techniques et des considérations géopolitiques et stratégiques. Les acteurs chinois, bien que disposant de solides capacités technologiques, se heurtent à une méfiance occidentale systémique alimentée par les craintes d'instrumentalisation étatique des données – inquiétudes qui, paradoxalement, rejoignent celles exprimées à l'endroit du *CLOUD Act* américain mais conduisent à des réponses politiques asymétriques.

Aussi, la présence plus timorée de *clouders* chinois en Europe ne saurait être négligée. En tant que composante technologique de sa stratégie de Routes de la soie numériques, la Chine entend faciliter l'implantation des champions nationaux à l'étranger. Cela passe par le développement d'infrastructures numériques, dont le *cloud computing*, les *data centers*, la 5G, la fibre optique, la communication par satellite et l'IA. À ce jour, la Chine aurait signé près d'une vingtaine d'accords dans différentes régions du monde[36]. De nombreuses entreprises technologiques chinoises ont ainsi étendu leur influence de l'Asie à l'Afrique en passant par le Moyen-Orient, l'Amérique latine, mais aussi l'Europe. Alibaba Cloud, filiale du géant chinois du commerce électronique, a ainsi renforcé ses régions *cloud*[37] en Arabie saoudite, aux Émirats arabes unis, aux États-Unis (dont une à Washington D.C.), en Allemagne, au Royaume-Uni et devrait bientôt s'établir en France[38]. Cette stratégie d'expansion territoriale est également poursuivie par la plateforme sociale TikTok qui a investi plus d'un milliard d'euros dans la construction d'un très grand centre de données en Finlande, financé aux côtés de l'opérateur de centre de données chinois DayOne[39]. La filiale de ByteDance étend ainsi son maillage infrastructurel international après l'ouverture d'un premier centre de données en Irlande en 2023 et d'un second en Norvège en 2024[40] dans le cadre du Projet Clover[41]. TikTok a par ailleurs récemment annoncé la construction d'un centre de données au

36. J. Kurlantzick et J. West, « Assessing China's Digital Silk Road Initiative », Council on Foreign Relations, 18 décembre 2020.
37. Une région *cloud* désigne une entité géographique délimitée au sein de laquelle un fournisseur de services de *cloud* déploie un ensemble cohérent de ressources informatiques (infrastructures de calcul, de stockage, de mise en réseau et de gestion des données) destinées à héberger et à exécuter des services numériques.
38. C. Bohic, « La stratégie IA "full stack" d'Alibaba Cloud passe par la France », Silicon, 29 septembre 2025.
39. K. Wu et Y. Ngui, « Data Centre Operator Dayone Aims to Raise Over $1 Billion, Sources Say », Reuters, 17 octobre 2025 ; « Singapore's Dayone Plans EUR 1.2 Billion Hyperscale Data Centre in Finland », Data Center Forum, 26 août 2025.
40. « TikTok's Data Migration to Norwegian Data Center Has Begun », Data Center Forum, 4 novembre 2024.
41. TikTok investira 12 milliards d'euros sur dix ans dans le cadre du Projet Clover afin de rapatrier l'ensemble des données des 175 millions d'utilisateurs européens sur le territoire de l'UE. Cette politique s'inscrit dans un effort de protection des données personnelles, pourtant remis en cause pour son manque d'efficacité réelle par les commissions parlementaires sur TikTok. Lire les rapports parlementaires « La tactique TikTok : opacité, addiction et ombres chinoises », Sénat, 4 juillet 2023 et « Rapport sur les effets psychologiques de TikTok sur les mineurs », Tome I, Assemblée nationale, 4 septembre 2025.

Brésil, un projet d'investissement estimé à plus de 9 milliards de dollars[42]. Il convient toutefois de souligner que la cartographie de ces infrastructures demeure partielle. De nombreux fournisseurs de services *cloud* sont hébergés « en colocation », soit dans des centres de données exploités par des tiers, et ne possèdent pas nécessairement leurs propres infrastructures (ce qui rend leur identification plus difficile). Une estimation précise du nombre de *data centers* exploités par les *clouder* chinois est par conséquent difficile à établir.

Une relation de dépendance à haut risque pour l'Europe

Dans un contexte géopolitique marqué par des tensions transatlantiques crispées autour de la régulation des services numériques et des grandes plateformes[43], l'hypothèse d'une interruption à grande échelle des services numériques aussi appelé « *kill switch* », sur la base d'une décision politique, quoique théorique, n'en demeure pas moins réaliste[44]. C'est précisément ce que suggère le chercheur David Monniaux du Centre national de la recherche scientifique (CNRS) dans une tribune publiée dans *Le Monde* en octobre 2025, interrogeant les conséquences potentielles d'un ordre présidentiel américain enjoignant aux GAFAM de cesser leurs prestations à l'égard des gouvernements européens[45]. Cette perspective peut néanmoins être relativisée du côté français. La mise en œuvre d'une politique gouvernementale volontariste a permis de soutenir les acteurs européens et nationaux du *cloud* et d'encadrer strictement le choix des services numériques employés par l'administration française. Les commandes passées en 2025 sur le marché de l'Union des groupements d'achats publics (UGAP) auprès d'OVH s'élevaient ainsi à plus de 25 millions d'euros contre moins de 10,6 millions d'euros pour AWS et Microsoft réunis[46]. La situation internationale incertaine appelle néanmoins au passage à l'échelle d'alternatives européennes robustes et résilientes afin d'assurer la continuité des services numériques en cas de crise.

La dépendance technologique chronique à un faible nombre d'acteurs étrangers expose l'Europe à des risques systémiques – une préoccupation partagée par les États-Unis – comme l'ont illustré les défaillances successives survenues en octobre 2025. La panne mondiale d'Amazon Web Services le 20 octobre 2025, consécutive à une défaillance d'un centre de données en Virginie, suivie le 29 octobre par celle de Microsoft Azure, a mis en évidence

42. « Brazil to Begin Construction on Tiktok Data Center in Six Months, Minister Says », Reuters, 10 octobre 2025.
43. E. Badaoui, « États-Unis : l'arsenalisation de la liberté d'expression », *in* T. de Montbrial et D. David (dir.), *Ramses 2026. Un nouvel échiquier*, Paris, Ifri/Dunod, 2025, p. 318-321.
44. Voir introduction, p. 6.
45. Lire également R. Bacqué, D. Leloup et A. Piquard, *Nos nouveaux maîtres*, Paris, Albin Michel, 2026.
46. En 2024, les commandes publiques auprès d'OVH s'élevaient à 23,4 millions d'euros contre 11,7 millions d'euros pour AWS et Microsoft. Voir « L'adoption du *cloud* », disponible sur : www.numerique.gouv.fr.

la fragilité d'infrastructures numériques interconnectées dont l'indisponibilité a engendré des conséquences économiques et opérationnelles majeures pour les États et entreprises européennes[47]. Entre autres exemples d'offres « de confiance » des *hyperscalers* américains, l'hébergement des données de santé des Français sur le *cloud* Azure de Microsoft par le *Health Data Hub* (Plateforme des données de santé) a suscité de vives inquiétudes quant au potentiel accès à des données sensibles par les services de renseignements américains. Ce choix est aujourd'hui remis en cause par la plateforme qui cherche à opérer une migration vers un hébergeur souverain par crainte que les autorités américaines procèdent à une collecte des données de santé des citoyens français[48]. Ces inquiétudes sont d'autant plus corroborées par les allégations récentes de la société Microsoft, qui a confirmé en juillet 2025 qu'elle transférerait, sur demande des autorités américaines, les données des utilisateurs bien qu'elles soient stockées sur le territoire français[49].

Les risques liés à la cybersécurité, la disponibilité, la confidentialité et l'intégrité des données stockées dans le *cloud* conduisent à une tendance mondiale à la relocalisation des données. En témoignent les législations contraignantes adoptées par l'Arabie saoudite, les Émirats arabes unis, la Chine, l'Europe et les États-Unis eux-mêmes, qui imposent le stockage domestique de leurs données.

47. « AWS, le service *cloud* d'Amazon, annonce avoir résolu la panne qui a touché des applications dans le monde entier », *Le Monde*, 21 octobre 2025 ; « Microsoft Azure, deuxième plateforme *cloud* au monde, touché par une panne », *Le Monde*, 29 octobre 2025.
48. A. Vitard, « Le Health Data Hub met 6,2 millions d'euros sur la table pour reprendre la main sur les données de santé », L'Usine Digitale, 2 juillet 2025.
49. D. Monniaux, « Que se passerait-il si Trump ordonnait aux Gafam de cesser leurs services *cloud* à l'égard de nos gouvernements ? », *Le Monde*, 23 octobre 2025.

Une exigence accrue de localisation des données

La souveraineté numérique, aujourd'hui défendue par tous[50], procède d'un mouvement de réaction aux velléités extraterritoriales de certains États présentées ci-dessus. Elle se traduit concrètement par l'adoption de normes contraignantes, en particulier sur la localisation des données. Contrairement à la norme extraterritoriale, dont la « mise en œuvre tient compte d'éléments situés en dehors du territoire », la norme territoriale est celle « dont tous les éléments de mise en œuvre se trouvent sur le territoire[51] » de l'État qui l'a émise. L'application territoriale ne devrait donc avoir d'effet que sur le territoire de l'État qui l'applique. Cette limitation strictement territoriale est toutefois difficilement concevable dans le contexte numérique, particulièrement s'agissant des données. Plusieurs États ont adopté des lois leur permettant d'exercer leur compétence sur les données, les serveurs ou les activités numériques situés sur leur territoire en forçant parfois cette localisation nationale[52]. Le fait que les données soient stockées sur le territoire d'un État rend celui-ci compétent pour les saisir, sans pour autant empêcher d'autres États de revendiquer l'exercice de leurs compétences sur ces données en invoquant un critère de rattachement autre que territorial (personnel ou matériel).

Russie, Chine : la localisation des données par le droit à des fins idéologiques

Dès les années 2000, la Russie et la Chine posent les prémices d'une réflexion sur la souveraineté numérique et réclament une gouvernance internationale d'Internet plus équilibrée face à l'hégémonie des géants du numérique américains[53]. L'affaire Snowden cristallise les craintes d'espionnage et entraîne un mouvement global de protectionnisme numérique visant principalement à sécuriser la circulation des données. La Russie, pionnière en matière de souveraineté numérique, adopte en 2014 la loi 242-FZ qui relocalise les données des citoyens et des entreprises russes sur le territoire national. Le critère territorial est ici doublé d'un rattachement personnel

50. A.-Th. Norodom, « Être ou ne pas être souverain, en droit, à l'ère numérique », *in* V. Ndior et L. Rass-Masson (dir.), *Enjeux internationaux des activités numériques*, Paris, Larcier, 2020.
51. B. Stern, « Une tentative d'élucidation du concept d'application extraterritoriale », *op. cit.*, p. 64.
52. A. Chander et U. P. Lê, « Data Nationalism », *Emory Law Journal*, vol. 64, n° 3, 2015, spécialement p. 682-713.
53. P. Türk, « La souveraineté numérique européenne, vers une troisième voie ? », *Pouvoirs*, n° 190, 2024.

puisque toutes les entreprises traitant de données de citoyens russes doivent les stocker sur le territoire russe. Cette initiative est complétée en 2019 par la loi sur le « Runet souverain » qui concède aux autorités le pouvoir d'opposer un contrôle entier sur les flux de données entrants et sortants du territoire[54].

Sur les pas de son allié russe, la Chine adopte dès 2017 plusieurs lois de localisation des données : la Loi sur la cybersécurité (2017), la Loi sur la sécurité des données (2021) et la Loi sur la protection des informations personnelles (2021) inspirée du RGPD européen. Cet arsenal législatif contraignant à portée extraterritoriale impose des obligations de localisation des données sur le territoire chinois pour les opérateurs d'infrastructures critiques et des contrôles stricts sur les transferts transfrontaliers de données. Consacrées au titre de ressources stratégiques nationales, les données chinoises et plus particulièrement leurs transferts transfrontaliers ont fait l'objet de nouvelles restrictions en 2025[55]. Ainsi, les régulateurs chinois exigent désormais des opérateurs d'infrastructures d'information non critiques qu'ils obtiennent des certifications en amont de certains transferts de données sensibles, dont les catégories sont élargies.

États-Unis : la localisation des données par le droit à des fins de sécurité nationale

Alors que les États-Unis défendent traditionnellement le principe de libre circulation des données (ou « *free flow of data* »), des initiatives réglementaires récentes tendent à infléchir cette tendance. Les données personnelles sensibles sont particulièrement visées, en ce qu'elles pourraient être transférées vers des pays rivaux des États-Unis. En octobre 2023, le Bureau du Représentant américain au commerce (USTR) a retiré le soutien des États-Unis aux objectifs de négociation commerciale numérique à l'Organisation mondiale du commerce (OMC), anéantissant des décennies de politique américaine. Ces objectifs incluaient la protection des flux transfrontaliers de données, l'interdiction des exigences de localisation des données et la protection du code source appartenant aux États-Unis contre la divulgation forcée aux gouvernements étrangers[56].

Ce changement de paradigme est consacré par l'adoption en février 2024 du décret présidentiel de l'ancien président Joe Biden sur la « prévention de l'accès aux données personnelles sensibles des citoyens et du

54. T. Derivry, « La souveraineté numérique russe en 5 questions avec Kevin Limonier », Sciences Po, 18 octobre 2022.
55. A. Huld, « New Guidelines on Handling Sensitive Personal Data in China in Effect November 1 », China Briefing, 11 septembre 2025.
56. M. Broadbent, « USTR Upends U.S. Negotiating Position on Cross-Border Data Flows », Center for Strategic and International Studies, 12 décembre 2023.

gouvernement américain par les pays préoccupants[57] ». Le texte entré en vigueur en avril 2025 sous la présidence de Donald Trump entend restreindre les transferts de données personnelles sensibles à certains pays considérés comme « préoccupants », à savoir la Chine, Cuba, le Venezuela, l'Iran, la Corée du Nord et la Russie. L'interdiction ciblée de certains transferts de données sensibles hors du territoire américain sert avant tout à prévenir leur exploitation et leur manipulation à des fins malveillantes, notamment dans le cadre d'activités d'espionnage, d'opérations cybernétiques ou d'influence rendues possibles par l'analyse de ces données à l'aide de technologies avancées comme l'IA. L'*Executive Order* s'inscrit toutefois moins dans une logique de protection de la vie privée que dans un effort de sécurité nationale, réaffirmant l'attachement des États-Unis au principe de libre circulation transfrontière des données.

La stratégie européenne sur les données repose quant à elle sur une approche relativement différente. L'Europe cherche moins à restreindre les flux de données qu'à en encadrer la circulation dans un cadre juridique commun, destiné à concilier protection des données, innovation et développement d'un marché unique de la donnée.

Europe : la localisation des données par le droit à des fins de protection et d'innovation

La construction d'un cadre réglementaire européen en faveur de la circulation des données

Dans la continuité de la Stratégie européenne pour les données présentée en 2020, l'UE a élaboré un corpus réglementaire conséquent, destiné à façonner un véritable marché unique de la donnée tournée vers l'innovation et la compétitivité :

- Le RGPD assure la protection des données personnelles des citoyens européens et encadre leur transfert hors de l'UE. Les données personnelles concernent toute information qui se rapporte à une personne physique identifiée ou identifiable.
- La loi sur la gouvernance des données (*Data Governance Act*) fixe les conditions de la circulation et du partage des données personnelles et non personnelles (industrielles, par exemple).
- La loi sur les données (*Data Act*) facilite l'accès, le partage et l'utilisation des données personnelles et non personnelles générées par l'Internet des

57. *Executive Order* n° 14117 du 28 février 2024 visant à empêcher l'accès aux données personnelles sensibles des Américains et aux données liées au gouvernement des États-Unis par les pays concernés.

objets (IoT) et les données de performance. Il établit des règles pour favoriser la portabilité des données entre les fournisseurs de services de *cloud* et l'interopérabilité des données[58].

- La directive Open Data rend les données publiques (administrations et services publics) plus accessibles et réutilisables pour encourager l'innovation et la transparence.
- Le règlement sur l'IA (*AI Act*) insiste sur la nécessité d'accès à des données de manière fiable, responsable, non discriminatoire et de haute qualité pour entraîner les systèmes d'IA à haut risque[59].
- Le règlement sur les marchés numériques (*Digital Markets Act* ou DMA) encadre les combinaisons de données que peuvent effectuer les grandes plateformes par l'accumulation massive de celles-ci, limite l'utilisation de données agrégées et les pratiques anticoncurrentielles des grandes plateformes numériques au sein de l'Union.
- Enfin, le règlement sur les services numériques (*Digital Services Act* ou DSA) limite les risques systémiques liés à l'utilisation massive des données par les grandes plateformes numériques (notamment par leurs systèmes de recommandation algorithmique).

La constitution d'un tel espace européen de circulation et de mutualisation des données permet non seulement de renforcer la souveraineté numérique européenne, mais aussi de stimuler l'innovation et la recherche technologique, notamment en IA, en fournissant aux chercheurs et aux entreprises un accès sécurisé à des volumes de données de haute qualité. Ce dernier objectif d'innovation est consolidé par la simplification progressive des réglementations encadrant le secteur numérique. Depuis 2024, la Commission a entrepris un vaste chantier de réflexion sur la régulation du numérique, s'inspirant pour ce faire des recommandations des rapports Draghi (septembre 2024) et Letta (avril 2024). Ces rapports remarqués préconisaient d'assouplir les exigences réglementaires et de créer une cinquième liberté fondée entre autres sur la libre circulation des données afin de lâcher la bride de l'innovation technologique en Europe et renforcer l'autonomie stratégique du continent.

Mario Draghi a de nouveau appuyé cette demande en septembre 2025, appelant même à une « simplification radicale » des réglementations numériques pour stimuler l'innovation en IA au sein de l'UE[60]. Cette vaste initiative d'amendement des textes réglementaires s'est concrétisée en novembre 2025 par une nouvelle loi, communément nommée paquet

58. L'interopérabilité des données désigne la capacité de systèmes d'information distincts à échanger, comprendre et exploiter des données de manière compatible.
59. Un système d'IA à haut risque est défini comme un système qui présente « un risque significatif d'atteinte à la santé, à la sécurité ou aux droits fondamentaux des personnes » (art. 6, règlement UE 2024/1689 sur l'intelligence artificielle).
60. C. Moreau et M. Henning, « Mario Draghi appelle à un assouplissement du RGPD et à une suspension partielle de l'*AI Act* », Euractiv, 16 septembre 2025.

« omnibus numérique ». Elle repense en profondeur la stratégie européenne sur les données, opérant un virage marqué de la protection des données à leur mise en commun à des fins d'innovation.

Concrètement, les règles du RGPD relatives à la protection des données personnelles sensibles pourraient être assouplies afin de permettre leur collecte et leur traitement – sur la base d'un « intérêt légitime » – dans le cadre de l'entraînement et de l'inférence de systèmes d'IA[61]. S'agissant du règlement sur l'IA, la mise en application de certaines de ses dispositions pourrait être retardée de plusieurs mois, notamment les exigences relatives à la transparence, la robustesse et la traçabilité des systèmes d'intelligence artificielle à haut risque[62]. Des modifications sont également prévues concernant le règlement sur les services numériques (DSA) en raison de potentielles superpositions du texte avec d'autres réglementations européennes, notamment sur l'IA[63]. Une révision du règlement sur les marchés numériques (DMA) est également entamée depuis le mois d'août et accorde une attention particulière aux services basés sur l'IA[64].

La volonté de la Commission de simplifier son corpus réglementaire pour stimuler l'innovation en IA soulève néanmoins des interrogations, notamment face aux pressions croissantes exercées par la Maison-Blanche sur les politiques numériques de l'UE. Le paquet « omnibus numérique » intervient en effet dans un contexte où les États-Unis multiplient les avertissements à assouplir les réglementations visant les grandes plateformes, jugées trop contraignantes pour les entreprises américaines. Les déclarations récentes du secrétaire américain au Commerce, qui conditionnent l'aboutissement d'accords commerciaux à un allègement des règles concernant le DSA et le DMA, illustrent ces pressions[65]. De même, la récente offensive de Marco Rubio à l'égard du RGPD jugé comme une « réglementation inutilement contraignante » notamment en matière d'obligation de localisation des données, suggère qu'une ligne de front se creuse entre Washington et Bruxelles[66]. Ce rapport de force transatlantique semble d'autant plus avoir déjà fait ses preuves. En février 2025, la Commission européenne a abandonné la directive sur la responsabilité en

61. Les données personnelles sensibles, au sens de l'article 9 du RGPD, désignent notamment les informations révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses, l'appartenance syndicale, ainsi que les données génétiques, biométriques, de santé ou relatives à la vie sexuelle et à l'orientation sexuelle d'une personne. Le traitement desdites données est interdit sauf cas spécifique (consentement de la personne, intérêt public, etc.)
62. V. Lequeux, « Numérique : la Commission européenne dévoile son chantier de simplification », Toute l'Europe, 19 novembre 2025.
63. A. Datta, « La Commission prépare une nouvelle vague de simplification des règles numériques », Euractiv, 18 novembre 2025.
64. M. Henning, « La Commission entame sa révision du DMA en mettant l'accent sur l'IA », Euractiv, 27 août 2025.
65. A. Datta, « Washington presse l'UE d'alléger ses règles numériques visant les géants tech américains », Euractiv, 24 novembre 2025.
66. R. Bellan, « US Tells Diplomats to Lobby Against Foreign Data Sovereignty Laws », TechCrunch, 25 février 2026.

matière d'IA, à la suite des critiques de « surréglementation » de l'intelligence artificielle portées par James D. Vance à son encontre[67].

Les initiatives de simplification de la Commission suscitent également des débats en Europe, notamment au Parlement européen, divisé sur la question entre partisans de l'innovation et partisans de la protection des droits et libertés fondamentaux. Par ailleurs, une plus grande libéralisation du marché européen de la donnée pourrait paradoxalement renforcer l'avantage compétitif d'acteurs déjà dominants. En raison de leurs capacités financières, de leurs infrastructures *cloud* et de leurs outils d'analyse avancés, des entreprises comme Google, Amazon ou Microsoft se retrouvent bien souvent mieux positionnées pour exploiter rapidement et à grande échelle de nouveaux flux de données. Dans cette perspective, une attention particulière pourrait être portée au choix d'acteurs européens pour le traitement et l'exploitation de ces données – dans une logique de « préférence numérique européenne » inspirée du modèle « Buy European », afin de soutenir l'écosystème numérique régional[68].

L'élaboration d'une stratégie sur les données pour l'intelligence artificielle

L'IA, levier de puissance économique et vecteur de leadership technologique,[69] est au cœur d'une course mondiale à l'innovation qui mobilise aussi bien les États que les entreprises privées de la *tech*. Le déploiement de cette technologie repose concomitamment sur l'accès à des volumes inédits de données et leur stockage, et le traitement par le biais de centres de données spécialisés, dotés de capacités de calcul, dont les besoins ne cessent de croître à un rythme effréné. L'UE, consciente de son retard technologique face à la Chine et aux États-Unis, refonde et déploie depuis plusieurs mois sa stratégie sur l'IA. Elle se manifeste concrètement par l'adoption de plusieurs documents d'orientation pour l'Europe : *AI Continent Action Plan* (mai 2025), *Apply AI Strategy* (novembre 2025), *Data Union Strategy: Unlocking Data for AI* (novembre 2025).

La politique de simplification entreprise par la Commission européenne permettrait ainsi de mieux soutenir les acteurs européens de l'IA générative (IAG) déjà à la marge dans la compétition technologique mondiale. Dans ce cadre, la localisation des données ne serait pas conçue comme une fin en soi, mais comme un levier stratégique visant à sécuriser les données sensibles, à renforcer la résilience des infrastructures et à permettre leur exploitation

67. A. Datta et T. Hartmann, « Après les critiques de JD Vance, la Commission retire la directive sur la responsabilité en matière d'IA », Euractiv, 12 février 2025.
68. Sur la préférence européenne dans les achats publics, lire la tribune de Stéphane Séjourné : « "Buy European" : le commissaire européen Stéphane Séjourné et 1.141 dirigeants d'entreprise lancent un appel en faveur de la préférence européenne dans les achats publics », *Les Échos*, 1er février 2026.
69. P. Riché, « Philippe Aghion, prix Nobel d'économie 2025 : "Le facteur-clé de la puissance économique, c'est le leadership technologique" », *Le Monde*, 13 octobre 2025.

dans un environnement conforme aux valeurs européennes. Ainsi, les futures initiatives législatives – dont la proposition de règlement sur le développement de l'informatique en nuage (*EU Cloud and AI Development Act*)[70] ou la loi sur les réseaux numériques (*Digital Networks Act*)[71] – prolongent cette ambition de fédérer les capacités *cloud*, moderniser le cadre juridique du partage de données et garantir un accès plus large aux ressources computationnelles nécessaires à l'entraînement des modèles avancés d'IA.

La Stratégie pour l'union des données publiée par la Commission le 19 novembre 2025 entend explicitement « faciliter l'accès aux données pour l'IA » et s'inscrit dans une dynamique qui vise simultanément à assurer une protection élevée des données et à créer les conditions d'une exploitation plus large des données de haute qualité pour soutenir l'innovation en intelligence artificielle. Cette politique contribuerait à :

- élaborer une « boîte à outils pour contrer la localisation injustifiée » des données par des États membres imposant des contraintes non justifiées aux flux transfrontières de celles-ci ;
- développer des espaces de données européens communs dans des secteurs clés dont la défense et le spatial et des laboratoires de données pour faciliter leur disponibilité ;
- et créer des synergies entre les espaces de données et l'écosystème d'IA européens[72].

Les espaces européens communs de données sont des infrastructures ouvertes, sécurisées et interopérables qui permettent de mutualiser des volumes massifs de données de haute qualité. Il s'agit là d'une condition essentielle au développement de modèles d'IA performants et fiables. Leur déploiement, soutenu par la Commission européenne et le programme-pilote Horizon Europe, pourrait contribuer à structurer un véritable marché unique de la donnée favorable à l'innovation. Des espaces de données sectoriels sont par exemple consacrés à certaines filières industrielles comme l'automobile avec l'initiative Catena-X, qui organise le partage sécurisé de données entre constructeurs et équipementiers[73].

Ainsi, bien que la stratégie européenne sur les données pour l'IA ne consacre pas explicitement une politique de localisation des données, elle

70. L'objectif de ce règlement prévu pour 2025, est de tripler la capacité des centres de données européens en cinq à sept ans en simplifiant leur déploiement. Parallèlement, une politique unifiée du *cloud* pour les administrations publiques est pensée pour renforcer la souveraineté numérique, encourager la croissance des fournisseurs européens et garantir l'accès à des infrastructures hautement sécurisées pour les usages critiques.

71. Ce texte entend faciliter le développement d'infrastructures et de plateformes numériques intégrées de bout en bout pour le *cloud*.

72. « European Data Union Strategy », Commission européenne, disponible sur : https://digital-strategy.ec.europa.eu.

73. F. Musiani, « Gaia-X : le pari d'un cloud européen souverain », *Polytechnique Insights*, 18 juin 2025.

instaure toutefois une localisation fonctionnelle et stratégique à l'échelle de l'UE. Celle-ci se superpose au principe de libre circulation des données par la structuration d'un espace de gouvernance, de mutualisation et de valorisation des données au sein du marché intérieur.

Les limites de la localisation des données par le droit

La pleine maîtrise des flux de données paraît peu crédible à l'heure du *cloud*, les données pouvant être partout[74]. Un serveur situé sur le territoire d'un État peut concerner des citoyens étrangers et les données circulent à travers plusieurs territoires, si bien qu'elles sont susceptibles d'être soumises à plusieurs juridictions successives[75]. Jennifer Daskal identifie ainsi différents problèmes attachés à la logique de territorialisation juridique des données[76] : les données sont mobiles, divisibles et cloisonnées, rendant leur localisation plus difficile. Il peut y avoir en conséquence une déconnexion entre la localisation de l'accès aux données et la localisation des données elles-mêmes, de même qu'entre les données et les utilisateurs de ces données. Les internautes perdent ainsi le contrôle de leurs données puisque ce sont les fournisseurs de services, Google ou Microsoft par exemple, qui décident de la localisation des données, sous réserve de ce que peuvent leur imposer les législations nationales ou régionales.

Ce contrôle des tiers sur nos données soulève deux enjeux[77]. D'une part, la localisation du siège social de ces fournisseurs de services – plus tangible – est finalement plus pertinente que celle des données pour justifier de l'exercice d'une compétence étatique. Il s'agit de l'argument soulevé par le gouvernement américain dans l'affaire Microsoft. D'autre part, l'utilisateur n'a plus le contrôle direct de ses données, ce qui renforce les obligations de protection et de confidentialité des fournisseurs de services indispensables à l'établissement d'un lien de confiance avec les utilisateurs. Cette situation aboutit à un paradoxe, en cela que les fournisseurs apparaissent comme les opérateurs les plus fiables pour permettre aux États d'exercer leur compétence et accéder aux données, mais ils doivent également garantir la protection des données à leurs clients. Or, la protection des données à l'égard

74. P. Schiff Berman, « Legal Jurisdiction and the Deterritorialization of Social Life », *Vandervilt Law Review En banc*, vol. 71, n° 7, p. 23 : « Non seulement l'emplacement [des données] est arbitraire, mais il est également malléable. Les données peuvent être facilement déplacées d'un endroit à un autre, instantanément et de manière algorithmique, sans qu'aucun être humain ne prenne consciemment la décision de les déplacer. Enfin, c'est le fournisseur de services, et non l'utilisateur final, qui contrôle en dernier ressort l'emplacement des données. Même si une personne vit toute sa vie dans un même territoire et dépose de l'argent dans la succursale locale d'une institution financière multinationale, les données relatives à ce compte peuvent être déplacées n'importe où, en fonction du système de stockage des données de l'institution financière » (notre traduction).
75. C. Bômont, « Maîtriser le *cloud* computing pour assurer sa souveraineté », *op. cit.*, p. 137.
76. J. Daskal, « The Un-Territoriality of Data », *Yale Law Journal*, vol. 125, n° 2, 2015, p. 326-398, p. 366 et suivantes.
77. *Ibid.*, p. 377-378.

des États repose sur ces acteurs économiques, qui restent soumis aux législations nationales pouvant exiger d'eux la fourniture de données, notamment pour des raisons de sécurité nationale.

Afin de résoudre ce paradoxe, il faudrait que les législations de localisation des données incluent systématiquement les exigences de respect des droits fondamentaux des utilisateurs[78] mais que les conditions générales d'utilisation respectent également les standards internationaux de protection des droits humains, tels que le droit au respect de la vie privée ou la liberté d'expression[79]. Au-delà de l'affirmation de ces principes, l'analyse de la pratique ne confirme pas ces exigences. En tout cas, le choix du fournisseur le mieux à même de protéger sa vie privée et ses données personnelles ne peut reposer sur le seul utilisateur. La volonté de localisation des données, même si elle part de l'idée de protéger les données des citoyens ainsi que les données sensibles des États, apparaît comme un vœu pieux. Les mouvements contradictoires observés de localisation territoriale de la donnée par le droit s'expliquent à la fois par la nature de la compétence exercée, normative (abstraite) ou d'exécution (concrète), et par la subjectivité dans laquelle on se situe (État d'origine ou État d'accueil). L'ubiquité de l'espace numérique fait que le rattachement territorial défendu par un État peut être contredit par le rattachement territorial avancé par d'autres.

Ces éléments mettent en évidence les limites d'une stratégie fondée uniquement sur le droit : la souveraineté ne peut être garantie si elle ne repose pas également sur la maîtrise matérielle des infrastructures numériques. Là encore, l'UE se heurte à des contraintes structurelles qui entravent l'émergence d'une réelle souveraineté numérique. Dès lors, la réponse la plus crédible et durable pour l'Europe réside dans l'ambition de développer, fédérer et faire croître un écosystème continental d'offres *cloud* suffisamment robuste pour briser la dépendance aux géants américains.

78. L'article 15 de la convention de Budapest sur la cybercriminalité adoptée le 23 novembre 2001 à Budapest, STE n° 185, exige que chaque Partie « veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures [...] soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés ». La convention des Nations Unies contre la cybercriminalité – Renforcement de la coopération internationale pour la lutte contre certaines infractions commises au moyen de systèmes d'information et de communication et pour la communication de preuves sous forme électronique d'infractions graves est construite sur le même modèle sur ce point mais, adoptée le 24 décembre 2024 à New York mais non encore entrée en vigueur, inclut deux clauses de garantie de protection des droits de l'homme (articles 6 et 24), pourtant jugées insuffisantes par la société civile. Voir, par exemple, D. Brown, « New UN Cybercrime Treaty Primed for Abuse », Human Rights Watch, 30 décembre 2024, disponible sur : www.hrw.org.

79. Voir à ce sujet, « L'évolution des conditions d'utilisation des réseaux sociaux et leur impact sur les droits de l'homme », Étude exploratoire 2022-2023, Programme de recherche « Gouvernance et régulation des réseaux sociaux », octobre 2023.

Limites et leviers pour l'Europe

Les limites structurelles à l'émergence d'un marché du *cloud* compétitif en Europe

Le marché du *cloud* en Europe, affaibli par des vulnérabilités structurelles, a fait l'objet d'une prise de conscience politique, certes tardive mais désormais convergente. Les rapports Draghi (2024) et Letta (2024), les travaux de la Commission IA (2024), la Boussole pour la compétitivité européenne (2025), ou encore la *Revue nationale stratégique* (2025) en France appellent tous à refonder en profondeur l'architecture numérique du continent et à construire un « vrai *cloud* européen » pour réduire les risques de vassalisation[80].

En Europe, la multiplication des solutions hybrides au détriment de l'autonomie stratégique numérique

L'UE ne dispose pas d'infrastructures numériques paneuropéennes suffisamment sécurisées, résilientes et interconnectées pour soutenir l'essor d'une économie fondée sur les données et *a fortiori* sur l'IA. À cela s'ajoute une forte fragmentation du marché unique : l'hétérogénéité des règles nationales, l'insuffisante interopérabilité des systèmes et la rareté des initiatives transfrontalières constituent autant de freins à l'innovation empêchant le passage à l'échelle d'acteurs européens. En pratique, de nombreuses initiatives dites « souveraines » s'appuient partiellement sur les technologies des grands fournisseurs internationaux[81]. Les opérateurs européens et les *hyperscalers* créent conjointement des offres *cloud* régionales, tandis que les *hyperscalers* apportent leur savoir-faire technique (infrastructures à grande échelle, services avancés) en garantissant que les données restent hébergées au sein de l'UE. Ce modèle hybride présente des avantages évidents : il permet d'exploiter l'innovation et les économies d'échelle des géants du *cloud* tout en assurant le respect des exigences locales de résidence et de sécurité des données.

80. A. Piquard, « Tech : il faut "acheter européen" pour éviter d'être une "colonie numérique", plaide le collectif Eurostack », *Le Monde*, 7 mai 2025.
81. A. Vitard, « Comment Gaia-X justifie-t-il la présence d'entreprises américaines et chinoises en son sein ? », L'Usine Digitale, 7 mai 2021.

En France, des offres de *cloud* de confiance « hybrides » émergent, soutenues par les infrastructures *hyperscales* américaines : « Bleu » d'Orange et de Capgemini en partenariat avec Microsoft et ; « S3NS » de Thalès et Google. Le directeur de l'ANSSI estime que les technologies Microsoft ou Google opérées par Bleu ou S3NS ne confèrent aucun contrôle direct aux fournisseurs américains sur les données hébergées, lesquelles demeurent sous la responsabilité exclusive d'entités européennes[82]. Ces offres se distinguent par ailleurs d'initiatives de « *cloud* souverain » proposées par des *hyperscalers* eux-mêmes, comme l'*Amazon European Sovereign Cloud*. Dans le cas de Bleu et S3NS, les infrastructures sont opérées par des entreprises européennes juridiquement indépendantes, ce qui permet de limiter l'applicabilité des législations extraterritoriales américaines. À l'inverse, malgré les garanties avancées par AWS, son offre (faussement) souveraine demeure liée capitalistiquement à la maison-mère et est donc susceptible de relever du droit américain. Ce phénomène participe d'une forme de « *sovereignty washing* », en présentant comme souveraines des offres qui reposent en réalité sur des infrastructures soumises juridiquement à des lois extraterritoriales[83].

Pour autant, ces enjeux juridiques ne doivent pas masquer la problématique plus large de la dépendance structurelle aux technologies étrangères qui dépasse le seul cadre de la cybersécurité. À cet égard, le collectif Eurostack, qui réunit 200 petites et moyennes entreprises, start-ups et plusieurs grands groupes européens (dont Airbus ou OVH par exemple), a alerté en mai 2025 la Commission européenne sur l'urgence de bâtir une véritable souveraineté numérique afin d'éviter que l'Europe ne devienne une « colonie numérique » de la Chine et des États-Unis. Dans une lettre adressée à Ursula von der Leyen, il rappelle que 80 % des dépenses européennes en logiciels et services *cloud* profitent aujourd'hui à des entreprises américaines et appelle ainsi à un « *Buy European Tech Act* ». Doté d'objectifs chiffrés – réserver 25 % des marchés publics du numérique aux solutions européennes, puis 50 % d'ici 2030 –, il entend également privilégier le recours à l'*open source*. Le collectif recommande également d'exclure des marchés publics les solutions impliquant des dépendances extraterritoriales américaines, y compris les solutions hybrides comme Bleu ou S3NS, et insiste sur le besoin de renforcer l'interopérabilité des services pour faciliter la migration vers d'autres fournisseurs. Il propose enfin un effort massif d'investissement public et privé *via* un fonds dédié au financement des technologies de rupture.

82. Ces offres satisfont aux exigences capitalistiques qui imposent aux acteurs extra-européens de ne pas détenir plus de 30 % de la solution, condition destinée à garantir que son contrôle et sa localisation restent en France. Lire A. Vitard, « Les offres S3NS et Bleu sont-elles vraiment immunisées aux lois américaines ? L'Anssi répond », L'Usine Digitale, 2 juin 2025.
83. A. Yen, « "La dépendance de l'Europe aux technologies américaines est un château de cartes sur le point de s'effondrer" », *Les Échos*, 24 février 2026.

La difficile implantation d'un modèle de certification européenne pour le cloud

En France, l'ANSSI a élaboré le label SecNumCloud 3.2, une qualification de sécurité renforcée attribuée aux fournisseurs qui respectent des normes très strictes. SecNumCloud exige notamment que le prestataire garantisse la confidentialité et la robustesse des données sensibles, et inclut un principe d'immunité vis-à-vis des lois étrangères. À ce jour, seize offres de prestataires de services informatiques en nuage sont certifiées par l'ANSSI. Le *cloud* hybride Bleu a obtenu en novembre le Jalon 1 de la certification par l'ANSSI, qui valide ainsi sa stratégie d'évaluation des services *cloud*. L'offre de *cloud* de confiance PREMI3NS de S3NS a également obtenu le Jalon 1 en mai 2025. Le recours à la certification de cybersécurité SecNumCloud est implicitement encadré par la loi visant à sécuriser et réguler l'espace numérique (SREN) de mai 2024. L'article 31 dispose que lorsque des systèmes ou applications traitent des données d'une sensibilité particulière dont l'accès illégal pourrait entraîner des troubles à l'ordre public (santé, fichier de justice, défense), l'État et ses opérateurs doivent s'assurer que les services *cloud* utilisés appliquent des garanties de sécurité empêchant tout accès non autorisé par des autorités publiques de pays tiers.

À l'échelle européenne, l'Agence pour la cybersécurité (ENISA) a développé le *European Cybersecurity Certification Scheme for Cloud Services* (EUCS), prévu par le *Cybersecurity Act* de 2019, pour harmoniser les niveaux de sécurité des services *cloud* à travers l'UE. L'EUCS définit plusieurs paliers de sécurité : basique, substantiel, élevé, etc. Alors que les négociations sont toujours en cours, les États membres peinent à s'accorder sur l'intégration d'une clause d'« immunité » dans l'EUCS (hébergement exclusif en UE, siège social et propriété européenne). La France, l'Italie, l'Espagne et l'Allemagne soutiennent l'inclusion de tels critères, tandis que d'autres États redoutent un effet protectionniste[84]. À ce jour, la Commission a amendé la proposition pour maintenir au niveau le plus élevé un critère de localisation et d'origine « européenne », mais la version finale de l'EUCS en cours de discussion ne comporte pas explicitement l'option d'« immunité légale » promise face à la portée extraterritoriale de certaines lois étrangères. La Commission nationale de l'informatique et des libertés (CNIL) souligne d'ailleurs que, dans le projet actuel, l'EUCS ne garantit pas la protection contre l'accès d'une puissance étrangère aux données stockées, contrairement à la certification française SecNumCloud[85]. Alors que des États et acteurs industriels appellent à parvenir à un consensus sur l'EUCS,

84. C. Bômont, « Technical Is Political: When a *Cloud* Certification Scheme Divides Europe », European Union Institute for Security Studies, 3 novembre 2025.
85. « Cloud : les risques d'une certification européenne permettant l'accès des autorités étrangères aux données sensibles », CNIL, 19 juillet 2024.

l'adoption rapide d'un référentiel commun avec le plus haut niveau d'exigence semble cruciale pour lever l'incertitude réglementaire[86].

Il convient de préciser que toutes les données n'exigent pas le même niveau de sécurité, ni le recours à un *cloud* certifié. En revanche, s'agissant des données critiques de l'État ainsi que les données de R&D ou les détails de production des entreprises, l'utilisation d'un *cloud* certifié « de confiance » garantit non seulement la localisation de l'hébergement des données dans l'UE, mais aussi le respect de normes strictes de chiffrement et de gestion des accès. Les traitements moins sensibles pourraient être confiés à des *clouds* publics classiques ou à des offres commerciales standards renforcées par des mesures techniques (chiffrement client, gestion des clés) ou contractuelles. Cette approche graduelle s'inscrit dans une stratégie *multicloud* où les charges de travail sont distribuées entre plusieurs environnements en fonction de leur sensibilité et des besoins métiers[87]. Par exemple, une administration nationale pourrait héberger ses bases de données classifiées sur un *cloud* certifié SecNumCloud, tout en exécutant ses applications bureautiques ou analytiques courantes sur des *clouds* publics (AWS, Google Cloud, Azure ou autre).

Les limites industrielles à la localisation des données en Europe

En dépit de la volonté de faire advenir un *cloud* européen, l'UE est aussi entravée par des faiblesses structurelles inhérentes à son mode d'organisation. L'Europe souffre d'abord d'un sous-investissement chronique et d'un manque de capitalisation suffisante pour faire face aux besoins massifs en capacité de calcul, en infrastructures de centres de données, en connectivité et en innovation dans l'IA et le *cloud* – investissements que les États-Unis et la Chine assument à grande échelle. En 2021, 7 % des investissements mondiaux en IA émanaient de l'UE, contre 40 % pour les États-Unis et 32 % pour la Chine[88]. En l'absence d'un instrument financier européen fort, à l'instar de l'« Union de l'épargne et de l'investissement » proposée par Enrico Letta dans son rapport *Much More Than a Market*[89], les initiatives européennes restent fragmentées, peu coordonnées et souvent moins performantes pour rivaliser avec les investissements des géants du numérique. Aussi est-il dans l'intérêt économique de la France et de l'UE d'élaborer une Union de l'épargne et de l'investissement, pour mettre à profit les quelque 33 000 milliards d'euros d'épargne privée.

86. C. Bômont, « Technical Is Political: When a *Cloud* Certification Scheme Divides Europe », *op. cit.*
87. A. Bittencourt, « EU Cloud Sovereignty – Four Alternatives to Public Clouds », Unit8, 9 juin 2025.
88. *La souveraineté technologique européenne et les infrastructures numériques*, Rapport du Parlement européen, 11 juin 2025.
89. E. Letta, *Much More Than a Market*, avril 2024, disponible sur : https://european-research-area.ec.europa.eu.

Par ailleurs, la coexistence d'une diversité d'acteurs de petite taille, souvent spécialisés dans des niches, ne suffit pas à créer les effets d'échelle nécessaires face aux *hyperscalers*. Le manque de ressources et les difficultés à offrir des services comparables à ceux des grandes plateformes sont autant de freins structurels à l'émergence d'acteurs européens véritablement compétitifs. Le recours massif des entreprises et administrations européennes aux services *cloud* américains s'explique logiquement par une convergence de facteurs économiques et techniques difficilement contestables. Les *hyperscalers* offrent en effet une combinaison stratégique d'avantages concurrentiels que les alternatives européennes peinent à égaler : fiabilité des infrastructures, robustesse, scalabilité quasi illimitée permettant d'absorber les pics de charge et diversité de services intégrés. À cela s'ajoutent l'interopérabilité avec l'écosystème logiciel dominant, majoritairement américain, et une expertise technique forte de plusieurs décennies d'innovation. Afin de lutter contre un tel effet de concentration, il est recommandé à la Commission européenne de procéder à la classification des fournisseurs de services *cloud* en tant qu'intermédiaires au titre du règlement sur les marchés numériques (DMA)[90]. Une telle mesure contribuerait à limiter des pratiques anticoncurrentielles telles que l'auto-préférence, l'exploitation des données des entreprises clientes à des fins concurrentielles et les conditions disproportionnées de résiliation de services qui empêchent la migration vers d'autres fournisseurs de services[91].

Des leviers d'action à la portée de l'Europe

Assurer la continuité des services numériques en cas d'interruption

Lors du sommet franco-allemand sur la souveraineté numérique, Microsoft a conclu un protocole d'accord avec l'entreprise de logiciels allemande SAP permettant à sa filiale Delos Cloud d'assurer le maintien des services Azure pour les clients européens frappés par d'éventuelles sanctions américaines. Cet accord, qui confère à Delos l'accès au code source de Microsoft, vise à garantir une continuité temporaire des services en cas d'interruption imposée par un gouvernement étranger. En France, Bleu, partenaire local de Microsoft également basé sur Azure, étudie actuellement la mise en œuvre d'un mécanisme similaire pour protéger les administrations et entreprises

90. La Commission européenne mène actuellement une enquête destinée à examiner la désignation d'Amazon et de Microsoft en tant que « contrôleurs d'accès ». En cas de qualification des géants du numérique, leurs services *cloud* pourront être réglementés par le DMA. Lire A. Datta, « Cloud : les géants américains Amazon et Microsoft font l'objet d'une enquête dans le cadre du DMA », Euractiv, 18 novembre 2025.

91. M. Nie et F. Tasin, « What the EU Needs to Do to Challenge Big Tech Cloud Dominance », *Tech Policy Press*, 19 juin 2025.

françaises contre de telles mesures de rétorsion[92]. L'Europe aurait donc intérêt à institutionnaliser et étendre la mise en œuvre de mécanismes de continuité de service. Des mesures contraignantes pourraient imposer aux fournisseurs de services *cloud* opérant sur le territoire européen de garantir l'accès au code source et assurer le transfert technique vers des opérateurs européens en cas de sanctions ou d'interruptions arbitraires des services numériques.

Garantir la résilience de nos infrastructures critiques

La question de la résilience de nos infrastructures critiques, tant en matière d'accès aux données que de puissance de calcul, doit donc être traitée par les gouvernements européens. L'UE gagnerait à accélérer massivement les investissements dans des infrastructures *cloud* souveraines dotées en capacités de stockage et de calcul pour assurer aussi bien la protection des données que l'innovation technologique, particulièrement en IA. Face aux risques liés à l'interruption des services numériques par un gouvernement étranger, il semble essentiel que l'Europe se munisse d'infrastructures résilientes, numériques mais aussi énergétiques – régulièrement ciblées par des cyberattaques sans lesquelles les infrastructures numériques ne peuvent fonctionner. Des solutions alternatives pourraient être étudiées afin de garantir la continuité des services de l'État. Ainsi, le développement d'infrastructures de stockage de données souveraines, improprement appelées « ambassades des données » (*Data Embassies*)[93], permettrait d'héberger dans un pays tiers de confiance, l'ensemble des données souveraines qui se rapportent à un État : données relatives aux citoyens, aux infrastructures critiques, à la défense et à la sécurité, à la santé, etc. Une ambassade des données assurerait la continuité de l'État en cas de crises majeures : cyberattaques d'ampleur, catastrophes naturelles affectant les infrastructures numériques ou énergétiques critiques, conflit armé ou menace grave à l'intégrité de l'État. Ce modèle est employé par l'Estonie, devenue en 2017 le premier pays à établir une ambassade des données, suivie par la Principauté de Monaco en 2021[94].

92. R. Fléchaux, « Microsoft contre le "kill switch" de Trump : SAP aujourd'hui, Bleu demain ? », CIO, 21 novembre 2025.
93. A.-Th. Norodom, « Numérique, entreprises et États : l'usurpation diplomatique », *Revue du droit public et de la science politique en France et à l'étranger*, 2025/3, p. 17-23.
94. Pour l'Estonie : « L'Estonie va protéger ses données dans une e-ambassade », *Les Échos*, 15 juillet 2017 ; pour Monaco : A. Gertaldi, « La première e-Ambassade de Monaco au Luxembourg », *Monaco Tribune*, 19 juillet 2021.

Diversifier les partenariats pour réduire nos dépendances

Enfin, l'Europe a tout intérêt à poursuivre sa politique numérique internationale en consolidant ses partenariats avec ses alliés. Une telle stratégie lui permettrait de réduire ses dépendances traditionnelles, de promouvoir des objectifs communs de souveraineté numérique, de diversifier l'accès aux ressources et de renforcer sa sécurité économique et numérique, tout en limitant sa dépendance vis-à-vis des États-Unis[95]. En témoignent les partenariats déjà établis avec le Japon, Singapour, la Corée du Sud et le Canada. Ainsi, le dernier accord numérique conclu avec la Corée du Sud en mars 2025 inclut des dispositions sur les flux de données et la protection des données personnelles[96]. L'UE œuvrerait ainsi à la diffusion de standards internationaux pour les infrastructures *cloud*, notamment en matière d'interopérabilité technique des systèmes et de portabilité des données (article 20 du RGPD)[97]. Dans ce cadre, l'Europe pourrait maintenir son influence dans les « affaires numériques mondiales », tout en luttant contre les pratiques monopolistiques et anticoncurrentielles des géants du numérique. Une telle dynamique pourrait même contribuer à la réactivation de son pouvoir normatif à l'échelle internationale, dans la lignée de l'« effet Bruxelles ».

95. C. Bômont, « Autonomy Is Not Autarky: But Is The EU's New Digital International Strategy's Focus on Partnerships Enough? », European Union Institute for Security Studies, 13 juin 2025.
96. K. Verhelst, « EU and Korea Seal Digital Trade Deal », *Politico*, 11 mars 2025.
97. V. Chhimpa, « How National AI Clouds Undermine Democracy », *Tech Policy Press*, 24 septembre 2025.

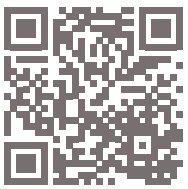
Conclusion

L'Europe cherche à garantir la sécurité des données (encadrement des transferts vers des pays tiers) au même titre que leur exploitation (circulation et mise en commun) pour stimuler l'innovation en intelligence artificielle. Ces objectifs, à la fois divergents et complémentaires, doivent être envisagés dans un contexte international incertain, qui impose de concilier les impératifs de sécurité nationale avec les exigences d'une compétition économique et technologique exaltée, justifiant l'élaboration d'une double stratégie sur les données. Face aux législations extraterritoriales qui s'imposent aux fournisseurs de services *cloud* extra-européens, une politique de maîtrise absolue des données se révèle structurellement inexécutable. Tant que l'Europe dépendra majoritairement d'*hyperscalers* soumis au *CLOUD Act* ou au FISA américain, aucune obligation de localisation, aussi ambitieuse soit-elle, ne pourra pleinement prémunir les données européennes contre des ingérences extérieures. Par conséquent, afin d'affirmer sa souveraineté dans le domaine du numérique et *a fortiori* sa souveraineté en matière de données, l'UE doit concrétiser son ambition d'autonomie stratégique dans le *cloud*. Cela implique de soutenir l'émergence de solutions européennes, de maîtriser au moins certains maillons de la chaîne de valeur technologique et d'harmoniser les politiques des États membres afin de permettre aux acteurs européens de « scale-up » à la hauteur des besoins industriels et publics.

Alors que la souveraineté numérique a été une fois de plus élevée au rang de priorité par le Conseil de l'UE en octobre 2025 dans ses conclusions sur les priorités pour la décennie numérique, une vision commune peine pourtant à advenir. Tandis que la France plaide en faveur « d'une forme inconditionnelle de souveraineté numérique », d'autres États cherchent à mieux délimiter la portée de certaines exigences en la matière[98]. Force est de constater que les obstacles à surmonter demeurent, tant sur le plan juridique que technique. D'une part, l'arsenal normatif européen, fût-il renforcé et simplifié pour stimuler l'innovation, se révèle impuissant face aux législations étrangères à portée extraterritoriale sur les données. D'autre part, la fragmentation du marché européen du *cloud*, l'insuffisance chronique d'investissements dans les infrastructures numériques souveraines et le retard technologique accumulé face aux géants américains constituent autant d'entraves à l'émergence d'une véritable alternative européenne crédible et compétitive.

98. A. Datta, « Cloud, IA : l'UE doit renforcer sa souveraineté, selon la ministre danoise du Numérique », Euractiv, 13 octobre 2025.

Dans ce contexte, l'urgence d'un sursaut européen s'impose, quoique les perspectives demeurent peu encourageantes : sans une volonté politique résolue, se traduisant par des investissements massifs et une coordination effective entre États membres, transcendant les intérêts nationaux divergents, l'Europe risque de voir son ambition de souveraineté numérique et d'autonomie stratégique se dissoudre dans les compromis diplomatiques. Le risque à terme pour le continent réside dans l'éventualité de demeurer un simple marché captif pour les puissances technologiques rivales. Espérons que l'Europe, forte de ses valeurs et de ses atouts industriels, saura mobiliser à temps les leviers d'action à sa portée.



27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org