COMMISSION

TECH

RAPPORT ANNUEL

Les Dépendances

Dépendances structurelles et souveraineté digitale : la France face à l'oligopole mondial du cloud

2025-2026

1ère édition

2025-2026

1ère édition

Remerciements

*“La **Commission Tech de Conversation Géo Eco** remercie chaleureusement les chercheurs, intégrateurs, fournisseurs de cloud français, européens et américains, ainsi que tous les professionnels et collègues interrogés tout au long de la rédaction du rapport pour leur confiance et leur temps.”*

Notre équipe

PERLE FAINAS

KING'S COLLEGE LONDON
Co-Présidente de Commission

OTERIA CYBER SCHOOL
Co-Président de Commission

ADAM BERNARD

MAXIM HADADA

ESCP BUSINESS SCHOOL
Membre

PSIA SCIENCES PO PARIS
Chargée de veille

CAROLINE MARQUES

VALENTINE SCHMITZ

MAASTRICHT UNIVERSITY
Membre

KONSTANZ UNIVERSITÄT -
UTRECHT UNIVERSITY
Membre

MAXIME PLANTET

MAXIME GILLET DEVIN

UNIVERSITÉ DE POITIERS
Membre

Contact :
commissiontech@conversationgeoeco.com

2025-2026

1ère édition

Table des matières

Introduction

« *On a besoin, si on veut une plus grande souveraineté européenne, de protéger d'abord nos données. C'est pour ça qu'on soutient un agenda commun, justement, de préservation de nos données en Europe et de protection à l'égard des lois extraterritoriales ou de ce qui peut les menacer. Donc la certification de la cybersécurité pour les services de cloud est à cet égard un agenda très important et une initiative importante à venir.* »

Emmanuel Macron le 18 novembre 2025 au Sommet sur la souveraineté numérique européenne à Berlin[1].

Dans cette déclaration, le président souligne le besoin de se libérer des dépendances technologiques à tous les niveaux des chaînes de valeur dans le but d'atteindre une réelle souveraineté européenne, y compris en passant par le niveau du cloud.

Bien que le sujet de l'élaboration d'un cloud souverain européen soit loin d'être récent, l'accroissement de la demande de services cloud sur les dernières années – due notamment à la crise sanitaire qui a développé le digital dans les entreprises et la mutation technologique et sociétale – a remis le sujet au sein du débat public. Utiliser des services *clouds* concède de nombreux avantages, comme une flexibilité accrue ou la possibilité de s'affranchir d'une infrastructure coûteuse.[2] Cependant, malgré l'usage massif de ces technologies, leur mise en œuvre reste réservée à un cercle restreint d'acteurs.

Ce marché oligopolistique, dominé par des acteurs principalement américains ou "***hyperscalers***", expose la France à des risques multiples : risques juridiques liés à l'application extraterritoriale de législations étrangères, risques opérationnels en cas de rupture d'accès aux services, et risques stratégiques touchant à la confidentialité des données sensibles des administrations, des entreprises et des citoyens européens. Cette concentration du marché cloud entre les mains d'acteurs non-européens n'est pas sans conséquences sur la capacité des États à exercer pleinement leur **souveraineté numérique**, entendue ici comme la "*capacité de l'État à*

[1] Discours du Président de la République à l'occasion du Sommet sur la souveraineté numérique européenne, 18 novembre 2025
[2] Dominique Luzeaux, *Cloud souverain : souveraineté et résilience, ou confiance ?* Revue Défense Nationale, N° 855(10), pp.14–21, 2022

agir dans le cyberespace"[3], à le réguler et à peser sur l'économie numérique.[4]

Dans ce contexte, la question du cloud souverain apparaît comme un **enjeu structurant pour la politique industrielle et numérique, au niveau français ou européen.** Alors que les infrastructures cloud deviennent un support essentiel du fonctionnement de l'économie de la donnée, la dépendance aux fournisseurs technologiques étrangers soulève de nombreuses questions quant à la capacité de la France et de l'Union européenne à garantir la protection de ses infrastructures numériques et données stratégiques. De ce fait, ce rapport produira un état des lieux des **dépendances** auxquelles la France fait face aujourd'hui, ainsi que l'efficacité des solutions apportées. Puis, dans un second temps, se penchera sur les possibilités pour un cloud souverain ou de confiance pour renforcer la souveraineté digitale et l'autonomie de la France au vu de ces dépendances.

Nous entendrons dans ce rapport par **dépendance**, toute situation dans laquelle un acteur, public ou privé, se trouve dans l'incapacité de substituer, dans un délai raisonnable et sans coût disproportionné de sortie, un fournisseur ou une technologie par une alternative fonctionnellement équivalente respectant le droit européen. Cette définition s'appuie notamment sur les travaux de la Commission d'enquête sénatoriale sur le devoir de souveraineté numérique, qui soulignent la nécessité de "*conserver une capacité autonome d'appréciation, de décision et d'action pour l'État dans le cyberespace*" et de "*garantir une "autonomie informationnelle" suffisante à nos concitoyens de plus en plus dépendants d'intermédiaires techniques au fonctionnement souvent opaque*".[5] Pensée de manière multidimensionnelle, cette dépendance s'apparente à un système d'enfermement qui s'auto-entretient à tous les niveaux, et non à un simple problème technique à résoudre couche par couche. De ce fait, sa compréhension exige une lecture transversale, que notre première partie illustre.

Le chapitre 1 cartographie les dépendances technologiques, qui s'exercent dans les couches profondes de l'infrastructure même du cloud, depuis la privatisation des standards et la domination des câbles sous-marins, jusqu'au matériel propriétaire et au verrouillage par les services PaaS. Des

[3] Gérard Longuet, *Le devoir de souveraineté numérique*, Rapport n° 7 de la Commission d'enquête du Sénat, 1er octobre 2019, avant-propos.
[4] Martin Untersinger, « *L'incertaine mais nécessaire « souveraineté numérique* » [archive] », Le Monde, 20 novembre 2019.
[5] Gérard Longuet, *Le devoir de souveraineté numérique*, Rapport n° 7 de la Commission d'enquête du Sénat, 1er octobre 2019, avant-propos.

dépendances souvent invisibles car présentées comme de simples choix techniques, mais qui constituent en réalité des barrières structurelles à la sortie. Dans un second temps, le chapitre 2 analysera quant à lui les dépendances industrielles et financières, d'une part via la concentration du marché du cloud et ses mécanismes de verrouillage, ainsi que l'asymétrie des capacités d'investissement entre *hyperscalers* américains et acteurs européens. Cette partie analysera également les modèles hybrides tels que Bleu et S3NS, et la possibilité réelle qu'ils représentent dans l'achèvement d'une véritable souveraineté industrielle. Finalement, le chapitre 3 examine les dépendances juridiques et extra territoriales, en exposant que l'extraterritorialité juridique d'autres pays peut permettre un accès aux données européennes malgré le RGPD, révélant une asymétrie juridique structurelle. Se basant sur cette cartographie, la deuxième partie analyse les stratégies françaises et européennes visant à répondre à ces dépendances, en évaluant leur portée réelle face aux dynamiques industrielles, technologiques et juridiques identifiées. La troisième partie met ensuite en lumière les vulnérabilités critiques qui en découlent pour les acteurs publics et stratégiques. Enfin, une dernière partie formulera des recommandations opérationnelles visant à renforcer concrètement la souveraineté numérique.

Ce document s'adresse aux décideurs publics ainsi qu'aux acteurs privés dans toute leur diversité : entreprises clientes de services cloud ainsi qu'aux fournisseurs eux-mêmes, dont les choix techniques et de positionnement marché participent directement à la configuration du paysage souverain français et européen. En tant que *think tank* étudiant indépendant, nous avons choisi la voie de la pluridisciplinarité dans le but d'engager de nouvelles conversations entre secteur public et privé ainsi qu'entre fournisseurs et utilisateurs de cloud. Cette méthode nous a menés à auditionner plusieurs experts du milieu, employés, chercheurs ou eurodéputés. Ce rapport a ainsi pour ambition de produire une analyse rigoureuse accessible à ces audiences simultanément, pour des objectifs à court, moyen et long terme.

PARTIE I

Cartographie des dépendances structurelles du cloud français

I. Chapitre 1 : Dépendances Technologiques

L'analyse de la souveraineté numérique est trop souvent réduite à une dimension juridique ou géographique, se focalisant quasi exclusivement sur la localisation des données et la conformité réglementaire. Cette approche, bien que nécessaire, constitue une erreur stratégique qui masque la réalité des rapports de force. C'est précisément l'argument central de ce rapport : **la véritable dépendance de l'écosystème français ne réside pas uniquement dans le stockage de la donnée, mais aussi dans les couches technologiques profondes qui permettent de la traiter, de la transporter et de la valoriser.**

L'examen technique de l'offre des "*Hyperscalers*" américains : Amazon Web Services, Microsoft Azure, Google Cloud, révèle une stratégie de verrouillage systémique. Cette stratégie n'est pas une simple conséquence de leur excellence opérationnelle, mais une architecture délibérément conçue pour **rendre le coût de la réversibilité prohibitive** et maintenir les clients dans un état de **captivité technologique durable**. Ce chapitre s'attache donc à déconstruire, couche par couche, les mécanismes de cette dépendance, depuis l'abstraction logicielle jusqu'à la physique des câbles sous-marins. Pour bien appréhender cette architecture, il convient de rappeler les définitions du NIST, reprises par l'Autorité de la concurrence, qui divisent le cloud en trois grandes catégories : l'IaaS (*Infrastructure as a Service*) pour la mise à disposition de ressources informatiques brutes, le PaaS (*Platform as a Service*) pour la fourniture d'environnements de développement, de bases de données et d'outils analytiques, et le SaaS (*Software as a Service*) pour les logiciels entièrement gérés.

A. Dépendance aux hyperscalers

Pour rappel, le terme d'*hyperscalers* désigne les géants technologiques qui opèrent des infrastructures cloud mondiales, capables de faire évoluer massivement leurs ressources digitales et de dicter, par la force de leurs investissements capitalistiques, les standards de l'industrie.

L'écosystème numérique français, en partant des administrations publiques centrales jusqu'aux startups incubées à Station F, s'est progressivement construit "en surcouche" des infrastructures américaines. Cette posture place donc la France dans une situation de **"souveraineté déléguée"** : nous

conservons la maîtrise apparente de la couche applicative, mais nous avons perdu le contrôle des fondations.

1. La perte de maîtrise des standards et la "Norme de Fait"

Historiquement, l'industrie informatique s'est développée sur des cycles de standardisation ouverts, pilotés par des organismes internationaux tels que l'ISO (Organisation internationale de normalisation) ou l'IETF (*Internet Engineering Task Force*). Ces instances garantissaient une interopérabilité fondamentale, en s'appuyant sur des protocoles ouverts et documentés, ce qui permettait à des acteurs hétérogènes de communiquer librement sans risque d'enfermement propriétaire.

Cependant, depuis plusieurs années, les normes qui régissent l'économie digitale mondiale sont désormais, en partie, décidées unilatéralement dans les bureaux de Seattle et de Mountain View. Cette privatisation de la norme entraîne des conséquences opérationnelles directes. Lorsque Amazon décide de modifier l'architecture de ses instances de calcul, de déprécier une version de son API S3 ou de changer ses protocoles de chiffrement, l'ensemble de l'industrie française du logiciel est contraint de s'aligner.

Cette dépendance se traduit par une **"dette technique subie"**. Les grands intégrateurs français comme Capgemini ou Atos, ainsi que les Directions des Systèmes d'Information (DSI) des grandes entreprises françaises et Européennes, doivent allouer une part croissante de leurs ressources non pas à l'innovation, mais au maintien en condition opérationnelle (MCO) pour suivre le rythme imposé par les *hyperscalers*. **La roadmap technologique de la France n'est donc plus décidée à Paris, mais dictée par les cycles de produits américains.**

2. Le "*Lock-in*" des compétences et la dépendance au sentier

Une dépendance plus insidieuse, car humaine et culturelle, s'est installée : celle des compétences. La complexité croissante des environnements cloud, couplée à une pénurie mondiale de talents, a transformé la formation en vecteur de domination.

Les *hyperscalers* ont déployé des programmes massifs de certification tels que AWS Solutions Architect, Microsoft Certified, Azure Administrator, Google Cloud Professional, qui sont devenus les standards de recrutement. Les écoles d'ingénieurs françaises et les organismes de formation continue,

pour assurer l'employabilité de leurs étudiants, ont intégré ces cursus propriétaires au détriment des technologies ouvertes ou souveraines.

Notre système éducatif forme ainsi une génération d'architectes **culturellement et techniquement incapables de penser en dehors des écosystèmes américains.** Ce phénomène crée une “*path dependence*”. Lorsqu'un architecte certifié AWS doit concevoir une nouvelle infrastructure critique, il privilégiera naturellement les briques qu'il maîtrise, percevant les alternatives européennes comme risquées ou nécessitant un réapprentissage coûteux. Ce **verrouillage cognitif** sécurise les parts de marché des acteurs américains pour les décennies à venir, indépendamment de la qualité intrinsèque des offres concurrentes.

B. *Lock-in* technologiques & briques critiques

Le verrouillage technologique n'est pas un accident ; c'est le modèle économique même du cloud public. Il s'opère par une stratégie de **"capture des briques critiques"** qui s'étend de l'infrastructure physique la plus tangible jusqu'aux couches logicielles les plus abstraites.

1. La conquête de l'infrastructure physique : Câbles et Connectivité

Contrairement à l'imaginaire d'un cloud "immatériel" flottant, la domination des *hyperscalers* repose sur une mainmise physique de l'infrastructure mondiale :

Historiquement, les câbles sous-marins, par lesquels transitent 99 % du trafic intercontinental, étaient financés et opérés par des consortiums d'opérateurs télécoms nationaux (Orange, Tata Communications, AT&T). Ce modèle de consortium garantissait une forme de neutralité du réseau et de réciprocité. Ce paradigme s'est toutefois effondré au cours de la dernière décennie, sous le double effet de l'explosion du trafic entre les centres de données et de la force de frappe capitalistique écrasante des géants de la technologie.

En 2025, les GAFAM **contrôlent désormais environ 71 % de la capacité mondiale de fibre optique sous-marine. Sur certaines routes stratégiques, telles que la liaison transatlantique, cette domination**

dépasse les 90 %[6]. Les opérateurs historiques sont relégués au rang de clients ou de partenaires minoritaires pour la maintenance ("*wet plant*"). L'exemple du projet "*Waterworth*", annoncé par Meta en février 2025, illustre cette nouvelle géopolitique des câbles. Un câble de 50 000 km, potentiellement le plus long au monde, reliant les États-Unis, l'Inde et le Brésil.

Contrairement aux câbles traditionnels qui passent par les goulots d'étranglement géopolitiques (Canal de Suez, Mer Rouge, Mer de Chine méridionale), Waterworth adopte une stratégie de contournement "Sud-Sud" pour éviter les zones de conflit et de sabotage (houthistes en Mer Rouge, tensions sino-américaines). Conséquences pour l'Europe : Ce câble opère en circuit fermé pour les besoins propres de Meta. En reliant directement les USA aux marchés émergents sans passer par les hubs européens traditionnels, il contribue à faire de l'Europe une **"périphérie connectée"** plutôt qu'un nœud central. L'Europe perd sa centralité dans le routage mondial de l'information.[7]

2. Le verrou du Silicium

La standardisation autour de l'architecture x86 (Intel/AMD) a longtemps permis une portabilité théorique des applications : un code compilé pour un serveur Intel chez AWS pouvait théoriquement tourner sur un serveur Intel chez OVHcloud. Cette ère s'achève peu à peu avec l'avènement du **"Custom Silicon"**. Les *hyperscalers* conçoivent désormais leurs propres puces pour optimiser les coûts et créer une différenciation propriétaire.

Cette stratégie d'intégration verticale provoque une fragmentation accélérée du marché, chaque *hyperscaler* imposant désormais ses propres composants spécialisés :

[6]Pearson, Sasha (pour l'ECDPM), *Troubled waters: Europe's subsea telecommunications network*, 18 mars 2026.
https://ecdpm.org/work/troubled-waters-europes-subsea-telecommunications-network
[7]University of Oxford, *Expert comment: What does Meta's undersea cable plan mean for geopolitics*, 10 mars 2025.
https://www.ox.ac.uk/news/2025-03-10-expert-comment-what-does-meta-s-undersea-cable-plan-mean-geopolitics

- AWS : Les processeurs Graviton en sont à leur quatrième génération. En 2025, AWS indique que plus de 50% de ses nouvelles instances EC2 reposent sur ces puces propriétaires.[8]

- Google Cloud : Déploie massivement ses puces Axion et ses TPU (*Tensor Processing Units*) pour l'IA, créant un écosystème matériel verticalement intégré.

- Microsoft Azure : A lancé ses puces Azure Maia (accélérateur IA) et Cobalt (CPU) pour réduire sa dépendance à Nvidia et Intel.

Le piège est économique avant d'être technique. Ces puces offrent un rapport performance/prix imbattable : jusqu'à -40% de coût pour le client[9] par rapport aux instances x86 classiques. Les Direction des Systèmes d'Information français, sous pression budgétaire, sont donc incités à migrer leurs charges de travail vers des alternatives comme Graviton ou Axion.

Cependant, une fois le code optimisé et compilé pour les jeux d'instructions spécifiques d'un processeur Graviton ou pour l'architecture matricielle d'un *Tensor Processing Unit*, la migration vers un cloud souverain devient extrêmement complexe, voire financièrement rédhibitoire. En effet, n'ayant pas ou peu accès à ces composants propriétaires, les acteurs européens comme OVH cloud ou Scaleway utilisent majoritairement des standards de marché.

Dès lors, migrer une application "Graviton-native" vers une architecture standard implique une perte de performance massive ou une réécriture complète du code. Ce mécanisme constitue en réalité **la réinvention du verrouillage matériel à l'ère du cloud.**

[8]Network World, Graviton progress: 50% of new AWS instances run on Amazon custom silicon, 2 janvier 2025. https://www.networkworld.com/article/3631134/graviton-progress-50-of-new-aws-instances-run-on-amazon-custom-silicon.html
[9] Amazon Web Services (AWS), Amazon EC2 Graviton : Mise en route, Documentation technique continue. https://aws.amazon.com/fr/ec2/graviton/getting-started/

3. Le piège du PaaS et les barrières douanières

Si l'IaaS (Infrastructure brute) est commoditisée, **la véritable capture de valeur se fait sur le PaaS (*Platform as a Service*) et la donnée.** L'utilisation de services de bases de données propriétaires comme Amazon DynamoDB, Google BigQuery ou Azure Cosmos DB crée une dépendance technique absolue.

Ces services n'ont pas d'équivalent standard direct. Contrairement à une base de données SQL standard (PostgreSQL, MySQL) qui peut être exportée et réimportée ailleurs, une application construite sur DynamoDB utilise des API et des logiques de données propriétaires. En sortir ne demande pas un simple transfert de données, mais une réécriture de l'application.

De plus, les *hyperscalers* ont érigé une barrière douanière privée : les frais de sortie : Egress Fees. Il s'agit de facturer le transfert de données sortant du cloud vers Internet ou vers un concurrent à des tarifs prohibitifs, souvent 80 fois supérieurs au coût réel de la bande passante.[10]

L'année 2025 a marqué un tournant régulatoire sur ce sujet. L'Arcep, dans sa décision n° 2025-0340 du 20 février 2025, a pris une position forte en proposant un plafond tarifaire à 0 € pour les frais de transfert de données liés au changement de fournisseur.[11] Cette décision anticipe l'interdiction totale prévue par le Data Act européen pour janvier 2027. Néanmoins, la friction demeure. Pour les contrats en cours et les volumes massifs, la facture de sortie reste un dissuasif puissant.

Le cloud fonctionne comme un péage asymétrique : on peut faire entrer ses données gratuitement, mais on ne peut jamais vraiment les faire sortir sans payer.

[10] Prince, Matthew (Pour Cloudflare), AWS's Egregious Egress, 23 juillet 2021. https://blog.cloudflare.com/aws-egregious-egress/

[11] Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep), Décision n° 2025-0340, 20 février 2025. https://www.arcep.fr/uploads/tx_gsavis/25-0340.pdf

TABLEAU 1

Comparatif des barrières financières à la sortie[12]

Fournisseur	Politique Egress Fees	Franchise (Free Tier)	Coût estimé pour 100 To	Impact Stratégique
AWS	Élevés	100 Go/mois	~9 000 $	Barrière Bloquante
Microsoft Azure	Élevés	100 Go/mois	~8 700 $	Barrière Bloquante
Google Cloud	Élevés	200 Go/mois	~8 500 $	Barrière Bloquante
Oracle Cloud	Modérés	10 To/mois	~765 $	Friction Moyenne
OVHcloud	Gratuit / Illimité	Illimité	0 €	Fluidité Totale
Scaleway	Gratuit / Illimité	Illimité	0 €	Fluidité Totale

Source : Holori, Egress costs: Comparison between main cloud providers, 3 octobre 2024[13].

Si les couches d'infrastructure et de données font d'ores et déjà l'objet d'un verrouillage systémique redoutable, l'accélération fulgurante des modèles d'intelligence artificielle menace aujourd'hui de transformer cette dépendance en une véritable impasse stratégique.

[12]Holori, Egress costs: Comparison between main cloud providers, 3 octobre 2024. https://holori.com/egress-costs-comparison/
[13] https://holori.com/egress-costs-comparison/

C. Le mur technologique de l'Intelligence Artificielle

L'avènement de l'IA générative en 2024-2025 a agi comme un accélérateur de dépendance, créant une **barrière technologique infranchissable** pour les acteurs conventionnels.

1. La "*Cudification*" et la pénurie organisée de GPU

Si l'intelligence artificielle est souvent perçue comme une bataille d'algorithmes et de données, elle repose en réalité sur une infrastructure industrielle d'une intensité physique sans précédent. La souveraineté en IA ne se joue pas seulement dans les lignes de code des modèles, mais dans la capacité à accéder à la puissance brute de calcul nécessaire pour les entraîner. Cette dépendance s'articule autour d'un double verrou, à la fois matériel et logiciel, dont le centre de gravité se trouve aux mains d'un seul acteur : Nvidia.

La dépendance en IA remonte à la chaîne de production du calcul. L'écosystème logiciel de l'IA (PyTorch, TensorFlow) est massivement optimisé pour la plateforme CUDA de Nvidia. **C'est la *"Cudification"* de l'industrie :** CUDA n'est pas qu'une simple surcouche, c'est un modèle de programmation propriétaire développé par Nvidia qui permet d'exploiter la puissance de calcul parallèle de ses cartes graphiques. L'écrasante majorité des bibliothèques d'IA et des projets de recherche mondiaux ayant été codés pour interagir exclusivement avec ce langage, le logiciel se retrouve intimement verrouillé au matériel Nvidia.

Par conséquent, faire tourner ces modèles sur des puces de concepteurs concurrents, comme AMD, Intel, ou d'éventuelles alternatives européennes, nécessite une traduction ou une réécriture du code extrêmement complexe.

Ce monopole de fait, empêche l'émergence d'une infrastructure d'IA souveraine, l'accès à la puissance de calcul étant conditionné par l'allégeance à un seul acteur américain. Or, les *hyperscalers* américains ont sécurisé, via des accords massifs et des préfinancements, la quasi-totalité de la production de GPU de dernière génération.

Des acteurs européens tentent de réagir : par exemple, Scaleway a annoncé fin 2025 la disponibilité des premiers clusters européens de GPU Nvidia

Blackwell Ultra, poursuivant ainsi ses investissements initiés avec le lancement de son supercalculateur "*Nabuchodonosor*".[14]

Cependant, le différentiel d'échelle reste écrasant. Les acteurs français du "Tier 2" doivent se battre pour des allocations de quelques centaines de cartes quand Meta ou Microsoft en commandent des centaines de milliers. Les délais de livraison pour les acteurs européens atteignent souvent 12 à 18 mois, les rendant structurellement incapables de rivaliser sur l'offre d'entraînement de grands modèles de langage (LLM) en temps réel.[15]
Ainsi, la maîtrise éventuelle des algorithmes par l'Europe restera vaine et illusoire tant que le socle matériel nécessaire à leur entraînement sera soumis aux capacités d'approvisionnement et au calendrier dictés par les géants américains.

2. L'abstraction par l'API : La perte de savoir-faire

Les services d'IA "clés en main", qui masquent la complexité de l'entraînement et du déploiement des modèles derrière de simples appels réseau (API OpenAI sur Azure, Vertex AI sur Google), constituent un piège de facilité.

En les utilisant, les startups françaises d'IA s'épargnent la gestion complexe de l'infrastructure GPU, mais elles lient le destin de leur produit à un tiers américain.

L'exemple de Mistral AI, champion français de l'IA, est révélateur de cette ambiguïté. Bien que prônant l'*open-weight*, Mistral a signé un partenariat stratégique pluriannuel avec Microsoft en février 2024. Ses modèles les plus performants sont disponibles en priorité sur l'infrastructure Azure AI Studio via des API managées.

Cette stratégie, pragmatique pour le scale-up de Mistral, illustre l'illusion de la "souveraineté de l'IA" : même nos champions applicatifs dépendent in fine de la puissance de calcul sous pavillon américain pour l'entraînement et l'inférence à grande échelle. **La valeur ajoutée se déplace du modèle vers l'infrastructure qui le fait tourner, et cette infrastructure est américaine.**

[14] Scaleway, offre de son supercalculateur dédié à l'IA, Nabuchodonosor, basé sur l'infrastructure NVIDIA DGX H100, 5 octobre 2023.
https://www.scaleway.com/fr/news/scaleway-detaille-loffre-de-son-supercalculateur-dedie-a-lia-nabuchodonosor-base-sur-linfrastructure-nvidia-dgx-h100/
[15] GPU Loans, AI GPU Financing 2026: Data Center Guide, 2026.
https://www.gpuloans.com/blog/ai-gpu-financing-2026-data-center-guide

3. Mécanisme de la boucle fermée

Pour verrouiller définitivement ces champions de l'IA sur leurs infrastructures, les *hyperscalers* déploient une ingénierie financière d'une redoutable efficacité. Le modèle fonctionne de manière circulaire en trois temps. Tout d'abord, lors de la phase d'investissement, un *hyperscaler* injecte massivement des fonds et des crédits cloud dans une startup d'IA de premier plan.

Ensuite, par un engagement de réciprocité, la startup s'oblige contractuellement à utiliser exclusivement ou prioritairement l'infrastructure de l'investisseur pour l'entraînement et l'inférence de ses modèles.

Enfin, par un mécanisme de reconnaissance de revenu, l'argent initialement investi revient à l'*hyperscaler* sous la forme de facturations d'infrastructure, "*Cloud Revenue*", ce qui permet de gonfler artificiellement la croissance de sa propre division cloud.

Ces mécanismes de vases communicants financiers et technologiques se matérialisent aujourd'hui par des alliances structurantes qui redessinent le marché. Trois exemples majeurs illustrent cette dynamique :

- Microsoft & OpenAI : Microsoft a investi plus de 13 milliards de dollars dans OpenAI. En retour, OpenAI utilise principalement Azure. Une grande partie de cet investissement est versée en crédits Azure, ce qui s'apparente à un véritable aller-retour financier : l'argent sort des coffres de Microsoft sous forme d'investissement, pour y retourner presque aussitôt sous forme de factures d'hébergement. **Les revenus** générés par l'utilisation massive de GPU par OpenAI **sont ainsi comptabilisés dans le chiffre d'affaires d'Azure, rassurant les investisseurs boursiers sur la croissance de l'IA.**

- Amazon & Anthropic : Amazon a investi 4 milliards de dollars dans Anthropic. En contrepartie, Anthropic a désigné AWS comme son fournisseur cloud principal et s'est engagé à utiliser les puces Trainium et Inferentia pour ses futurs modèles.

- Google & Anthropic : Google a également investi 2 milliards de dollars dans Anthropic, sécurisant un engagement d'utilisation de ses TPU et de Google Cloud

Cette pratique rappelle dangereusement les "échanges de capacité" qui avaient gonflé la bulle des télécoms au début des années 2000. La FTC, examine désormais si ces partenariats constituent des acquisitions déguisées échappant au contrôle des fusions, et s'ils faussent la concurrence en privant les autres acteurs d'accès aux modèles de pointe.[16]
Le constat qui découlera de cette enquête est critique pour l'Europe : il confirme que nos acteurs ne luttent pas seulement contre une avance technologique américaine, mais contre **une architecture de marché dont les dés sont financièrement trafiqués.**
Face à un tel oligopole capable de verrouiller l'intégralité de la chaîne de valeur par des milliards de dollars captifs, l'idée de s'en remettre aux seules forces du marché pour faire émerger une IA ou un cloud souverain relève désormais de l'utopie. De plus, des critiques s'élèvent sur la transparence comptable (normes ASC 606 aux Etats-Unis).

Si une part significative de la croissance du cloud provient de l'argent que les *hyperscalers* se versent indirectement à eux-mêmes via des startups déficitaires, la santé réelle du marché pourrait être surestimée. Si la bulle de l'IA éclate et que ces startups ne parviennent pas à monétiser leurs services, les *hyperscalers* se retrouveront avec des infrastructures GPU dépréciées et des revenus fantômes.

[16]Federal Trade Commission (FTC), FTC Launches Inquiry into Generative AI Investments and Partnerships, 25 janvier 2024.
https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-launches-inquiry-generative-ai-investments-partnerships

À RETENIR

Dépendances Technologiques

- En définitive, la cartographie de nos dépendances révèle que la perte de souveraineté numérique française et européenne dépasse largement la simple question de la localisation des serveurs ou de l'extraterritorialité du droit américain. **Elle est profondément structurelle et s'exerce avec une redoutable efficacité à chaque strate de la chaîne de valeur**.

- Au niveau de l'infrastructure physique, l'Europe risque la relégation au rang de **"périphérie connectée"** face aux nouvelles routes sous-marines privées des géants du net.

- Plus haut dans la pile, **l'avènement des puces propriétaires réinvente le verrouillage matériel,** rendant toute réversibilité technologiquement ardue.

- Cette captation se poursuit au niveau de la donnée, où **l'adoption massive des services PaaS propriétaires et la persistance des barrières douanières privées transforment le cloud en un péage asymétrique** où la donnée entre librement mais ne ressort qu'au prix fort.

- Enfin, l'explosion de **l'intelligence artificielle** a parachevé ce maillage de dépendances.

- De la "Cudification" des algorithmes à la pénurie organisée de la puissance de calcul, en passant par les mécanismes d'aller-retour financier qui lient le destin de nos champions applicatifs aux infrastructures cloud américaines, le marché est aujourd'hui verrouillé par un oligopole aux ressources virtuellement illimitées. Les *hyperscalers* ont ainsi transformé leur avance technologique originelle en **barrières à l'entrée et à la sortie difficilement franchissables.**

- Face à ce constat, briser cette dépendance au sentier ne pourra se satisfaire d'une simple posture défensive ou d'ajustements réglementaires ciblés. Cela exigera une **volonté politique et industrielle inédite pour repenser l'innovation souveraine non plus comme une simple surcouche applicative, mais depuis les fondations mêmes de l'infrastructure.**

II. Chapitre 2 : Dépendances industrielles et financières

L'analyse de la souveraineté numérique française et européenne s'inscrit fondamentalement dans une réalité industrielle et financière asymétrique. La dépendance de la France à l'égard des fournisseurs de services cloud extra-européens, repose sur une architecture économique minutieusement construite : un marché oligopolistique verrouillé par des **barrières à l'entrée colossales, des pratiques tarifaires de rétention, et soutenu par des capacités d'investissement financier (CapEx) hors d'atteinte pour les acteurs locaux.** Les conséquences de cette asymétrie dépassent le simple cadre concurrentiel pour se traduire en un transfert massif de valeur au détriment de l'économie européenne.

Face à ce constat, l'émergence récente de modèles d'hybridation, associant des capitaux et des infrastructures de télécommunications français à des licences technologiques américaines, illustre parfaitement la tension inhérente à la stratégie nationale. Ces partenariats de "cloud de confiance" – à différencier du "cloud souverain" – tentent de concilier le besoin immédiat de conformité sécuritaire avec **le renoncement, au moins partiel, à une autonomie industrielle complète.** Ce chapitre déconstruit de manière exhaustive les mécanismes de cette dépendance industrielle et financière, en examinant la concentration du marché, le gouffre des dépenses d'investissement creusé par la révolution de l'intelligence artificielle, et les limites économiques intrinsèques des nouveaux consortiums hybrides.

A. La concentration du marché et ses mécanismes de verrouillage

Le marché européen et français du cloud se caractérise par une asymétrie profonde entre une demande en croissance exponentielle et une offre dominée par une poignée d'acteurs oligopolistiques.

L'Autorité de la concurrence française, dans ses avis successifs de juin 2023 (Avis 23-A-08) et de juin 2024 (Avis 24-A-05), a formellement qualifié cet environnement de complexe, hautement concentré et porteur de risques

majeurs pour la compétition économique et l'innovation.[17] La dynamique de ce marché s'explique par des effets de réseau massifs, des économies d'échelle inaccessibles aux nouveaux entrants, et des pratiques tarifaires conçues pour maximiser la captation de la clientèle tout en rendant toute migration ultérieure prohibitive.

1. L'état des lieux d'un marché accaparé par les hyperscalers

La croissance du marché mondial et européen du cloud est fulgurante, portée par la numérisation des processus métiers, le stockage massif de données et, plus récemment, par les exigences infrastructurelles de l'intelligence artificielle générative. Sur le plan mondial, le marché des infrastructures en tant que service (IaaS) a enregistré une croissance de 22,5 % en 2024 pour atteindre près de 171,8 milliards de dollars.[18] En élargissant le périmètre à l'ensemble des services d'infrastructure cloud, les dépenses mondiales ont dépassé pour la première fois le cap des 400 milliards de dollars sur l'année complète 2025, avec un taux de croissance trimestriel s'accélérant continuellement.[19]

Pour le seul marché européen, les prévisions de Synergy Research Group estiment que les revenus liés à l'infrastructure cloud, incluant l'IaaS, le PaaS et le cloud privé hébergé, dépasseront les 75.6 milliards d'euros en 2025, affichant une croissance annuelle de 24 % par rapport à 2024. L'Allemagne, le Royaume-Uni, et la France demeurent les principales destinations de ces investissements en Europe.[20]

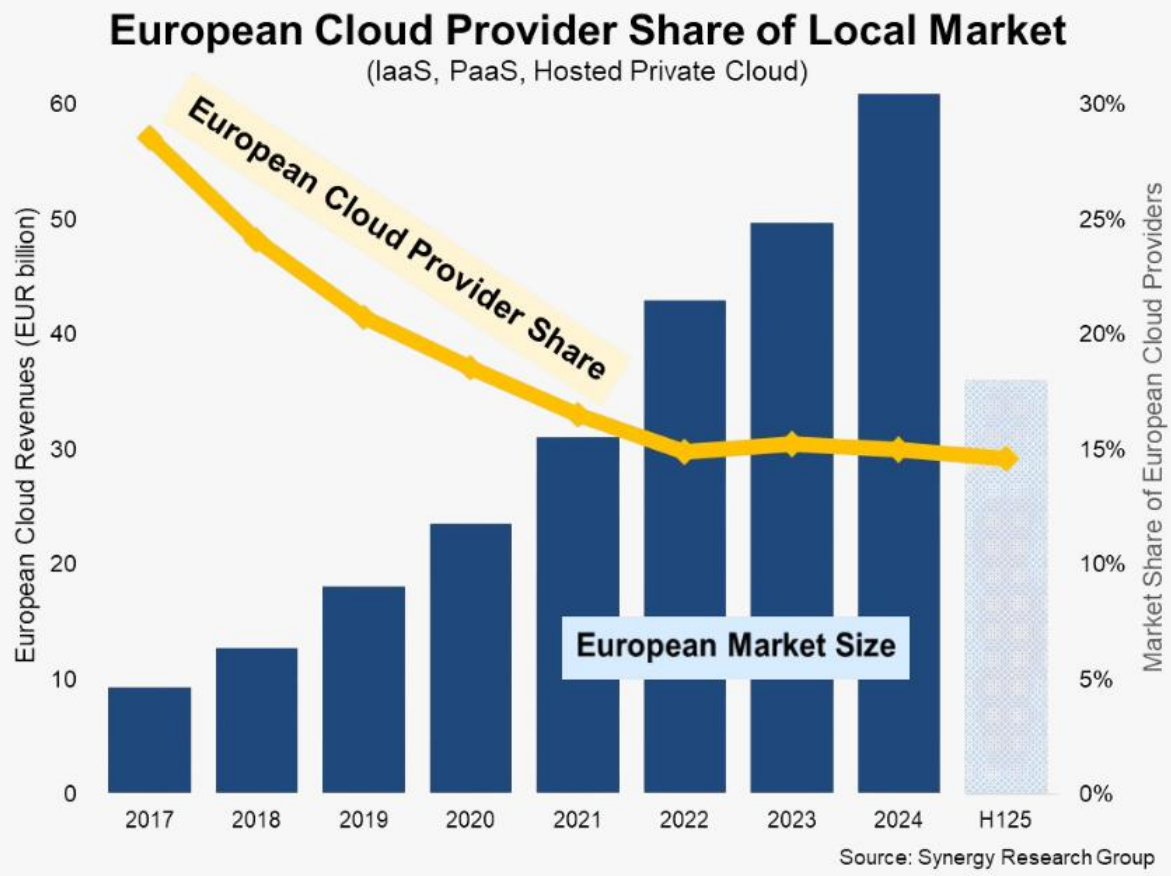
Toutefois, cette immense création de valeur ne profite que marginalement aux industriels européens. Les données consolidées démontrent que trois acteurs américains : Amazon Web Services, Microsoft Azure et Google Cloud Platform, captent **à eux seuls 70 % du marché régional européen**.[4] À l'échelle mondiale, leur emprise dépasse les 60 % de l'ensemble des

[17]OCDE, Competition in the Provision of Cloud Computing Services, DAF/COMP/WD(2025)21, 19 juin 2025.
https://one.oecd.org/document/DAF/COMP/WD(2025)21/en/pdf
[18] Gartner, Gartner Says Worldwide IaaS Public Cloud Services Market Grew 22.5% in 2024, 6 août 2025.
https://www.gartner.com/en/newsroom/press-releases/2025-08-06-gartner-says-worldwide-iaas-public-cloud-services-market-grew-22-point-5-percent-in-2024
[19]Statista, Big Three Hold Dominant Lead in Accelerating Cloud Market, 5 Mai 2026.
https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/
[20] Synergy Research Group, European Cloud Providers Local Market Share Now Holds Steady at 15%, 4 Juillet 2025.
https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15

dépenses d'infrastructure cloud des entreprises, avec une domination nette d'AWS qui conserve 28 % à 37,7 % des parts de marché selon les segments, suivi par Microsoft Azure (21 % à 23,9 %) et Google Cloud (10 % à 14 %).[2]

GRAPHIQUE 1

Part de marché des fournisseurs de services cloud européens



Face à cette hégémonie, les fournisseurs européens de cloud, incluant des acteurs historiques des télécommunications et de l'hébergement comme SAP, Deutsche Telekom, OVHcloud, Telecom Italia, Scaleway, ou Outscale, ont vu leur part de marché s'effondrer structurellement. Alors qu'ils détenaient 29 % du marché européen en 2017, cette part a été réduite de moitié pour se stabiliser autour d'un seuil critique de 15 % depuis 2022.[4] La structure de ce marché met en exergue l'incapacité actuelle de l'industrie européenne à inverser la tendance macroéconomique. Les fournisseurs locaux sont cantonnés à des marchés de niche, des exigences locales de souveraineté stricte ou des offres de cloud privé hébergé. Ces secteurs

croissent structurellement moins rapidement que les offres publiques de type IaaS et PaaS.[4]

TABLEAU 2

Analyse de la concentration du marché cloud, basée sur les données d'intelligence économique de Synergy Research Group et Gartner.[2]

Fournisseur Cloud	Part de marché mondiale IaaS (2024)	Part de marché mondiale Cloud Infra (Q4 2025)	Positionnement et Part en Europe (2024-2025)
Amazon Web Services (AWS)	37,7 %	28 %	Leader de l'Oligopole (Inclus dans les 70 %)
Microsoft Azure	23,9 %	21 %	Co-leader de l'Oligopole (Inclus dans les 70 %)
Google Cloud Platform (GCP)	~10 % à 12 %	14 %	Challenger principal (Inclus dans les 70 %)
Acteurs Européens (Cumulés)	< 2 % (individuellement)	Marginale	15 % (Part de marché globale stabilisée)

Cette segmentation oligopolistique est particulièrement prononcée dans les couches supérieures du cloud. S'il est vrai que les acteurs français parviennent encore à concurrencer les géants sur l'IaaS grâce à des prix agressifs, l'intégration verticale de ces *hyperscalers* vers les couches supérieures (PaaS et SaaS) et l'ampleur de leurs catalogues rendent la lutte difficile pour des fournisseurs de taille intermédiaire.[1]

2. Crédits cloud

En amont du cycle d'adoption, l'oligopole consolide sa position dominante par une politique d'acquisition client agressive - car fondée sur une force de frappe financière et un niveau de gratuité inatteignables pour les fournisseurs locaux - **reposant sur la distribution de crédits cloud.**[21]

Concrètement, il s'agit de subventions immatérielles prenant la forme d'enveloppes financières virtuelles, permettant aux entreprises d'utiliser gratuitement les infrastructures du fournisseur jusqu'à épuisement d'un plafond prédéfini. Ces avantages en nature, distribués massivement aux incubateurs, aux universités, aux étudiants et aux jeunes pousses de la French Tech, peuvent atteindre plusieurs centaines de milliers de dollars par startup. Sous couvert de soutien à l'innovation, ces programmes tels qu'AWS Activate, Microsoft for Startups ou Google Cloud for Startups créent une dépendance architecturale et financière dès la phase de conception des logiciels.

Les startups, incitées par la gratuité initiale, optimisent leurs codes pour exploiter les composants propriétaires de l'*hyperscaler*. Ce choix génère un verrouillage technologique profond. La rentabilité de cette stratégie pour l'*hyperscaler* se matérialise quelques années plus tard : dès lors que l'entreprise cliente a épuisé ses crédits et commence à passer à l'échelle, elle se retrouve dans **l'incapacité technique et financière d'assumer les coûts de réécriture de son code** vers un standard interopérable européen. Elle devient alors une source de rente captive, payant le prix fort pour une infrastructure dont elle ne peut plus s'extraire. L'Autorité de la concurrence identifie très clairement ces crédits non pas comme de simples offres promotionnelles, mais comme des leviers transversaux affectant globalement la concurrence et bloquant l'expansion des concurrents locaux de taille plus modeste.[5]

[21]Autorité de la concurrence, Avis 23-A-08 du 29 juin 2023 portant sur le fonctionnement concurrentiel de l'informatique en nuage (« cloud »), 29 juin 2023. https://www.autoritedelaconcurrence.fr/sites/default/files/integral_texts/2023-06/23a08.pdf

B. Dominance financière et asymétrie des investissements : la fracture du capital

La dépendance du marché français n'est, en dernière analyse, que le symptôme d'une cause structurelle plus profonde : **une asymétrie écrasante des capacités d'investissement en capital et en recherche et développement.** L'industrie du cloud exige des économies d'échelle colossales. Elle est fondamentalement devenue une industrie lourde, une course à l'infrastructure physique impliquant l'acquisition massive de foncier, le raccordement à des réseaux électriques à très haute tension, l'achat continu de millions de serveurs, la conception de puces de silicium sur mesure et la construction de systèmes de refroidissement à l'échelle industrielle.

1. L'hyper-concentration des dépenses d'investissement (CapEx) et l'ère de l'IA

L'avènement et la transition accélérée vers l'intelligence artificielle, en particulier les modèles d'IA générative nécessitant des puissances de calcul phénoménales, ont propulsé les dépenses d'infrastructures cloud dans une dimension financière inédite, créant une fracture du capital infranchissable pour la quasi-totalité des fournisseurs européens.[4] L'analyse des rapports financiers des géants technologiques américains au tournant des années 2024-2025 témoigne d'une inflation spectaculaire de leurs investissements en infrastructures matérielles.[22]

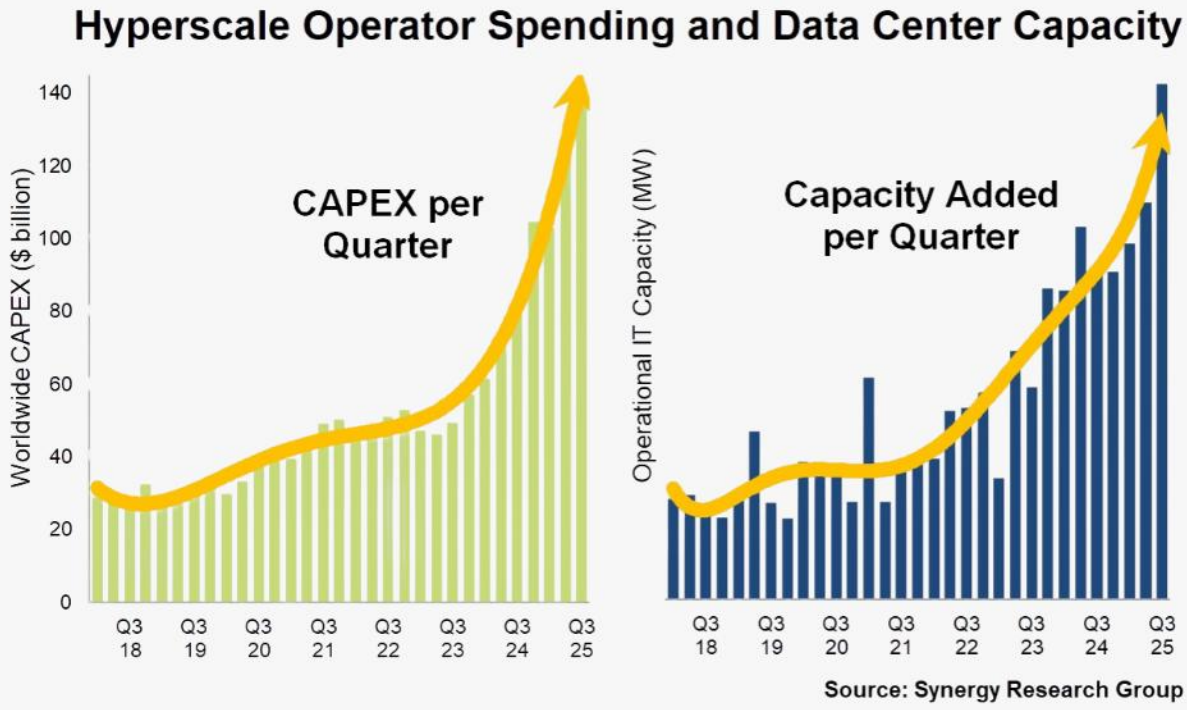
La course aux armements infrastructurels est vertigineuse. Selon les données de la première moitié de l'année 2025, le quatuor de tête : Microsoft, Amazon, Alphabet et Meta a collectivement investi la **somme de 155 milliards de dollars en dépenses d'investissement (CapEx),** un montant supérieur au budget de nombreux États souverains pour l'éducation ou les services sociaux.[23] Cette frénésie s'est encore accélérée au fil de l'année. Au troisième trimestre 2025, si l'on élargit le périmètre aux 21 principaux *hyperscalers* mondiaux, les dépenses ont atteint un montant

[22] Juniewicz, Isabel (pour Epoch AI), Hyperscaler capex has quadrupled since GPT-4's release, 26 février 2026.
https://epoch.ai/data-insights/hyperscaler-capex-trend
[23] The Guardian, Big tech has spent $155bn on AI this year. It's about to spend hundreds of billions more, 2 août 2025.
https://www.theguardian.com/technology/2025/aug/02/big-tech-ai-spending

record de 142 milliards de dollars sur ces trois seuls mois, soit une croissance fulgurante de près de 180 % sur trois ans.[24]

GRAPHIQUE 2

Dépenses des opérateurs *hyperscalers* et capacité des centres de données[25]



Les prévisions budgétaires à court terme accentuent encore ce déséquilibre. Pour l'année 2025, Amazon prévoyait d'investir plus de 100 milliards de dollars, principalement pour soutenir sa branche AWS et ses infrastructures IA.[6] De même, Alphabet a rapporté près de 40 milliards de dollars de CapEx sur les deux premiers trimestres de 2025, et Microsoft a engagé plus de 30 milliards sur un seul trimestre pour étendre les capacités de calcul de ses services d'IA Copilot.[6] Le volume de ces investissements absorbe désormais une part écrasante des flux de trésorerie opérationnels de ces entreprises. Les analyses financières de grandes banques d'investissement estiment que les dépenses liées à l'IA pour les grands *hyperscalers* atteindront 94 % de leurs flux de trésorerie opérationnels,

[24] Synergy Research Group, Hyperscale Spending Spree is Driving Dramatic Growth in Data Center Capacity, 19 December 2025 https://www.srgresearch.com/articles/hyperscale-spending-spree-is-driving-dramatic-growth-in-data-center-capacity

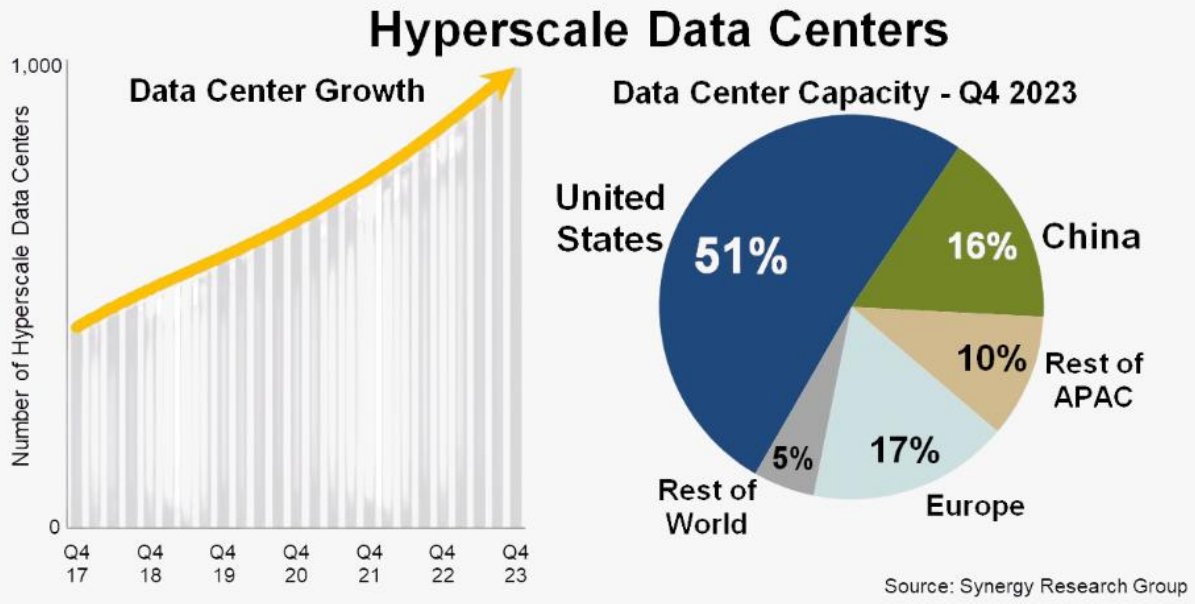
[25] Synergy Research Group, Hyperscale Spending Spree is Driving Dramatic Growth in Data Center Capacity, 19 December 2025 https://www.srgresearch.com/articles/hyperscale-spending-spree-is-driving-dramatic-growth-in-data-center-capacity

après rachats d'actions et dividendes, sur la période 2025-2026, en hausse par rapport aux 76 % déjà exceptionnels enregistrés en 2024.[26]

Cette débauche de capitaux se traduit physiquement par une multiplication des infrastructures critiques à l'échelle planétaire. Fin 2024, le nombre de méga-centers de données franchissait le seuil des 1 136 sites.[27] À la fin de l'année 2025, ce nombre approchait les 1 300 infrastructures, avec une concentration géopolitique inquiétante : 55 % de la capacité opérationnelle mondiale est située sur le seul territoire des États-Unis, tandis que l'Europe et la Chine se partagent la majorité du reste.[7]

GRAPHIQUE 3

Hyperscale Data Centers



[26] Buntz, Brian (pour R&D World), White House wins pledge from tech firms including Amazon, Google, Meta and Microsoft to fund power for AI data centers, 4 mars 2026. https://www.rdworldonline.com/white-house-wins-pledge-from-tech-firms-including-amazon-google-meta-and-microsoft-to-fund-power-for-ai-data-centers/

[27] Synergy Research Group, Hyperscale Data Center Count Hits 1,136; Average Size Increases; US Accounts for 54% of Total Capacity, 19 mars 2025 https://www.srgresearch.com/articles/hyperscale-data-center-count-hits-1136-average-size-increases-us-accounts-for-54-of-total-capacity

De surcroît, la capacité moyenne de chaque nouveau site augmente drastiquement pour accommoder les grappes de processeurs graphiques extrêmement énergivores, modifiant la donne sur la résilience des réseaux électriques nationaux.[10] En France, la Commission de régulation de l'énergie (CRE) a souligné que la demande induite par ces infrastructures impose des défis majeurs sur l'équilibre offre-demande électrique, avec une capacité estimée passant de 10 GW en 2023 à 15 GW projetés en 2035, nécessitant des adaptations systémiques lourdes.[28]

2. Comparaison avec les acteurs Français

L'asymétrie financière devient manifeste et structurellement problématique lorsqu'elle est mise en perspective avec les bilans des champions industriels français et européens du secteur. OVHcloud, leader européen incontesté et porte-étendard du cloud souverain de type "*pure player*" - c'est-à-dire un acteur dont l'activité est exclusivement dédiée aux infrastructures *clouds* - affiche des performances financières remarquables à son échelle, démontrant la viabilité d'un modèle alternatif, mais qui demeurent sans aucune commune mesure avec les moyens de l'oligopole américain.

Pour son exercice fiscal 2024, OVHcloud a généré un chiffre d'affaires consolidé de 993,1 millions d'euros, enregistrant une croissance organique de 10,7 % dans un contexte économique incertain.[13] L'entreprise fondée par Octave Klaba opère 45 centres de données répartis sur 4 continents et affiche une excellente rentabilité avec une marge EBITDA[29] ajustée de 38,4 %.[30] En matière de stratégie d'investissement, le CapEx récurrent représente environ 16 % de son chiffre d'affaires, et le CapEx de croissance s'élève à environ 24 %.[31] Les investissements annuels de l'opérateur français s'établissent ainsi autour de 100 millions d'euros.

[28] Commission de régulation de l'énergie (CRE), Comment gérer les nouveaux équilibres dynamiques entre l'offre et la demande, Février 2026. https://www.cre.fr/fileadmin/Documents/Rapports_et_etudes/2026/Rapport_Prospective_Equilibres_offre_demande.pdf

[29] **EBITDA** ou Earnings Before Interest, Taxes, Depreciation and Amortization, se traduit en français par bénéfice avant intérêts, impôts, dépréciation et amortissement.

[30] OVHcloud, Résultats financiers de l'exercice 2025 (FY25), 21 octobre 2025. https://corporate.ovhcloud.com/fr/newsroom/news/financial-results-fy25/

[31] OVHcloud, Q1 FY24 Revenue (Communiqué de presse), 11 janvier 2024. https://corporate.ovhcloud.com/sites/default/files/2024-04/2024-01-11-ovhcloud-q1-fy24-pr-eng-vdef_2.pdf

Cependant, **d'un point de vue strictement arithmétique et macroéconomique, le rapport de force financier est de l'ordre de 1 à 100, voire de 1 à 200.** Les dépenses d'investissement combinées d'une entreprise comme Microsoft ou Amazon sur quelques jours de l'année 2025 dépassent la totalité du budget annuel d'investissement du principal fournisseur européen.[6] Cette disparité structurelle démontre une chose : l'ambition de concurrencer les *hyperscalers* sur l'ensemble du spectre fonctionnel est une équation économique impossible à résoudre pour des acteurs de taille intermédiaire agissant seuls.[2]

TABLEAU 3

Comparatif de l'échelle industrielle illustrant la fracture du capital entre les *hyperscalers* et l'industrie souveraine.

Métrique Financière Stratégique (Estimations 2024/2025)	Amazon (AWS)	Alphabet (Google Cloud)	OVH cloud
Chiffre d'Affaires Annuel Cloud (Ordre de grandeur)	~130 Milliards $ (AWS 2024)	> 40 Milliards $	~993 Millions € (2024)
CapEx Total Annuel / Projection (IA, Cloud & Infra)	~200 Milliards $ (Projection 2026)	> 50 Milliards $ (Est. 2025)	~100 Millions € (10% du CA)
Bénéfice Opérationnel lié au Cloud	~45 Milliards $ (AWS 2024)	Données agrégées positives	Marge EBITDA ~38,4%

Une part de la résilience financière des *hyperscalers* réside également dans leur modèle économique intégré, qui subventionne la croissance de leur infrastructure cloud. AWS représente 57 % du profit opérationnel total d'Amazon, compensant les faibles marges de son cœur de métier dans le commerce de détail, tandis que l'infrastructure d'Alphabet bénéficie des revenus massifs de son monopole publicitaire.[3] Les fournisseurs de cloud européens, opérant souvent de manière autonome sans ces moteurs de rentabilité annexes, doivent financer leur croissance exclusivement sur les marges de leurs services d'hébergement.

3. Le transfert de valeur macroéconomique et l'effet d'éviction technologique

Au-delà de la simple concurrence entre entreprises, cette domination financière engendre un problème macroéconomique profond pour la France et l'Europe : un transfert de valeur massif et structurellement asymétrique. Chaque adoption généralisée du cloud public américain par l'industrie, le secteur de la santé, le secteur bancaire ou l'administration française se traduit par une **exportation nette de capital.**[11]

Le coût de l'abonnement mensuel (OpEx) versé par une entité française finance directement la recherche, la capacité de calcul, l'achat de GPU, et la puissance algorithmique d'une entité dont le siège social et la propriété intellectuelle sont situés hors du territoire national. Ce déséquilibre, conceptuellement lié à la notion de "value gap" (transfert de valeur ou écart de valeur), induit que la matière première stratégique du XXIe siècle, la donnée, est non seulement stockée, mais surtout **traitée, enrichie et monétisée sous contrôle d'intérêts économiques étrangers**. L'économie française s'expose ainsi au risque systémique de devenir une simple consommatrice de rentes technologiques, perdant la maîtrise de sa chaîne de valeur numérique.

Parallèlement, cette surface financière illimitée des *hyperscalers* produit un effet d'éviction majeur sur le marché des fusions et acquisitions technologiques mondiales. Les acteurs américains disposent de réserves de liquidités telles qu'ils **survalorisent structurellement les jeunes pousses innovantes** (ex. : Rachat de Wiz par Google pour 33 Milliards de dollars), rendant leur rachat prohibitif pour les entreprises européennes. Comme le soulignait une mission d'information parlementaire française, des entreprises de cybersécurité ou de briques cloud innovantes, à l'instar d'Alcide, finissent inexorablement absorbées par des sociétés américaines, les acteurs européens ne pouvant s'aligner financièrement sur les multiples de valorisation proposés outre-Atlantique.[32] Le tissu industriel français est ainsi continuellement drainé de ses meilleures innovations, siphonnées par l'écosystème financier de la Silicon Valley ou de Seattle.

[32]Warsmann, Jean-Luc et Latombe, Philippe (pour l'Assemblée nationale), Rapport d'information n° 4299 : Bâtir et promouvoir une souveraineté numérique nationale et européenne, 29 juin 2021. https://www.assemblee-nationale.fr/dyn/15/rapports/souvnum/l15b4299-t1_rapport-information

C. Les partenariats hybrides (Bleu, S3NS)

Face au constat lucide d'un marché verrouillé, d'une fracture d'investissement irrécupérable à court terme par les seuls acteurs nationaux, et sous la pression croissante de l'extraterritorialité du droit américain, que nous analyserons dans le chapitre suivant, l'État français a opéré une inflexion stratégique majeure. En 2021, la doctrine de l'État a été mise à jour via la circulaire “Cloud au Centre”. L'ambition affichée par ce modèle hybride repose sur un compromis théorique : **capter l'avance technologique et fonctionnelle des plateformes américaines, tout en tentant d'y superposer un cadre de contrôle juridique et opérationnel souverain.**

C'est dans ce contexte réglementaire et institutionnel que le modèle du partenariat industriel hybride a émergé, donnant naissance à deux acteurs majeurs qui redessinent l'architecture du marché : Bleu et S3NS. Ce modèle repose sur un mécanisme financier de licence technologique. Des acteurs historiques français, bénéficiant d'infrastructures locales, de capacités d'investissement propres et opérés exclusivement par des citoyens européens, achètent le droit d'utiliser, de distribuer et d'héberger les technologies des hyperscalers américains au sein d'un environnement hermétique. L'ambition affichée est l'obtention de la plus haute qualification de sécurité nationale, le visa SecNumCloud 3.2 délivré par l'ANSSI, garantissant en théorie l'immunité juridique contre les injonctions extra-européennes.

1. L'architecture économique et industrielle de Bleu et S3NS

La structure industrielle de ces coentreprises obéit à une logique de capitalisation et de gouvernance nationales, tout en s'adossant à l'ingénierie logistique et logicielle américaine. Le financement des infrastructures physiques (centres de données) incombe aux partenaires français, tandis que **la propriété intellectuelle logicielle reste américaine.**

Le consortium Bleu (Orange, Capgemini et Microsoft): Fondé conjointement par deux champions technologiques nationaux, l'opérateur de télécommunications Orange et l'entreprise de services du numérique Capgemini, Bleu se positionne comme une entreprise de services cloud indépendante et de droit français.[33] Son modèle d'affaires consiste à

[33]Bleu, Site officiel.
https://www.bleucloud.fr/

commercialiser la suite collaborative Microsoft 365 (incluant les outils de productivité et Microsoft Teams) ainsi qu'un sous-ensemble étendu des services de la plateforme Microsoft Azure, sous un pavillon souverain visant la qualification SecNumCloud 3.2.[16]

D'un point de vue industriel, les centres de données de Bleu sont localisés en France, distribués sur deux régions distinctes (séparées de plus de 300 kilomètres) pour assurer une résilience et une continuité de service équivalentes aux standards des hyperscalers. Bleu s'adresse particulièrement au cœur régalien et industriel de la nation : les opérateurs d'importance vitale (OIV) et de services essentiels (OSE), qui englobent les secteurs dont l'arrêt ou la compromission menacerait la sécurité, l'économie ou la survie même de la Nation (comme la distribution d'énergie, les transports, les télécommunications, le système bancaire ou la santé), ainsi que les grandes administrations centrales (ministères régaliens, services fiscaux, agences étatiques).

La pertinence de ce modèle hybride a d'ores et déjà convaincu de grands donneurs d'ordres stratégiques d'engager leur transition. Le groupe énergétique EDF, l'industriel Dassault Aviation, et Orange Business lui-même (qui y migre 70 % de sa propre infrastructure informatique interne) ont officiellement choisi Bleu pour sécuriser leurs données sensibles.[16]

Le modèle S3NS, fruit de l'alliance stratégique entre Thales et Google Cloud, s'incarne dans une société de droit français créée en juin 2022. Contrôlé intégralement par Thales, leader européen de la cybersécurité et de la défense, il exploite sous licence la technologie de Google Cloud Platform.
Contrairement à Bleu, dont la genèse a pris plus de temps, S3NS a adopté une stratégie industrielle de mise sur le marché en deux étapes pour occuper rapidement le terrain commercial.

Dans un premier temps, S3NS a lancé en 2023 l'offre de transition « Contrôles Locaux » (désormais nommée CRYPT3NS). Cette offre utilise les infrastructures européennes standard de Google, mais S3NS y agit comme un tiers de confiance gérant les clés de chiffrement externes (EKM : External Key Manager) depuis la France. Cela garantit théoriquement une souveraineté de la donnée par la cryptographie, bloquant l'accès technique de Google aux données claires. Dans un second temps, S3NS déploie son offre cible “Cloud de Confiance” (PREMI3NS), conçue pour répondre aux exigences de SecNumCloud 3.2. Cette architecture implique une infrastructure matérielle physiquement et logiquement isolée du réseau

public de Google, hébergée dans trois centres de données dédiés en région parisienne, et opérée, supervisée et sécurisée par le personnel de S3NS soumis au droit français. Cette stratégie semble avoir fonctionné, compte tenu qu'en décembre 2025 S3NS a officiellement obtenu la qualification SecNumCloud 3.2 en décembre 2025 pour ses services IaaS, PaaS et CaaS.

2. L'effet d'éviction et la fracture de l'écosystème français

Si la réponse opérationnelle apportée par les partenariats hybrides Bleu et S3NS satisfait à court terme aux impératifs de conformité réglementaire des DSI, elle soulève une problématique industrielle et financière majeure qui fracture profondément l'écosystème technologique français. Les acteurs dits "*pure players*", qui développent, investissent et opèrent l'intégralité de leurs propres piles technologiques (à l'image d'OVHcloud, Scaleway, 3DS Outscale ou Cloud Temple), dénoncent un modèle économique asymétrique qui s'apparente, selon eux, à une **"souveraineté de façade" ou une "pseudo-souveraineté".** Les auditions menées par la commission ont mis en lumière le risque que cet engagement puisse s'apparenter davantage à un artifice de communication qu'à une véritable souveraineté[34]

Cette critique structurelle s'articule autour du concept fondamental de la captation de la valeur ajoutée et de la rente technologique. Dans le cadre des consortiums Bleu ou S3NS, la propriété intellectuelle du code, le développement algorithmique, l'optimisation des hyperviseurs[35] et le cœur d'innovation de l'infrastructure (notamment les services PaaS d'intelligence artificielle) demeurent intrinsèquement américains. Le versement récurrent de redevances et de droits de licence (*licensing*) à Microsoft ou Google engendre un flux financier substantiel qui continue de nourrir les bilans, la R&D et la capitalisation boursière des hyperscalers.[15] L'acteur français, qu'il s'agisse de Thales, d'Orange ou de Capgemini, assume la part la plus intensive en capital physique (le financement de la tôle et du béton des datacenters), le risque financier de la commercialisation, la responsabilité légale face à l'ANSSI, et le centre de coût humain du support technique. En échange, il est relégué dans une position de franchisé de luxe ou de super-intégrateur, **abandonnant les marges exceptionnelles liées à la création de la propriété intellectuelle logicielle.**

[34] Adam, Quentin, Yann Lechelle et Michel Paulin, Tribune: N'est pas cloud à la française qui veut, Les Échos, 29 juin 2022. https://www.lesechos.fr/idees-debats/cercle/opinion-nest-pas-cloud-a-la-francaise-qui-veut-1582536

[35] **Hyperviseur :** Logiciel que vous pouvez utiliser pour exécuter plusieurs machines virtuelles sur une seule machine physique.

Au niveau macroéconomique, la légitimation de ces offres hybrides par l'obtention du label SecNumCloud crée un puissant effet d'éviction (*crowding-out effect*) sur le marché intérieur.[30] L'onction institutionnelle et l'octroi implicite du blanc-seing étatique risquent de détourner la commande publique, les marchés ministériels et les colossaux budgets de transformation numérique des grandes entreprises du CAC 40 au profit des technologies américaines labellisées françaises, au détriment des alternatives purement européennes.[15]

Les dirigeants des industriels locaux, à l'instar d'Octave Klaba (président et fondateur d'OVHcloud) ou Yann Lechelle (ancien dirigeant de Scaleway), ont maintes fois alerté par voie de presse et rapports sur le péril mortel de cette dynamique. Ils argumentent de l'impossibilité de bâtir une véritable industrie de pointe européenne si la demande interne solvable (celle de l'État et des OIV) se contente d'acheter des solutions où la technologie sous-jacente échappe à la maîtrise locale. Si les acteurs souverains sont privés de cet effet de levier sur leur propre marché intérieur, ils seront affamés de la trésorerie vitale nécessaire pour financer leurs propres CapEx, recruter des ingénieurs de haut niveau, et concevoir les futures générations d'infrastructures numériques capables de rivaliser mondialement. Néanmoins, si cette analyse macroéconomique est fondée, elle s'inscrit aussi dans une évidente logique de lobbying : ces acteurs étant les premiers lésés sur le plan commercial par l'émergence des offres hybrides, leur discours relève autant de la protection légitime de leurs intérêts financiers que de la défense de la souveraineté nationale.

De surcroît, le modèle financier hybride pose la question de l'indépendance à long terme. La pérennité fonctionnelle de ces offres pourrait rester tributaire de l'engagement des partenaires américains à maintenir et transférer leurs mises à jour logicielles dans la bulle isolée (*air-gapped*) française. Si, à l'avenir, pour des raisons géopolitiques, tarifaires ou réglementaires, un *hyperscaler* était amené à limiter ou retarder le déploiement de ses innovations dans ces environnements de confiance, l'offre locale s'exposerait à un risque d'obsolescence rapide face au marché mondial. L'entreprise française partenaire n'ayant pas développé le code source, elle n'aurait **aucune capacité de substitution**, illustrant la précarité fondamentale de toute dépendance industrielle établie en bout de chaîne de valeur.

À RETENIR

Dépendances industrielles et financières

- En définitive, l'analyse des dynamiques industrielles et financières démontre que l**a souveraineté numérique ne peut se résumer à une simple localisation territoriale des serveurs**. Le marché du cloud s'est mué en une industrie lourde, régie par des barrières à l'entrée (CapEx) que la révolution de l'intelligence artificielle a rendues virtuellement infranchissables pour les acteurs européens agissant de manière isolée. **À travers le mécanisme du value gap, la France et l'Europe font face à un transfert de valeur systémique** : la commande publique et privée locale finance directement la R&D d'un oligopole américain toujours plus concentré.

- Face à cette asymétrie structurelle, le modèle hybride incarné par **les consortiums Bleu ou S3NS offre un compromis pragmatique à court terme.** Il apporte une réponse de conformité immédiate aux donneurs d'ordres stratégiques pressés de moderniser leurs infrastructures.

- Cependant, **ce modèle de "franchise technologique" fige l'industrie européenne en bout de chaîne de valeur**. En renonçant à la maîtrise de la propriété intellectuelle algorithmique au profit d'une protection purement physique et contractuelle, **la stratégie nationale prend le risque d'institutionnaliser sa dépendance technologique** et de fragiliser durablement la croissance de ses propres *pure players*.

- Si la bataille des infrastructures matérielles et de l'hyper-capitalisation semble, pour l'heure, dominée par les géants outre-Atlantique, la viabilité même de ces solutions de repli repose en réalité sur un autre pilier, bien plus insidieux : celui de **la loi**. Dès lors que la technologie sous-jacente est d'origine étrangère, c'est l'étanchéité du bouclier juridique qui détermine l'étendue réelle de notre souveraineté. **C'est précisément cette confrontation avec l'extraterritorialité du droit américain et la guerre normative internationale qui constitue le prochain défi de l'indépendance numérique européenne.**

III. Chapitre 3 : Dépendances juridiques et extraterritoriales

Avec l'émergence fulgurante des nouvelles technologies, en particulier celle de l'Intelligence Artificielle, la Commission Européenne a privilégié une approche fondée sur la régulation de l'espace digital, faute de pouvoir innover à la même échelle et vitesse que les Etats Unis. Le Règlement Général sur la Protection des Données (RGPD), qui vise à protéger les données privées des citoyens européens, est ainsi cité en masse pour témoigner du pouvoir législatif des Institutions européennes.

Pourtant, Washington D.C. détient un levier juridique moins connu du grand public européen : les lois extraterritoriales, qui permettent de contourner les régulations européennes. En effet, quand deux ordres juridiques s'opposent, il va de soi que la juridiction qui détient le quasi-monopole sur l'objet sous-jacent, finisse par prévaloir sur l'ordre qui en dépend. Cette partie analysera les contradictions entre les lois extraterritoriales des États Unis et les protections juridiques européennes des données.

A. L'extraterritorialité américaine : l'accès illimité aux données hébergées en Europe des entreprises américaines

L'extraterritorialité fait référence à des lois dont le champ d'application va au-delà du territoire de la juridiction qui les édicte, par exemple des lois américaines, qui s'applique au-delà du territoire des Etats Unis.

C'est à la suite des attentats du 11 septembre 2001 que le Congrès américain a multiplié l'adoption de lois extraterritoriales, inscrites dans une logique de "*guerre contre le terrorisme*" ("*war on terror*"). D'autres motifs, notamment la lutte contre le blanchiment d'argent, les crimes, les réseaux de traite humaine et l'exploitation sexuelle d'enfants et les cybercrimes[36], sont invoqués pour le droit de surveillance des données par les autorités américaines.

[36]U.S. Department of Justice. « CLOUD Act Resources ». Consulté le 1 février 2026. https://www.justice.gov/criminal/cloud-act-resources.

Ces lois s'appliquent aux systèmes de communications et informations, mais elles ont également des répercussions sur les données hébergées dans le cloud, qui s'est développé depuis. Parmi les textes les plus significatifs, nous pouvons citer :

1. Les lois extraterritoriales américaines

a. Cloud Act

Le *Clarifying Lawful Overseas Use of Data Act*[37] ou Cloud Act a été adopté par le congrès des Etats Unis en mars 2018. Il s'agit d'une loi fédérale, qui vise à permettre un accès accéléré à des informations digitales essentielles au nom de la sécurité nationale.

Les fournisseurs de services de communication électronique (ECS) ou de services informatiques à distance (RCS) doivent permettre l'accès, le back-up et la préservation des informations (communications ou données), qu'elles soient hébergées aux Etats-Unis ou ailleurs (Cloud Act, § 2713). Selon la division criminelle du département de la justice américain, l'accès à ces informations est essentiel non seulement pour le gouvernement américain, mais également pour des partenaires étrangers des Etats-Unis afin d'accélérer les investigations de crimes graves.

Pour le Cloud Act, la demande par les autorités américaines peut être contestée par l'entreprise visée. Par ailleurs, la demande par les autorités américaines doit être motivée et proportionnée. De l'autre côté de l'Atlantique, les citoyens européens peuvent théoriquement faire recours devant un juge américain lors d'une procédure publique.

b. FISA 702[38]

Contrairement au Cloud Act, qui porte sur les données stockées par des entreprises américaines, la section 702 de la loi sur la surveillance du renseignement étranger (FISA) a une portée sur les communications électroniques globales.

Ainsi, cette législation autorise les services de renseignements américains à collecter, analyser et partager "de façon appropriée" des renseignements

[37] § 2713. U.S. Department of Justice. « CLOUD Act White Paper ». Consulté le 1 février 2026. https://www.justice.gov/criminal/media/999391/dl?inline.
[38] Revue critique de droit international privé. « § 2713 ». Revue critique de droit international privé, 2019/3, p. 681.https://droit.cairn.info/revue-critique-de-droit-international-prive-2019-3-page-681?lang=fr

sur des étrangers (les citoyens américains étant explicitement exclus) concernant des menaces pour la sécurité nationale des Etats Unis[39].

Cet accès aux données de certains citoyens et entreprises répond à un problème rencontré en 2008 dans le traçage de terroristes par les Etats Unis. En effet, des groupes terroristes à l'étranger, utilisaient des comptes emails de fournisseurs de services américains sans que les services d'intelligences américains puissent accéder aux communications. Cette loi tente de contrer ce manquement, mais elle est accompagnée de distorsions.

Le risque d'un défaut de protection des données européennes semble être modéré pour le Cloud Act. En revanche le FISA 702, quant à lui, présente un risque systémique, en permettant la collecte systématique de renseignements de non-Américains, via des programmes de surveillance électronique comme PRISM. Ainsi, ce programme porte atteinte à la protection des données personnelles, étant donné que cette procédure peut se faire sans mandat individuel et sans contrôle judiciaire[40].

c. USA Patriot Act

USA Patriot Act (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*) : Cette loi antiterroriste, signée un mois après les attentats du 11 septembre 2001, permet aux agences de renseignements américaines de surveiller les communications téléphoniques et sur internet de personnes soupçonnées de terrorisme ou d'espionnage[41].

Cette surveillance électronique peut être faite sans mandat préalable. Elle permet notamment aux services de renseignements d'accéder à des dossiers financiers, scolaires et médicaux, sans que la personne ciblée ne soit notifiée. Ainsi, cette loi met sérieusement en danger la protection des données des citoyens européens.

[39] Office of the Director of National Intelligence. « *FISA Section 702* ». Consulté le 18 février 2026. https://www.intel.gov/foreign-intelligence-surveillance-act/fisa-section-702.
[40] Le Monde. « PRISM, Snowden, surveillance de la NSA : tout comprendre en 6 étapes ». 2 juillet 2013.https://www.lemonde.fr/technologies/article/2013/07/02/prism-snowden-surveillance-de-la-nsa-tout-comprendre-en-6-etapes_3437984_651865.html
[41]NumSpot. « *Cloud Act, Patriot Act vs RGPD : que faut-il retenir ?* ». Consulté le 1 février 2026. https://numspot.com/ressource/cloud-act-patriot-act-vs-rgpd-que-faut-il-retenir/.

d. Executive Order 12333

L'**Executive Order (EO) 12333**, confère à la National Security Agency (agence de sécurité nationale américaine), l'autorité de collecter des communications émanant d'étrangers, qui ont lieu intégralement hors du territoire des États-Unis. Les communications peuvent également être interceptées, lorsqu'une personne située hors des États-Unis communique avec une personne située aux États-Unis, ou inversement.

Selon ces textes juridiques, les autorités américaines pourraient ainsi demander des renseignements sur n'importe quel citoyen européen, selon des critères plus ou moins opaques. Si l'Union Européenne tente de légiférer à bon escient afin de protéger les données personnelles, sa dépendance technologique, mais aussi la supériorité juridique imposée par les États-Unis, posent problème dans l'application de ces protections, tels que le règlement général sur la protection des données (RGPD).

Les lois extraterritoriales américaines sont généralement méconnues du grand public, ce qui pose problème étant donné que les procédures d'investigation par les autorités américaines peuvent être conduites sans que la personne concernée en soit informée, comme pour le FISA 702. Toutefois, le FISA exige un périmètre précis, lié à une enquête judiciaire. La demande d'obtention d'informations peut également être contestée par l'entreprise devant la Cour suprême, qui n'est pas toujours alignée avec l'exécutif. Certaines entreprises sont transparentes quant aux demandes d'obtention d'information, telles que Microsoft qui publie deux fois par an, les requêtes formulées par les autorités américaines dans les pays européens dans lesquels elle opère. Ainsi l'application de la protection des données personnelles des européens dépend en partie des mécanismes de contrôle et de contestation mis en place par les entreprises et les autorités américaines, ce qui expose l'UE à une vulnérabilité structurelle liée à des décisions qui échappent à sa souveraineté juridique.

2. Les protections juridiques européennes : Le RGPD

Les dispositifs de protection pour les données personnelles en Europe relèvent depuis 2016 du règlement général sur la protection des données (RGPD). Comme pour les lois américaines, ce règlement comporte une dimension extraterritoriale : il s'applique non seulement aux traitements réalisés dans l'Union, mais également à toute organisation hors UE dès lors qu'elle cible des résidents européens.

Le RGPD revendique une portée extraterritoriale. L'Union européenne se vante même de son "effet Bruxelles", c'est-à-dire, la capacité de la régulation européenne à influencer les normes mondiales en matière de protection des données. Cependant cette ambition normative masque une réalité plus complexe : si le texte vise à protéger les citoyens européens, son efficacité est limitée par l'existence d'autres législations nationales, notamment américaines. Malgré l'intention du RGPD, qui vise à protéger les citoyens européens, les grandes entreprises soumises à ces lois étrangères disposent d'une marge de manœuvre créant des failles structurelles (*loopholes*) dans l'application du cadre européen, comme nous l'analyserons ci-dessous.

3. Le modèle chinois de protection des données : le PIPL

L'UE n'est pas la seule à édicter un corpus normatif afin de vouloir protéger ces citoyens. A l'instar du RGPD, la République populaire de Chine a adopté une loi sur la protection des données, abrégée par PIPL (*Personal Information Protection Law*).

Cette législation, entrée en vigueur le 1er novembre 2021, semble de prime abord inspirée par le RGPD, telles que le consentement préalable pour collecter les données, les droits pour les individus et les obligations pour les entreprises. Pourtant le penchant chinois du RGPD est plus centré sur la souveraineté nationale. Le PIPL empêche toutes données d'un citoyen chinois de quitter le territoire chinois. En effet, les transferts transfrontaliers de données sont fortement encadrés, voire bloqués, notamment pour des données considérées "importantes".[42]

Le PIPL est donc en quelque sorte une loi extraterritoriale inversée : toute entreprise opérant en Chine, même étrangère, doit impérativement héberger et traiter les données en Chine. Cela implique de passer par un cloud local, comme Alibaba Cloud ou Huawei Cloud. Cela permet aux entreprises chinoises (souvent liées au parti) de garder une part d'influence sur le marché chinois. En outre, l'Etat chinois vient renforcer son pouvoir sur l'information, par des audits (des contrôles) de sécurité obligatoire effectués par les autorités chinoises, qui peuvent se solder par des sanctions si les autorités jugent les opérations d'une entreprise non-conformes. [43]

[42] Personal Information Protection Law (PIPL). « PersonalInformationProtectionLaw.com ».Consulté le 7 mars 2026.
https://personalinformationprotectionlaw.com/
[43] *Ibid*

Ainsi on pourrait être porté à croire, qu'une protection dans les faits est possible, puisque la Chine parvient à interdire la sortie des données de ces citoyens. Pourtant, il y a des différences majeures entre la Chine et l'UE : contrairement à la Chine, qui est un régime autoritaire, l'UE ne peut pas imposer des contrôles arbitraires aux entreprises. Par ailleurs, l'UE ne détient pas un écosystème cloud indépendant, et manque structurellement d'alternatives européennes à grande échelle, comme Alibaba Cloud en Chine.

Outre les différences politiques et économiques entre la Chine et l'UE, le cadre juridique de l'UE et ses engagements dans des organisations internationales rendent impossible la transposition du modèle juridique chinois. Avec l'adhésion à l'Organisation mondiale du Commerce (OMC) en 1994, l'UE s'engage à respecter le corpus normatif de l'OMC. Ainsi, l'UE ne peut pas restreindre l'accès à son marché de la technologie afin de favoriser des acteurs "nationaux" ou "européens" (selon les article II, XVI et XVII du GATT). La Chine, en revanche, adhère également à l'OMC depuis 2001, mais sous un régime spécial, qui exclut partiellement la Chine des provisions juridiques de l'OMC en matière d'infrastructures critiques et de services numériques et informatiques. [44]

Même dans le cas hypothétique où l'UE ne serait pas contrainte par ces engagements internationaux, le fait est que les grandes entreprises de tech américaines sont souvent implantées sur le territoire européen, sous formes de filiales européennes. A l'instar de Microsoft Ireland Operations Ltd., Google Ireland Ltd. ou Amazon Web Services EMEA SARL au Grand-Duché du Luxembourg. Par conséquent, selon le droit européen sur le marché intérieur (art. 49 et 56 du TFUE), l'UE ne peut pas exclure des entreprises européennes de prestations de services dans un autre États membre de l'UE. [45]

[44] Organisation mondiale du commerce (OMC). « Organe d'appel : Communiqué de presse 243 ». 2001.. Consulté le 17 avril 2026.https://www.wto.org/french/news_f/pres01_f/pr243_f.htm
[45]Toute l'Europe. « La libre circulation des services et la liberté d'établissement ».Consulté le 18 février 2026.
https://www.touteleurope.eu/economie-et-social/la-libre-circulation-des-services-et-la-liberte-d-etablissement/

B. L'asymétrie juridique : Un risque invisible

1. La superposition de lois : le conflit de lois extraterritoriales

Comme vu précédemment, les données dans les cloud sont très mobiles. Ainsi une donnée peut être stockée dans un pays A, traitées par une entreprise dans un pays B et appartenir à un utilisateur d'un pays C. Ce millefeuille normatif, entraîne *de facto*, une supériorité de la loi du pays, qui détient le contrôle sur la quasi-totalité des données mondiales.

Ainsi, même si les données sont stockées sur des serveurs en Europe, par des entreprises américaines, elles restent accessibles par les autorités américaines. Autrement dit, l'extraterritorialité américaine neutralise les protections juridiques européennes. Surtout au vu de la domination des acteurs américains sur le marché européen.

En outre, ces lois américaines, dites **"extraterritoriales" posent des problèmes à trois niveaux au niveau de la protection des droits humains** (pour le reste du monde et notamment la France) :

1. **la violation de la vie privée ;**
2. **la diminution du droit à la liberté d'expression ;**
3. **la réduction du droit de la défense et d'un procès équitable** [46]

Au-delà des deux premiers dangers, qui mettent en péril des droits de l'homme essentiels, le troisième axe est aujourd'hui sérieusement en péril : celui du droit à un procès équitable. Outre le fait, que le recours doit être présenté par l'entreprise américaine (par exemple dans le cas du FISA), l'élargissement de la définition du terme "terrorisme" est préoccupant.[47] Depuis 2001, dans une logique de guerre "préventive" des opérations de neutralisation d'individus considérés comme "terroristes", peuvent être conduites même avant que ces personnes ne commettent un crime. Cela veut dire que potentiellement, une personne, qui a échangé par *email* ou téléphone avec une personne reliée à une organisation terroriste peut être mise sous surveillance terroriste, sans en être informée par le biais de

[46] Office of the United Nations High Commissioner for Human Rights (OHCHR). The Right to Privacy in the Digital Age. Rapport du Haut-Commissariat des Nations unies aux droits de l'homme, 2014.. Consulté le 1 février 2026.https://digitallibrary.un.org/record/777869?v=pdf

[47] Just Security. « The Massive Perils of the Latest U.N. Resolution on Terrorism ».Consulté le 17 avril 2026.https://www.justsecurity.org/64840/the-massive-perils-of-the-latest-u-n-resolution-on-terrorism/

demande d'information par les autorités américaines. Cette extension du périmètre de surveillance pourrait en apparence sembler une avancée, mais les dérives qu'elle autorise sont préoccupantes.
Pourtant ces dispositions légales très larges, mettent en danger la juste représentation de l'accusé, étant donné que même des avocats défendant les droits humains sont mis sur ces listes de surveillance terroristes. C'est le cas du Professeur et avocat Gavin Sullivan mis sous surveillance pour ces accompagnements juridiques pro bono à des personnes injustement présentes sur les listes de surveillance.[48] Cette définition vaste ouvre une brèche à des dérives juridiques et des persécutions potentiellement injustifiées à des fins politiques. Ainsi, des personnes peuvent être mise sur surveillance de terrorisme, sans avoir commis d'acte terroriste et avec un recours juridique compliqué.[49]

Même si le but premier avancé par les États-Unis est la lutte contre le terrorisme et la prolifération d'armes, ainsi que la préservation de la sécurité nationale toutes ces lois extraterritoriales font vaciller la souveraineté numérique de la France et de toute l'Europe. Dès lors que l'UE et la France ont un train de retard, quant au développement de cloud européen ou souverain, elles doivent se soumettre à l'ordre juridique édicté par les grands acteurs, qui régissent le marché du cloud.

2. Les précédents et la jurisprudence : De l'annulation du *Privacy Shield* aux incertitudes actuelles

À chaque fois que l'Union Européenne a tenté d'imposer un cadre réglementaire sur le transfert de données, celui-ci finit par être fragilisé, voire même entièrement invalidé.

En 2016, un accord transatlantique entre les Etats Unis et l'Union Européenne était entré en vigueur afin d'établir un bouclier de protection des données, le "*Privacy Shield*". A travers un mécanisme d'auto-certification des entreprises américaines, ce bouclier constituait une garantie juridique offrant un niveau de protection, jugé adéquat par la Commission Européenne pour le transfert de données de l'UE vers les Etats-Unis. Il est essentiel de noter que ce bouclier de protection ne concernait que la partie RGPD et non pas les données sensibles de recherche et

[48] Cours magistral de Gavin Sullivan, Global Security Law, Sciences Po Paris, novembre 2025. Voir également : https://www.law.ed.ac.uk/people/dr-gavin-sullivan
[49] Sullivan, Gavin. Watchlisting the World: Digital Security Infrastructures, Informal Law, and the "Global War on Terror".Consulté le 17 avril 2026.https://www.justsecurity.org/78779/watchlisting-the-world-digital-security-infrastructures-informal-law-and-the-global-war-on-terror/

développement, de défense ou de propriété intellectuelle, mais constituait tout de même une avancée dans ce domaine.

Pourtant, en 2020 dans l'arrêt "Schrems II", la Cour de Justice de l'Union Européenne a invalidé le "*Privacy Shield*". La Cour estimant que les lois extraterritoriales américaines, notamment le EO 12333 et le FISA 702, permettaient un accès disproportionné aux données des utilisateurs européens et que ceux-ci n'avaient pas de recours effectifs auprès des tribunaux américains.

Aujourd'hui un climat d'incertitude juridique règne à Bruxelles à ce sujet. Depuis 2023, le *EU-US Data Privacy Framework* (DPF) a été adopté pour remplacer le *Privacy Shield*. Cependant, ce nouveau mécanisme a déjà suscité de nombreuses critiques et risque d'être à nouveau invalidé par la CJUE, car le DPF ne remet pas en cause les fondements des programmes de surveillance américains (FISA section 702 ou EO 12333).

En attendant l'entrée en vigueur d'un nouveau cadre juridique, les géants du tech américains, étant toujours soumis au Cloud Act, FISA 702 et EO12333, doivent, en théorie, fournir l'accès aux données aux autorités américaines, même si elles sont stockées en Europe.

En conséquence, l'Union européenne se trouve confrontée à un paradoxe : elle affirme une exigence élevée de protection des données, mais dépend structurellement d'infrastructures numériques dominées par des acteurs soumis au droit américain.

À RETENIR

Dépendances juridiques et extra-territoriales

- Au-delà des mécanismes de dépendance économiques et technologiques, **la dimension extraterritoriale de certaines lois américaines** (Cloud Act, FISA 702,USA Patriot Act, EO 12333) **agissent comme une arme juridique silencieuse.** Sous le couvert de la lutte contre le terrorisme, ces lois donnent le pouvoir légal aux autorités et services secrets américains d'accéder à des données détenues par des entreprises américaines, même si elles sont hébergées en Europe.

- Malgré la bonne volonté de l'UE de protéger les données européennes à travers le RGPD, dans les faits, **la portée de ce règlement est contrainte par les lois extraterritoriales américaines, qui peuvent le contourner**. Ce paradoxe, exacerbe la dépendance de l'UE envers les Etats Unies, étant donné que l'UE n'a pas de pouvoir sur l'infrastructure technologique. Le manque de garde-fous de ces dispositions légales américaines posent **un réel risque de confidentialité pour les données des citoyens européens**, d'autant plus que les recours manquent de transparence et de contrôle citoyen ou institutionnel du côté européen.

PARTIE II

Analyse des stratégies Françaises & Européennes

IV. Chapitre 4 : Stratégies cloud de l'Union Européenne

Cette partie se concentre sur les dynamiques relatives au développement des initiatives politiques européennes sur le cloud. L'objectif est d'identifier quelles tendances sont les plus saillantes et quels sont les facteurs qui les conditionnent.

A. Trajectoire de la politique européenne du cloud : du marché numérique à la souveraineté stratégique

Les stratégies européennes actuelles se positionnent en réponse à l'émergence d'une ère « **techno polaire** », définie par l'ascension des big tech qui atteint un stade qui leur confèrent le pouvoir de contester le statut de l'État.[50] En réponse à cela, l'Union européenne appelle à davantage de **« *digital sovereignty* »**,[51] Une souveraineté qu'elle cherche à reconquérir à travers diverses actions politiques.

Cependant, l'intérêt de l'Union européenne pour les projets liés au cloud n'est pas récent. Au cours de la dernière décennie, la Commission européenne a financé plusieurs initiatives visant à développer des solutions d'interopérabilité multi-cloud, notamment des projets tels que mOSAIC, OPTIMIS et MODAClouds[52] . Toutefois, la plupart de ces premiers efforts sont restés des prototypes de recherche de courte durée n'évoluant pas vers des infrastructures pleinement opérationnelles. Néanmoins, ces projets demeurent importants dans la mesure où ils soulignent que l'intérêt de l'UE pour le cloud doit être compris comme l'un des éléments de la gouvernance du numérique illustrant, simultanément, la nature transversale de celle-ci.

En effet, la première initiative européenne pour le cloud la *European Cloud Strategy* de 2012 fait suite au Digital Agenda for Europe établi en 2010, qui

[50] Bremmer, I. The Technopolar Moment: How Digital Powers Will Reshape the Global Order. *Foreign Affairs*, 100(6), 112–128. https://www.jstor.org/stable/27121446
[51] (Promoting EU Digital Rules: Protecting European Sovereignty: MEPs Debate - Multimédia Centre, 2024)
[52] CORDIS. Cloud Computing Service on the mOSAIC and REMICS projects. *CORDIS | European Commission*. https://cordis.europa.eu/article/id/121209-cloud-computing-service-on-the-mosaic-and-remics-projects CORDIS. MOdel-Driven Approach for design and execution of applications on multiple Clouds. *CORDIS | European Commission*. https://cordis.europa.eu/project/id/318484 ; Petcu, D. Multi-Cloud. *Proceedings of the 2013 International Workshop on Multi-Cloud Applications and Federated Clouds - MultiCloud '13*. https://doi.org/10.1145/2462326.2462328

visait à favoriser le développement d'un marché unique du numérique et à promouvoir l'adoption des technologies telles que le cloud à travers l'union européenne[53]. Dans ce contexte, le cloud était avant tout pensé comme un outil visant à stimuler la croissance économique et l'innovation plutôt qu'un mécanisme d'autonomie stratégique auquel il est de plus en plus associé depuis plusieurs années maintenant.

À cet égard, les premières initiatives de l'UE (2010-2015) peuvent être situées comme représentant une **dynamique d'adoption du cloud et de construction d'un marché numérique**. Période durant laquelle l'accent fut porté sur la suppression des obstacles réglementaires, la promotion de l'interopérabilité et des standards, ainsi que l'établissement de clauses contractuelles types et de systèmes de certification destinés à renforcer la confiance et à accélérer l'adoption du cloud. L'objectif était de renforcer la collaboration public-privé à travers notamment le *European Cloud Partnership* visant à aligner les différentes exigences en matière de marchés publics et ainsi stimuler le marché et son innovation et donc sa compétitivité. Une dynamique témoignant de l'engagement d'alors de la Commission en faveur des standards ouverts et des solutions open source[54].

Une seconde phase s'établit à la suite du **développement des infrastructures de données et de l'interopérabilité au sein de l'écosystème numérique européen** (2016–2019). En effet, durant cette période l'UE s'est attelée à relier la politique du cloud à la gouvernance des données et aux infrastructures stratégiques, notamment à travers l'initiative européenne pour le cloud et le règlement sur la libre circulation des données non personnelles. Une dynamique illustrée également par le lancement de GAIA-X, ou de la *European Data Strategy* qui reflète cet effort de l'UE à créer un écosystème propice à l'innovation qui se fonde sur les données et les infrastructures cloud[55].

La troisième phase se concentre quant à elle sur la construction d'une **souveraineté numérique** et donc d'une **autonomie stratégique** (2019–) une logique incarnée par la stratégie européenne des données, la certification EUCS[56] et l'IPCEI-CIS[57]. Illustrant l'importance grandissante du cloud en tant que secteur stratégique étroitement lié à la souveraineté

[53] A Digital Agenda for Europe. EU4Digital. https://eufordigital.eu/library/a-digital-agenda-for-europe/
[54] Brownell, P. European Commission digital agenda and cloud strategy. Opensource.com. https://opensource.com/government/13/3/eu-digital-strategy
[55] EUR-Lex - 52020DC0066. Eur-Lex.europa.eu. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066
[56] European Cybersecurity Certification Scheme for Cloud Services
[57] IPCEI Next Generation Cloud Infrastructure and Services (CIS)

technologique, à la compétitivité industrielle et à l'autonomie géopolitique**.** Par conséquent, les initiatives européennes actuelles visant à atteindre une souveraineté du cloud s'inscrivent comme partie intégrante du tournant plus large de l'Union vers la souveraineté numérique.

Au sein de ce tournant vers une souveraineté numérique les enjeux sont multiples et le cloud revêt une importance particulière à travers sa position. En effet, il constitue l'une des sept couches formant l'architecture numérique mondiale[58][59]. Le degré de maturité de ces couches dépend des capacités économiques et technologiques de chaque pays, de sorte que leur développement s'inscrit dans des rythmes et au travers de trajectoires variées. Dans ce sens, au niveau Européen ce constat se traduit par un stade de développement sensiblement supérieur de la couche réseau en comparaison avec la couche applicative (c'est-à-dire les services applicatifs finaux, notamment les plateformes numériques tel que les sites web, applications mobiles), où la faiblesse relative des capacités européennes se transcrit par une dépendance accrue envers des acteurs technologiques étrangers, tels que Google, Microsoft ou encore Amazon. La couche cloud apparaît quant à elle à un stade de développement intermédiaire avec des faiblesses et limites apparentes que nous soulignions au sein des parties précédentes.

Dans cette logique et afin de combler son retard en développant davantage cette couche cloud, l'Union Européenne combine instruments réglementaires, normalisation et politiques industrielles[60]. Ces leviers d'action se concrétisent notamment par des efforts d'harmonisation de la certification européenne en matière de cybersécurité ou encore l'AI Continent Action Plan, qui traduit l'ambition européenne de se doter d'une capacité d'entraînement de modèles d'IA compétitive à l'échelle mondiale, notamment par la création d'AI Gigafactories

Cette doctrine de **souveraineté digitale** commune à l'UE et ses États membres résulte d'un désir de **réduire leurs dépendances technologiques, développer leurs capacités économiques et renforcer le**

[58] Cette distinction en couches constitue un outil analytique destiné à cartographier des dynamiques complexes, comme pour les produits numériques concrets, au sein desquels ces couches s'interpénètrent, et leurs capacités interagissent fréquemment. Il ne s'agit donc pas d'un modèle technique au sens du modèle OSI, mais d'un instrument d'analyse géopolitique permettant de raisonner sur les politiques nécessaires à l'atteinte de la souveraineté numérique européenne
[59] Sheikh, H. European Digital Sovereignty: A Layered Approach. *Digital Society.* https://doi.org/10.1007/s44206-022-00025-z
[60] Cooper, D. EU Cloud Initiatives in 2021 and 2022. *Global Policy Watch.* https://www.globalpolicywatch.com/2021/02/eu-cloud-initiatives-in-2021-and-2022/

système de sécurité[61]. Cependant même si une volonté commune s'établit, les intérêts restent divergents et peuvent s'élever comme barrière à l'implémentation de ces politiques de souveraineté. Cette divergence qui se présente encore et toujours, est un élément indissociable de la nature intergouvernementale de l'UE.

B. Souveraineté du cloud européen, un processus trop politique ?

Ainsi, l'évolution de l'*European Cybersecurity Certification Scheme for Cloud Services* (EUCS) exemplifie **l'impact de cette lutte inter-étatique sur le développement d'une souveraineté numérique**. La première version du schéma publiée par l'Agence de l'Union européenne pour la cybersécurité (ENISA) en décembre 2020 avait pour but d'harmoniser le marché Européen en remplaçant les certifications cloud nationales et en définissant les besoins sécuritaires pour les offres cloud, favorisant ainsi l'intégration des marchés nationaux et renforçant la confiance des utilisateurs.

Mais ce n'est pas cette proposition initiale qui conduisit à un litige entre différents Etats Membres mais la clause formulée par le conseil européen suite à des consultations publiques visant à assurer que les données ne tombent pas sous des juridictions non-européennes[62] comme avec le risque que présente l'extraterritorialité américaine. Cet amendement implique que les données doivent être non seulement hébergées et traitées exclusivement au sein de l'UE mais également que les fournisseurs doivent avoir leur siège en Europe et être majoritairement possédé par des entités européennes[63] .

Son inclusion fut soutenue notamment par la France dont la certification SecNum cloud est décrite comme l'ayant inspiré ainsi que par l'Italie, l'Allemagne et l'Espagne. En parallèle de nombreux fournisseurs européens de services cloud ont également exprimé leur soutien à cette disposition, exhortant l'ENISA à « ne pas céder aux pressions ». Face à eux le Danemark, l'Estonie, la Grèce, l'Irlande, les Pays-Bas, la Pologne et la Suède en cosignant un document informel s'opposèrent ainsi à ce que l'on appelle le «

[61] Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. Digital sovereignty - Rhetoric and reality. *Journal of European Public Policy*. https://doi.org/10.1080/13501763.2024.2358984
[62] Kabelka, L. Sovereignty requirements remain in cloud certification scheme despite backlash. Euractiv.https://www.euractiv.com/news/sovereignty-requirements-remain-in-cloud-certification-scheme-despite-backlash/
[63] Technical is political: When a cloud certification scheme divides Europe. European Union Institute for Security Studies. https://www.iss.europa.eu/publications/briefs/technical-political-when-cloud-certification-scheme-divides-europe

sovereignty requirement ». Faisant valoir l'exclusion d'un trop grand nombre d'entreprises, notamment américaines, et l'introduction de critères politiques dans ce qui était censé être un système de certification technique.

Cependant, une troisième version de l'EUCS, publiée en mars 2024, a supprimé l'exigence de souveraineté, proposant de laisser la question aux régulateurs nationaux. Ce retrait fut vivement critiqué par de multiples acteurs redoutant un phénomène de certification shopping, où les fournisseurs chercheraient à obtenir la certification EUCS dans les États membres aux conditions les moins strictes, entraînant des distorsions de marché et un abaissement effectif des standards de sécurité.

Cette divergence reflète donc les **priorités stratégiques distinctes** entre les États membres, qui dans la plupart des cas, découlent directement des liens industriels mis en place au niveau domestique. Ainsi d'un côté certains États privilégient la collaboration avec les acteurs technologiques dominants tels que les hyperscalers américains. D'un autre côté, les pays adoptant une approche davantage axée sur la sécurité et la souveraineté en misant sur le développement des infrastructures numériques nationales. La France s'inscrit dans cette seconde logique, défendant des exigences strictes.[64] En septembre 2024, le Conseil de l'UE exhorté une fois de plus la Commission européenne à accélérer les progrès concernant l'adoption de l'EUCS. Mais celle-ci reste en 2026 toujours un élément de discussion et de débat comme l'illustre l'échec fin janvier, de la Direction Générale des Entreprises (DGE), des arbitrages sur un SecNum Cloud Européen[65]. Ces conflits autour de l'EUC mettent donc en lumière **les** tensions structurelles qui accompagnent la mise en œuvre de la souveraineté numérique européenne : entre objectifs collectifs, intérêts nationaux divergents et arbitrages politiques ou techniques.

Cette difficulté d'implémenter la notion de souveraineté digital des discours à des politiques concrètes peut être notamment associée à deux facteurs que les initiatives européennes exacerbent : **les conflits distributifs** entre les États membres (compétition pour les subventions, déséquilibre de ressources et distorsion du marché unique) et **les conflits horizontaux interinstitutionnels** concernant les compétences ou le "qui fait quoi"

[64] Ibid.
[65] Fléchaux, R. SecNumCloud : touché, mais pas encore coulé ? Cio-Online.com. https://www.cio-online.com/actualites/lire-secnumcloud-touche-mais-pas-encore-coule-16839.html

(contestation de l'autorité des agence, politisation vs régulation, divergences institutionnelles)[66].

C. GAIA-X : vitrine d'une souveraineté numérique plus discursive que structurelle

Le cas de GAIA-X permet de prolonger cette analyse à une initiative plus intégrée, en montrant comment la même multiplicité d'intérêts et de priorités stratégiques se traduit au niveau de la création d'une infrastructure cloud fédérée. Le projet franco-allemand GAIA-X lancé en 2019 représente le **premier effort tangible visant à établir une infrastructure cloud fédérée et européenne**, afin de garantir un contrôle local des données [67] reposant sur sept axes complémentaires.

Premièrement sur le plan technique, où le projet définit des standards ouverts d'interopérabilité pour éliminer le *vendor lock-in* [68] (dépendance fournisseur) et permettre la portabilité des données entre fournisseurs. Il adopte également un modèle de cloud fédéré intégrant différents types de services (IaaS, PaaS, SaaS) dans un réseau commun soumis à des normes européennes de sécurité. La conformité réglementaire, notamment au RGPD, est quant à elle intégrée directement dans le code (*compliance by design*). Ensuite, un système de labellisation à trois niveaux structure l'offre, le niveau le plus exigeant imposant une localisation des données en Europe et une immunité aux lois extraterritoriales.

Sur le plan institutionnel et stratégique, la gouvernance réserve le droit de vote au conseil d'administration aux seuls membres ayant leur siège en Europe, y compris face aux *hyperscalers* américains membres de l'association. Enfin, GAIA-X favorise la création d'espaces de données sectoriels (*data hubs*) comme Catena-X dans l'automobile, et s'appuie sur une logique de *coopétition* entre fournisseurs européens pour constituer une masse critique capable de rééquilibrer le rapport de force face aux géants américains et chinois [69].

---

[66] Calcara, A. European cloud computing policy: failing in Europe to succeed nationally? *West European Politics*. https://doi.org/10.1080/01402382.2025.2491962

[67] Tardieu, H. Role of Gaia-X in the European Data Space Ecosystem. *Springer EBooks*. https://doi.org/10.1007/978-3-030-93975-5_4

[68] le vendor lock-in désigne une situation dans laquelle un client tel qu'une entreprise, une administration ou un particulier devient fortement dépendant d'un fournisseur spécifique de technologies ou de services, au point qu'il lui est difficile, coûteux ou techniquement complexe de changer de prestataire.

[69] Baur, A. European ambitions captured by American clouds: digital sovereignty through Gaia-X? *Information Communication & Society*. https://doi.org/10.1080/1369118x.2025.2516545 ; Bouaynaya, W., Cloarec, J., & Bidan, M. La territorialisation européenne de la souveraineté numérique : vers une

GAÏA-X illustre également les tensions attenantes à toute tentative de souveraineté numérique collective. Ces tensions se manifestent à travers une multiplicité de récits concurrents représentant chacun une conception propre de la souveraineté numérique. Ainsi six récits dominants sont identifiés au sein du projet :

- l'autonomie stratégique,
- la cybersécurité
- le néomercantilisme
- le cosmopolitisme de marché
- la protection de la vie privée
- et la propriété des données

Leur coexistence traduit l'impossibilité de réduire GAIA-X à une logique unique, le projet incarnant simultanément des ambitions territoriales et post-territoriales de souveraineté [70].

Ils **éclairent ainsi la manière dont la souveraineté numérique a géopolitisé le marché unique numérique européen**. Inscrivant dans le même temps, le concept de souveraineté numérique comme un discours à caractère performatif répondant aux évolutions économiques et technologiques et une notion dont les usages politiques successifs contribuent à constituer le champ politique et réglementaire qu'elles prétendent décrire.

Ces récits soulignent donc la difficulté d'atteindre une souveraineté du cloud tout en conciliant les intérêts des différents acteurs/États membres. Des limites que Baur (2025) confirme en montrant que GAIA-X, bien qu'initialement lancé pour contester la domination des fournisseurs cloud non-européens, les a paradoxalement incorporés en son sein. Soulevant en ce sens des interrogations profondes sur la capacité du projet à faire réellement progresser la souveraineté numérique en Europe.

Pour autant, malgré un échec à produire une infrastructure pleinement souveraine, la contribution de l'initiative est à nuancer. En effet, GAIA-X n'est pas forcément synonyme d'absence de résultats. L'initiative a contribué à

autonomie stratégique par coopétition. *Management International*. https://doi.org/10.59876/a-8jv2-9kyc ; Calcara, A. European cloud computing policy: failing in Europe to succeed nationally? *West European Politics*. https://doi.org/10.1080/01402382.2025.2491962

[70] Adler-Nissen, R., & Kristin Anabel Eggeling. The Discursive Struggle for Digital Sovereignty: Security, Economy Rights and the Cloud Project Gaia-X. *Journal of Common Market Studies*. https://doi.org/10.1111/jcms.13594

l'émergence d'une stratégie de standardisation des pratiques techniques avec une diversification des applications chez les fournisseurs cloud européens. La logique de coopétition que le projet incarne s'apparente également davantage à une autonomie stratégique du numérique qu'à une souveraineté au sens strict. **En substance, GAIA-X a davantage réussi à redéfinir les termes du débat et à structurer un espace de coopération inter-industriel qu'à produire une alternative opérationnelle aux hyperscalers américains.**[71] Cette dynamique se confirme en 2025 avec l'expansion de plus de 180 espaces de données, signe d'une maturité progressive, mais dont l'apport en termes de souveraineté reste encore à démontrer.

Ce décalage entre ambition collective et réalisation concrète au niveau européen invite à déplacer le regard vers l'échelle nationale. Car si GAÏA-X illustre les difficultés d'une souveraineté cloud construite à l'échelle de l'Union, certains États membres ont quant à eux su tirer parti de ces initiatives européennes pour avancer sur leurs propres objectifs stratégiques. Appelant dans ce sens à s'interroger sur les dynamiques opérantes entre l'échelle européenne, où les ambitions collectives peinent à se concrétiser, et l'échelle nationale, où certains États membres parviennent à valoriser ces mêmes initiatives à leur propre profit

D. Un échec Européen mais un succès national ?

Les difficultés à mettre en œuvre cette souveraineté digitale ne sont pas forcément pénalisantes pour les États membres au niveau individuel. C'est la lunette théorique que développe Calcara (2025)[72] dans son analyse des politiques européennes de cloud. Positionnant les Etats Membres comme utilisant stratégiquement les avancées réalisées au niveau européen (même incomplètes et non résolues) pour protéger et promouvoir leurs propres écosystèmes cloud nationaux. **Ainsi au lieu de conduire à plus d'intégration, l'échec au niveau de l'UE est conçu pour mener au succès national.**

Cette lecture renouvelle l'interprétation des blocages observés tout au long de ce rapport. Elle **invite à ne plus lire les conflits distributifs et interinstitutionnels identifiés dans les parties précédentes comme de**

[71] Bouaynaya, W., Cloarec, J., & Bidan, M. La territorialisation européenne de la souveraineté numérique : vers une autonomie stratégique par coopétition. *Management International*. https://doi.org/10.59876/a-8jv2-9kyc

[72] Calcara, A. European cloud computing policy: failing in Europe to succeed nationally? *West European Politics*. https://doi.org/10.1080/01402382.2025.2491962

simples obstacles à l'intégration, mais comme le reflet d'une logique nationale délibérée.
A travers son analyse empirique, il identifie trois mécanismes éclairant les moyens par lesquels les initiatives européennes bénéficient aux États membres analysés :

- **Certifications cloud :** des dispositifs à l'échelle de l'UE (comme l'EUCS) sont conçus pour compléter plutôt que remplacer les règles nationales. Cela crée un socle réglementaire commun qui oblige les hyperscalers américains à s'adapter, les conduisant souvent à former des coentreprises ou à conclure des accords de licence avec des entreprises nationales afin de satisfaire aux exigences de sécurité (par exemple, le consortium français « Bleu » impliquant Microsoft, Capgemini et Orange).

- **Politique industrielle** : des cadres comme les Projets Importants d'Intérêt Européen Commun (PIIEC / IPCEI) permettent aux États de contourner les règles strictes de concurrence et d'accorder **des aides d'État massives à leurs entreprises nationales**. Calcara (2025) souligne que la France et l'Allemagne dominent ces projets, accueillant respectivement 25 et 22 projets cloud, **utilisant ainsi le label européen pour financer leurs champions nationaux.**

- **Négociation bilatérale** : la pression combinée de la régulation et des financements européens renforce la position de négociation individuelle des États membres. Plutôt que d'exclure les géants américains, les États membres utilisent l'effet de levier de l'UE pour attirer d'importants investissements privés (ex. les 7,8 milliards d'euros d'Amazon et les 3,2 milliards d'euros de Microsoft en Allemagne) tout en maintenant un contrôle national.[73]

Ces mécanismes résonnent directement avec les récits néo-mercantilistes et sur l'autonomie stratégique identifiés par Adler-Nissen & Eggeling (2024). Ainsi loin de conduire à une architecture cloud véritablement souveraine à l'échelle continentale, ces initiatives servent avant tout d'instrument de positionnement pour des États membres aux intérêts industriels divergents.

La France en constitue l'illustration la plus nette : en réponse aux exigences de souveraineté formulées par les autorités françaises, Google Cloud a noué un partenariat avec Thales (projet S3NS), compatible avec la certification

[73] Ibid.

SecNum Cloud, tandis qu'Orange et Atos ont annoncé des partenariats stratégiques avec respectivement Google Cloud et AWS.

Le gouvernement français a annoncé un plan de 1,8 milliard d'euros pour soutenir les projets nationaux dans l'industrie cloud. En d'autres termes, il peut être avancé que **la rhétorique de souveraineté européenne sert ici de levier pour obtenir des concessions de la part des hyperscalers américains et ainsi rapatrier une partie de la valeur vers les acteurs nationaux et cela sans pour autant mettre fin à la dépendance structurelle**. L'Allemagne suit une logique similaire, ayant investi plus de 3 milliards d'euros dans l'infrastructure cloud d'Oracle, et Deutsche Telekom s'associant à Google Cloud via T-Systems pour offrir des services cloud souverains au secteur public allemand.

Le cas tchèque, offre quant à lui un contre-exemple révélateur des trajectoires nationales divergentes au sein de l'Union. En Tchéquie, le terme de « souveraineté numérique » est absent des principaux documents programmatiques des deux derniers gouvernements, malgré la place centrale accordée à la numérisation[74]. Il n'apparaît dans aucun discours majeur des dirigeants tchèques ni dans les débats parlementaires. Pour autant, le gouvernement tchèque, qui regardait initialement la souveraineté numérique avec suspicion, la percevant comme une forme de protectionnisme numérique opposé à sa tradition de libre-échange et son attachement au partenariat transatlantique a progressivement adopté une approche plus pragmatique. Cette adoption s'est déroulée à travers un processus d'adaptation sélective, résultat de l'interaction de différents récits sur la souveraineté numérique, se produisant principalement hors de la sphère publique[75]. **La Tchéquie illustre ainsi comment un État membre peut s'approprier les instruments européens (financements, certifications, politiques industrielles) sans en adopter le vocabulaire souverainiste, tout en avançant sur ses propres objectifs de modernisation numérique**. Cet exemple souligne ainsi comment ces états souffrant d'un désavantage structurel [76] naviguent entre contraintes européennes et priorités nationales.

[74] Šitera, D., & Eberle, J. Diluting digital sovereignty: Czechia's quiet selective adaptation to EU digital politics. *Journal of Contemporary European Studies*. https://doi.org/10.1080/14782804.2025.2549578
[75] Ibid.
[76] Les petits États et les économies de marché dépendantes d'Europe centrale et orientale (ECO) sont généralement des « preneurs » plutôt que des « façonneurs » du discours de l'UE, ce qui rend leurs réponses réactives plutôt que proactives.

En conclusion, loin de représenter de simples échecs, **les initiatives européennes de souveraineté cloud constituent un espace de négociation structuré dans lequel chaque État membre cherche à maximiser ses gains nationaux**. Ce constat invite à reconsidérer le sens même du « succès » ou de l'« échec » dans ce domaine : ce qui apparaît comme une impasse collective au niveau européen peut simultanément constituer un levier efficace d'autonomie stratégique pour certains États membres. Cela à condition d'en avoir la volonté politique et les capacités industrielles pour en tirer parti.

À RETENIR

Stratégies cloud de l’Union Européenne

- Ainsi, les dynamiques analysées dans ce chapitre dessinent un **tableau cohérent mais paradoxal de la politique cloud européenne.** L'Union européenne a progressivement construit, sur plus d'une décennie, un arsenal de leviers réglementaires, industriels et normatifs visant à reconquérir une forme de souveraineté du cloud. Pourtant, les deux cas d'étude retenus que sont l'EUCS et GAIA-X révèlent que cette ambition collective bute systématiquement sur la même réalité : la divergence des intérêts nationaux qui transforme chaque initiative européenne en **arène de négociation interétatique** avant même qu'elle ne puisse produire ses effets.

- Ce constat ne signifie pas pour autant l'échec total du projet européen, il invite plutôt à **changer la perspective analytique**. En effet, les initiatives que l'Europe peine à achever collectivement, certains États membres parviennent à en extraire un **bénéfice stratégique individuel**, en utilisant les cadres européens comme levier de négociation vis-à-vis des *hyperscalers* américains et comme justification et soutien pour leurs politiques industrielles nationales.

V. Chapitre 5 : Stratégie nationale pour le Cloud

En déclarant lors du Sommet pour l'action sur l'IA de février 2025[77] qu'il "*veut en être*", le Président de la République a confirmé l'ambition française de peser dans la compétition technologique mondiale. Cette posture s'appuie sur un engagement d'**investissement de 109 milliards d'euros** "*dans les prochaines années*"[78] annoncé à l'occasion de cet événement, ainsi que sur une stratégie cloud multisectorielle dont les fondements ont été posés dès 2021. Cette partie analyse les deux piliers normatifs de cette stratégie – **le label Cloud de Confiance** adossé au référentiel SecNumCloud, et **la doctrine « Cloud au Centre »** – en évaluant leur cohérence, leurs tensions internes et leurs limites opérationnelles.

A. Le Label Cloud de Confiance et SecNumCloud : instruments normatifs de la souveraineté numérique

1. Le label de Cloud de confiance

Le terme "Cloud de Confiance" définit une infrastructure privée qui s'appuie sur un de ces trois modèles technologiques : IaaS, PaaS ou SaaS. Cette appellation « Cloud de Confiance » définit une approche politique et stratégique des infrastructures d'hébergement des données sensibles de l'État ou d'acteurs privés. **L'enjeu central de ce label est la protection contre l'extraterritorialité du droit**. L'affaire des données de santé françaises hébergées sur les infrastructures Microsoft Azure illustre concrètement cette vulnérabilité, si bien que la CNIL a dénoncé les risques juridiques dès 2021.

[77] Présidence de la République. *Dossier de presse — Sommet pour l'action sur l'intelligence artificielle, 6-11 février 2025.* Élysée, 2025,
[78] Ibid.

Le label de cloud de confiance impose aux prestataires labellisés plusieurs contraintes cumulatives :

- Des contraintes géographiques : l'infrastructure doit être opérée par un acteur public ou privé européen sans lien juridique avec un pays tiers.
- Une infrastructure solide basée sur un système de redondance complet pour assurer une continuité et une résilience dans le service, tout en permettant de résister aux attaques par déni de service (DDOS).
- Des logiciels efficaces assurant la protection des données, notamment grâce à des solutions de chiffrement des données au repos (stockées sur un serveur)

En outre, ces trois modèles (IaaS, PaaS, SaaS) garantissent la sécurité des données hébergées tout en restant soumis à la réglementation et aux normes françaises et européennes, que ce soit en matière d'hébergement, ou de protection des données (RGPD), le tout dans une optique de souveraineté numérique de l'État.

2. Référentiel SecNumCloud

À l'instar du label Cloud de confiance, **le référentiel SecNumCloud** développé et délivré par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), constitue **un visa de sécurité pour les prestataires de services cloud.**

Ce visa n'est pas une simple attestation, mais une qualification obtenue après un processus d'audit rigoureux conduit par des organismes certificateurs agréés par l'ANSSI. **Il garantit que l'infrastructure cloud du prestataire répond aux exigences de sécurité nécessaires pour héberger les données sensibles des administrations et des entreprises stratégiques françaises et européennes.**

Le référentiel SecNumCloud, couvre l'ensemble du cycle de vie des données hébergées et impose des obligations strictes dans plusieurs domaines :

- Sécurité technique : chiffrement des données au repos et en transit, isolation des environnements clients, architecture résiliente contre les attaques ;

- Gestion de crise et cyberattaques : capacité à détecter, contenir et répondre aux incidents de sécurité, plan de continuité d'activité (PCA) et plan de reprise d'activité (PRA) ;

- Contrôle du matériel (hardware) : traçabilité complète des équipements, localisation physique des serveurs en France ou dans l'Union européenne ;

- Politique de recrutement : habilitations de sécurité pour le personnel ayant accès aux données sensibles, vérification des antécédents ;

- Gouvernance et conformité : documentation exhaustive des processus, audits réguliers, transparence sur les sous-traitants.

Cette exhaustivité vise "un objectif de protection des données du commanditaire, mais n'apporte pas de garanties techniques fortes contre un accès du prestataire aux données traitées sur le système d'information du service, uniquement des engagements contractuels" (ANSSI). C'est une nuance fondamentale pour évaluer la robustesse réelle du dispositif. SecNumCloud est un visa de sécurité qui fait promettre au prestataire de ne pas accéder aux données du client, même s'il n'existe aucune contrainte technique quant à leur obtention[79].

a. Sécurité technique ou souveraineté stratégique

SecNumCloud crée des divergences dans le développement de la stratégie cloud française, notamment dans la différenciation entre la sécurité technique et souveraineté stratégique. En effet, ce débat reflète une tension fondamentale dans la stratégie cloud française : faut-il privilégier la sécurité technique (garantie par SecNumCloud) ou la souveraineté stratégique (favorisant les acteurs purement français ou européens) ?

[79] Agence nationale de la sécurité des systèmes d'information. (2022, 8 mars). *Prestataires de services d'informatique en nuage (SecNumCloud) — Référentiel d'exigences* (Version 3.2). ANSSI. https://www.ssi.gouv.fr

Les partisans d'une approche pragmatique comme Vincent Courbin, directeur de projet interministériel de la DINUM, estiment que les partenariats avec des acteurs américains, encadrés par SecNumCloud, permettent d'**accéder à des technologies de pointe** tout en bénéficiant de **garanties de sécurité**. Les défenseurs d'une souveraineté stricte, comme l'entrepreneur Tarik Krim[80], considèrent au contraire que cette approche **crée une dépendance structurelle** et **affaiblit la capacité** de la France à **contrôler ses infrastructures numériques critiques**. Position rejointe par les conclusions du rapport Longuet de la commission sur la souveraineté numérique au Sénat en 2019[81] qui statue sur une meilleure articulation des acteurs publics et privés en faveur d'une souveraineté numérique stricte.

b. Place de la sensibilité de la donnée

La stratégie cloud de l'État repose sur une prémisse fondamentale : toutes les données publiques ne se valent pas et n'appellent pas le même niveau de protection. La qualification de la sensibilité des données constitue une pierre angulaire dans la construction du label SecNumCloud.

La sensibilité d'une donnée est caractérisée selon plusieurs critères cumulatifs. Le premier est la nature intrinsèque de l'information : le RGPD identifie des catégories particulières de données dont le traitement est par principe interdit sauf dérogation explicite : données de santé, données biométriques, données révélant l'origine ethnique, les convictions religieuses ou les opinions politiques. Le second critère est le contexte de production et d'usage : une donnée anodine en apparence peut devenir sensible dès lors qu'elle est produite dans un cadre régalien, qu'elle permet d'identifier un agent public ou qu'elle est susceptible de nuire à la continuité de l'action de l'État si elle était compromise. Le troisième critère, propre à l'administration française, est la classification de sécurité : le cadre interministériel de protection du secret distingue les informations non protégées, les informations sensibles et les informations classifiées (Confidentiel Défense, Secret Défense), chacune relevant d'un régime juridique et technique distinct. C'est à l'articulation de ces trois niveaux que la doctrine Cloud au Centre opère sa graduation.

L'hébergement de données sensibles dans des infrastructures cloud soulève un **risque d'exposition juridique et technique** que la stratégie nationale cherche à endiguer. Comme vu précédemment, le risque

[80] Krim, Tariq. *Lettre à ceux qui veulent faire tourner la France sur l'ordinateur de quelqu'un d'autre : Requiem pour la souveraineté numérique.* Cybernetica, 2021,
[81] Longuet, Gérard. *Le devoir de souveraineté numérique.* Rapport n° 7 (2019-2020), fait au nom de la commission d'enquête, Sénat, 1er oct. 2019

juridique est celui de l'extraterritorialité. Le risque technique, lui, est celui de la compromission : une infrastructure mal isolée, un personnel insuffisamment habilité ou une chaîne de sous-traitance opaque et/ou étrangères (cf. Chapitre 2) peuvent ouvrir des vecteurs d'accès non autorisés aux données les plus critiques.

c. Limites opérationnelles du référentiel SecNumCloud

Enfin, au-delà des questions de souveraineté, le référentiel SecNumCloud fait face à des objections d'ordre opérationnel. Nombreuses sont les critiques formulées autour de l'obtention du visa. Le processus, **estimé entre 18 et 36 mois**, est trop long, et les **frais d'audit** peuvent dépasser les **200 000 euros**. Cette barrière bloque les PME et les ETI dans leur obtention et réduit le nombre de prestataires qualifiés à certains groupes (Orange, Dassault ou Capgemini), malgré les dispositifs d'accompagnement, dont notamment plusieurs appels à projets comme AMI (appel à manifestation d'intérêt), ainsi que l'accompagnement des 27 entreprises à l'obtention du visa SecNumCloud, proposé par la Direction générale des entreprises et le ministère des Finances.

B. Cloud au Centre

1. Contenu et portée de la doctrine

La doctrine Cloud au Centre, publiée en mai 2021 dans la circulaire du Premier ministre n° 6282/SG relative à la doctrine d'utilisation de l'informatique en nuage par l'État, pose un nouveau principe directeur : toute **nouvelle solution numérique** développée ou achetée par l'État **doit être hébergée sur une infrastructure cloud.** Le Cloud devient alors le mode d'hébergement et de production par défaut des services numériques de l'État.

Cette doctrine fait de la sécurité des données son cheval de bataille, et établit une hiérarchisation des solutions cloud en fonction du niveau de sensibilité des informations détenues :

- Cloud interne de l'État (Cloud PI du ministère de l'intérieur et Cloud NUBO du ministère des finances) : pour les données les plus sensibles ou dont la compromission nuirait au bon fonctionnement des administrations régaliennes.
- Cloud qualifié par le visa SecNumCloud : pour des administrations avec des données sensibles.
- Clouds commerciaux (Onedrive, Google Drive, Amazon web services...) : utilisés pour des projets portant des données jugées non sensibles.

2. Objectifs et enjeux stratégiques

a. Transformation numérique

Cette doctrine a plusieurs enjeux sous-jacents mais qui restent stratégiques dans le développement numérique de la France. D'abord, cette doctrine se place dans une volonté d'**accélération de la transformation numérique** de l'État. Le cloud joue ici un rôle de **facilitateur structurel** dans la mise en place de nouvelles solutions numériques comme l'Assistant IA (cf. 4.3.1). Le cloud permet un développement plus rapide dans la mise en place de nouveaux outils numériques au sein des administrations. En effet, si pour un acteur privé comme une PME, le cloud est une solution coûteuse et peu ergonomique, à l'échelle de l'administration, l'aide à la mise en place de solutions cloud permet de répondre à un besoin matériel grandissant pour l'hébergement d'outils numériques, tout en garantissant des standards de qualité et de sécurité.

b. Souveraineté et sécurité

La doctrine Cloud au Centre s'inscrit dans une logique de protection de l'État autour de la conformité juridique et la préservation de la souveraineté numérique.

Sur le plan du droit, l'hébergement et le traitement des données publiques sont soumis au RGPD. La défaillance d'une administration dans la maîtrise de ses données est susceptible d'une sanction de la CNIL ou de l'ANSSI, prenant souvent la forme d’une amende.

Sur la question de la souveraineté, des défis structurels sont en jeu. En vue des risques d'extraterritorialité des données, **la doctrine Cloud au centre conditionne le traitement des données les plus sensibles** aux opérateurs SecNumCloud pour garantir un contrôle quant à la fuite de données par des ingérences étrangères.

c. Enjeu industriel

Au-delà de sa dimension défensive, la doctrine Cloud au centre s'affirme comme un instrument de politique industrielle en lien avec le plan France 2030 et l'initiative européenne GAIA-X. **Le gouvernement oriente** la commande publique vers **des acteurs cloud français ou européens** qualifiés sur le plan national, et accélère ainsi le développement technologique des entreprises françaises en vue de réduire l'écart avec les hyperscalers américains.

L'objectif poursuivi est double. Il s'agit, d'une part, de **renforcer la capacité des prestataires français** à se positionner sur un marché européen en forte expansion (estimé à plusieurs milliards d'euros à l'horizon 2030). D'autre part, cette dynamique doit permettre aux administrations publiques de **bénéficier d'une offre de services cloud performante, de qualité et conforme aux obligations légales.**

Cloud au centre articule ainsi **une logique de réciprocité** entre intérêt public et développement industriel : **la modernisation de l'État** aide au **développement du marché cloud souverain**, tandis que **la montée en qualité de cette filière** renforce en retour **les capacités numériques de l'administration française.**

3. L'État face aux géants du numérique

Le développement d'outils numériques souverains : l'État comme opérateur cloud

La mise en œuvre de la doctrine Cloud au Centre suppose, pour être crédible, que l'État dispose de ses propres solutions numériques conformes aux exigences SecNumCloud qu'il impose à ses prestataires. Dans cette logique, la DINUM a progressivement constitué une suite d'outils interministériels souverains, messagerie sécurisée (Tchap), espace collaboratif (Resana), visioconférence (Webinaire de l'État), suite bureautique (La Suite Numérique), hébergés sur des infrastructures qualifiées, réduisant la dépendance de l'administration vis-à-vis des grands éditeurs étrangers.

C'est toutefois dans **le domaine de l'intelligence artificielle générative** que cet effort prend sa dimension la plus **stratégique**. La stratégie sous-jacente émane d'une vision technologique ambitieuse pour l'administration : s'approprier une technologie nouvelle et prometteuse pour ne pas la subir, et **assurer la souveraineté numérique de l'État.** Initié par le département Etalab de la DINUM, le projet Albert concrétise cette ambition : présenté le 23 avril 2024 par le Premier ministre Gabriel Attal, il s'agit d'une IA générative souveraine, développée pour accélérer les formalités administratives et apporter des réponses sûres, claires et efficaces aux agents et usagers des services publics. Sur le plan technique, selon la sensibilité des données traitées, Albert peut être hébergé sur un cloud sécurisé (SecNumCloud), sur un cloud public ou sur un serveur local, ce qui le rend pleinement **compatible avec la graduation des niveaux de protection** prévue par la doctrine Cloud au centre.

Pour industrialiser l'accès à ces capacités, l'État a développé l'Albert API : une interface standardisée qui permet aux administrations d'interroger les modèles de langage sans avoir à déployer leur propre infrastructure de calcul. Ce dispositif est coordonné dans le cadre du programme ALLiaNCE, animé par le département Intelligence artificielle dans l'État (IAE) de la DINUM, qui propose un socle interministériel d'IA générative — traduction automatique, agents conversationnels, assistance au codage, traitement d'image – en accompagnant innovateurs publics, décideurs et spécialistes du numérique dans leurs démarches d'adoption.

L'étape la plus décisive de cette trajectoire est le lancement de **l'assistant IA** interministériel. Le choix de Mistral AI comme partenaire technologique est révélateur de la logique à l'œuvre : en retenant un acteur français et européen de premier rang, l'État opère une distinction explicite avec les hyperscalers américains, cohérente avec l'esprit de la stratégie cloud nationale. Toutefois, ce choix illustre également toute la complexité de la stratégie cloud nationale : comme souligné précédemment, l'émancipation algorithmique offerte par Mistral AI reste intrinsèquement liée aux infrastructures matérielles américaines nécessaires à son développement. La feuille de route numérique du ministère chargé de la Fonction publique pour 2026 confirme cette orientation, avec un accent sur l'industrialisation et le déploiement massif de l'IA souveraine, accompagné d'un repositionnement de la DINUM comme architecte technique de l'État. Cette expérimentation, qui implique 10 000 agents de la fonction publique, constitue le test grandeur nature de la capacité de l'État à déployer, à l'échelle, une IA générative conforme aux exigences de la doctrine cloud.

Le soutien à l'écosystème industriel du numérique de confiance

La stratégie nationale cloud ne saurait produire ses effets si l'offre nationale qualifiée demeure insuffisante pour répondre aux besoins des administrations. Le troisième pilier de cette stratégie répond précisément à cette contrainte, en cherchant à élargir et approfondir l'écosystème des prestataires éligibles à la commande publique souveraine.

En mars 2024, l'État a accompagné **27 nouvelles entreprises** dans leur démarche de qualification SecNumCloud 3.2, portant à **48** le nombre total de startups et PME engagées dans ce processus de montée en compétence cyber, pour un budget mobilisé de **9 millions d'euros**[82]. L'objectif affiché est double : élever le niveau de sécurité des offres SaaS et PaaS françaises et accroître la diversité des solutions qualifiées disponibles pour les administrations. La DINUM a par ailleurs publié une liste des services cloud prioritaires dont l'État a besoin, offrant aux fournisseurs qualifiés SecNumCloud une visibilité sur les débouchés garantis en cas de développement conforme aux besoins exprimés.

Sur le plan des achats publics, les résultats de cette politique commencent à être mesurables. Depuis l'application de la doctrine cloud, l'État a dépensé 132 millions d'euros en cumulé, avec une **progression de 50 %** des achats cloud entre 2023 et 2025, couvrant plus de **300 entités** et **1 000 projets**. Ces chiffres attestent d'une transformation réelle des pratiques d'achat, même si la part des acteurs souverains dans ce total reste un enjeu de politique publique ouvert[83].

[82] Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique / Direction générale des Entreprises. « France 2030 : la stratégie nationale cloud s'enrichit d'un nouvel appel à projets pour renforcer l'offre française et européenne de services cloud au profit de la souveraineté numérique et de l'IA. » *Presse Économie*, mars 2024.
[83] Ministère de l'Économie et des Finances, Direction générale des Entreprises, Direction interministérielle du numérique, & Agence nationale de la sécurité des systèmes d'information. *France 2030 : la stratégie nationale cloud s'enrichit d'un nouvel appel à projets.* Mars 2024.

Stratégie nationale pour le Cloud

À RETENIR

- En conclusion, la France a structuré sa stratégie cloud autour de deux instruments complémentaires: **le label Cloud de Confiance** adossé au **référentiel SecNumCloud**, et la **doctrine « Cloud au Centre »**. Le premier constitue un visa de sécurité rigoureux, délivré par l'ANSSI après audit, visant à protéger les données sensibles des administrations contre les risques d'extraterritorialité du droit. Le second, institué par la circulaire de mai 2021, impose le cloud comme mode d'hébergement par défaut des systèmes d'information de l'État, selon une graduation des niveaux de protection proportionnelle à la sensibilité des données.

- Cette architecture normative poursuit **trois objectifs stratégiques imbriqués** : accélérer la transformation numérique de l'administration, garantir la conformité juridique au RGPD, et stimuler le développement d'une filière industrielle souveraine en lien avec France 2030. Pour crédibiliser ces ambitions, la DINUM a engagé le déploiement d'une suite d'outils interministériels souverains tandis que l'État accompagne des entreprises dans leur qualification SecNumCloud.

- Ce dispositif se heurte néanmoins à des limites structurelles : le processus de qualification SecNumCloud, estimé entre 18 et 36 mois et pouvant dépasser 200 000 euros en frais d'audit, constitue une barrière à l'entrée défavorable aux PME ; par ailleurs, la tension non résolue entre sécurité technique et souveraineté stricte fragilise la cohérence doctrinale de l'ensemble. **Des arbitrages politiques clairs restent nécessaires pour déterminer si la France entend défendre une souveraineté numérique de principe ou une sécurité pragmatique adossée à des hyperscalers américains** (Microsoft, Amazon, et cætera...)

PARTIE III

Risques et Vulnérabilités

VI. Cartographie de la vulnérabilité

A. Définition de la vulnérabilité à la lumière du cloud

La vulnérabilité peut être appréhendée comme la combinaison d'une exposition à un aléa ou à un ensemble de menaces et d'une capacité insuffisante à contrôler, absorber ou atténuer les effets de cet aléa. Le GIEC définit ainsi la vulnérabilité comme une prédisposition à être affecté, incluant explicitement un déficit de capacité à faire face et à s'adapter (*lack of capacity to cope and adapt*)[84]. L'United Nations Office for Disaster Risk Reduction (UNDRR) propose une terminologie reliant la vulnérabilité aux conditions qui accroissent la susceptibilité aux impacts et à la capacité (ou l'absence de capacité) de réponse (*coping capacity*)[85]. Cette approche est cohérente avec des cadres opérationnels du risque qui distinguent mais articulent aléas, exposition, vulnérabilité et capacité, en conceptualisant le risque comme une fonction de ces composantes[86].

Appliquée au numérique public, cette grille conduit à définir la vulnérabilité comme une exposition à des risques (techniques, contractuels, juridiques, géopolitiques) couplée à une faible capacité de mitigation, particulièrement lorsque l'État dépend d'un fournisseur ou d'un écosystème propriétaire. Les obstacles techniques, contractuels et financiers à la migration (interopérabilité limitée, complexité de sortie, coûts de transfert de données) réduisent concrètement la capacité de substitution et de maîtrise du risque[87].

Ainsi, cette analyse tentera de questionner la vulnérabilité de la doctrine française « Cloud au centre » qui consacre le cloud comme mode

[84] Intergovernmental Panel on Climate Change. (2022). Climate change 2022: Impacts, adaptation and vulnerability—Summary for policymakers (AR6 WGII). https://www.ipcc.ch/report/ar6/wg2/downloads/report/IPCC_AR6_WGII_SummaryForPolicymakers.pdf

[85] United Nations Office for Outer Space Affairs. (n.d.). Disaster risk management. United Nations Platform for Space-based Information for Disaster Management and Emergency Response (UN-SPIDER). Retrieved May 11, 2026, from UN-SPIDER – Disaster Risk Management

[86] United Nations Office for Disaster Risk Reduction. (n.d.). *Vulnerability*. UNDRR terminology. Retrieved May 11, 2026, from UNDRR – Vulnerability

[87] Autorité de la concurrence. (2023). *Avis n° 23-A-08 relatif au fonctionnement concurrentiel du marché de l'informatique en nuage (cloud)*. https://www.autoritedelaconcurrence.fr/fr/avis/relatif-au-fonctionnement-concurrentiel-de-linformatique-en-nuage-cloud & OECD. (2025). *Cloud computing and public procurement: Sovereignty, competition and switching costs*. Organisation for Economic Co-operation and Development.

d'hébergement par défaut pour les nouveaux services et les évolutions substantielles, ce qui tend à élargir l'exposition potentielle à l'échelle de l'État[88]. Pour les données sensibles, l'État articule toutefois cette orientation avec une exigence renforcée de sécurité et de confiance via la qualification SecNumCloud, délivrée par l'ANSSI.[89].

B. Typologie de vulnérabilités

1. **Juridique / souveraineté :** exposition à des législations extraterritoriales et régimes d'accès aux données ; la stratégie nationale cloud explicite ce risque et l'objectif d'"application exclusive du droit européen" pour le "cloud de confiance". La vulnérabilité juridique et de souveraineté renvoie à l'exposition à des régimes d'accès aux données et à des normes extraterritoriales susceptibles de contraindre un prestataire ou un écosystème, ce qui motive, en France, l'objectif d'"application exclusive du droit européen" au cœur du "cloud de confiance" (Ministère de l'Économie, des Finances et de la Relance, 2021 ; U.S. Congress, 2018). Elle est explicitement prise en charge, sur le plan des exigences, par la qualification SecNumCloud, conçue notamment pour renforcer la résilience d'un service cloud face à une possible injonction fondée sur l'extraterritorialité et intégrant des exigences techniques, opérationnelles et juridiques.

2. **Économique / dépendance de marché** : concentration, pouvoir de négociation, pratiques tarifaires qui augmentent les coûts de sortie (*egress fees*) et rendent le multi-cloud difficile. La vulnérabilité économique tient à la concentration des marchés, à l'asymétrie de pouvoir de négociation et à des pratiques tarifaires qui renchérissent la sortie, au premier rang desquelles les *egress fees* (frais de transfert de données sortant), identifiées comme une préoccupation majeure parce qu'elles peuvent freiner la mobilité et compliquer le multi-cloud[90].

[88] DINUM. (2021, 15 septembre). *Note relative à la doctrine cloud de l'État : conformité des suites collaboratives.* Direction interministérielle du numérique. & Premier ministre. (2021, 5 juillet). Circulaire n° 6282-SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État (« cloud au centre »). Légifrance. https://www.legifrance.gouv.fr/circulaire/id/45205
[89] (Agence nationale de la sécurité des systèmes d'information [ANSSI], source, source)
[90] Autorité de la concurrence. (2023). *Avis n° 23-A-08 relatif au fonctionnement concurrentiel du marché de l'informatique en nuage (cloud).* https://www.autoritedelaconcurrence.fr/fr/avis/relatif-au-fonctionnement-concurrentiel-de-linformatique-en-nuage-cloud & OECD. (2025). *Cloud computing and public procurement: Sovereignty, competition and switching costs.* Organisation for Economic Co-operation and Development.

3. **Technique (lock-in)** : interopérabilité limitée, APIs propriétaires, orchestration *vendor-specific* → portabilité réduite, fragmentation du multi-cloud. La vulnérabilité technique (lock-in) recouvre les limites d'interopérabilité et de portabilité (APIs propriétaires, dépendances à des services managés, orchestration spécifique), qui tendent à fragmenter le multi-cloud et à réduire la capacité de substitution ; ces enjeux sont au cœur des recommandations visant à améliorer l'interopérabilité et la portabilité pour éviter un enfermement structurel[91].

4. **Opérationnelle / résilience** : indisponibilités, sinistres, continuité d'activité, reprise après incident (à annoncer ici, mais à traiter en cas d'étude en III). La vulnérabilité opérationnelle recouvre les risques d'indisponibilité, de sinistres et de défaillances de continuité (PCA/PRA), qui doivent être distingués des seules questions cyber : la portabilité ne remplace pas la résilience, mais la complète[92].

5. **Stratégique** : "client captif" quand la doctrine d'achat et la standardisation interne (outils, formats, licences, cloud) rendent l'État dépendant. Enfin, la vulnérabilité **stratégique** correspond à la situation de **"client captif"** lorsque l'accumulation de dépendances (standards internes, formats, licences, services critiques) transforme un choix technique initial en dépendance durable ; cette dynamique est cohérente avec les constats sur les obstacles au switching et les verrouillages qui limitent la contestabilité du marché[93]. Cette matrice a l'avantage de rendre comparables, d'un secteur à l'autre, les vulnérabilités de l'État, et de préparer l'analyse de la doctrine « **Cloud au centre** » : en faisant du cloud le **mode d'hébergement par défaut**, elle peut mécaniquement étendre l'exposition, tout en imposant des exigences renforcées pour les données sensibles via l'architecture de confiance et la qualification[94].

[91] OECD. (2025). *Cloud computing and public procurement: Sovereignty, competition and switching costs*. Organisation for Economic Co-operation and Development.
[92] OECD. (2025). *Cloud computing and public procurement: Sovereignty, competition and switching costs*. Organisation for Economic Co-operation and Development.
[93] Autorité de la concurrence. (2023). *Avis n° 23-A-08 relatif au fonctionnement concurrentiel du marché de l'informatique en nuage (cloud)*. https://www.autoritedelaconcurrence.fr/fr/avis/relatif-au-fonctionnement-concurrentiel-de-linformatique-en-nuage-cloud & OECD. (2025). *Cloud computing and public procurement: Sovereignty, competition and switching costs*. Organisation for Economic Co-operation and Development.
[94] Délégation interministérielle au numérique. (n.d.). Cloud au centre : la doctrine de l'État. Numérique.gouv.fr. https://numerique.gouv.fr/offre-accompagnement/cloud-administrations/la-doctrine-de-letat/ & Premier ministre. (2021, 5 juillet). Circulaire n° 6282-SG du 5 juillet 2021 relative à

Ces catégories de vulnérabilité fournissent un cadre d'analyse général, mais leur portée ne peut être pleinement appréciée qu'au travers de cas concrets. Le secteur de la santé offre, à cet égard, un premier exemple particulièrement éclairant en raison de la sensibilité des données traitées et des contraintes juridiques qui entourent leur hébergement.

C. Santé

Le 30 novembre 2019 est créée la Plateforme des données de santé (PDS), également appelée Health Data Hub, destinée à faciliter le partage des données de santé issues de sources très variées afin de favoriser la recherche. Cet organisme avait pour but de centraliser, organiser et mettre à disposition les données de santé afin de soutenir l'innovation, tout en facilitant l'exercice des droits des patients et la diffusion de standards d'usage et d'échange. Elle accompagne aussi, y compris financièrement, les projets sélectionnés et favorise l'accès à certains jeux de données à faible risque pour la vie privée. A titre d'exemple, en 2024, le Health Data Hub a enregistré une augmentation de plus de 60 % du nombre de projets accompagnés, illustrant son rôle croissant de soutien aux porteurs de projets de recherche[95].

Cependant, la sensibilité de ces données tient à la fois à leur nature médicale, à leur caractère intime, mais aussi à leur volume, à leur granularité et aux possibilités de croisement qu'elles offrent, lesquelles permettent de retracer avec une grande précision la trajectoire sanitaire des personnes concernées. C'est précisément en raison de cette concentration de données particulièrement sensibles qu'un niveau de protection élevé devait être recherché, non seulement sur le plan technique, mais également sur le plan juridique.

Néanmoins un paradoxe émerge dès lors que la PDS a recours pour l'hébergement de ses données à Microsoft Ireland. En effet, bien que les données fussent stockées en France par l'intermédiaire d'une entité établie dans l'Union européenne, l'hébergeur appartenait à un groupe dont la société mère était soumise au droit américain, le FISA 702 (c.f. Chapitre 3). Le paradoxe réside ainsi dans le fait que des données, appelant par leur sensibilité même, une maîtrise juridique aussi étanche que possible, sont

la doctrine d'utilisation de l'informatique en nuage par l'État (« cloud au centre »). Légifrance. https://www.legifrance.gouv.fr/circulaire/id/45205

[95] Health Data Hub. (2025). *Rapport annuel 2024*. https://www.health-data-hub.fr/sites/default/files/2025-05/Health-Data-Hub-Rapport-annuel-2024.pdf

confiées à une infrastructure demeurant partiellement inscrite dans un environnement juridique extra-européen.

C'est pourquoi en 2024, la CNIL est revenue sur ses avis antérieurs, jusqu'alors favorables[96], pour émettre certaines réserves et recommandations concernant la sécurité, l'hébergement et la protection contre les accès extraterritoriaux de la PSD[97]. La CNIL a convenu que la sécurité globale de la plateforme pouvait être regardée comme assurée sous réserve de la mise en œuvre effective et de la réévaluation régulière des mesures prévues. Cependant, elle alerte sur la question de l'hébergement qui soulève une difficulté proprement juridique. Compte tenu de la sensibilité et du volume des données en cause, la CNIL a estimé qu'un niveau de protection élevé devait également être garanti à l'égard des risques d'accès par des autorités publiques de pays tiers. Elle a, dans cette perspective, recommandé que l'hébergement et les services associés soient réservés à des entités relevant exclusivement des juridictions de l'Union européenne ou présentant des garanties spécifiques, telles que celles offertes par la certification SecNumCloud.

L'avis de la CNIL met ainsi en évidence que, pour ce type d'infrastructure, la localisation des données sur le territoire de l'Union ne suffit pas, à elle seule, à neutraliser l'ensemble des vulnérabilités juridiques susceptibles d'affecter leur protection.

1. L'écosystème numérique de la santé en France

Comme le démontre l'avis du CNIL[98] en 2024, l'analyse de la vulnérabilité du secteur de la santé ne peut se limiter à la seule exposition à un risque juridique extraterritorial. Elle suppose également d'examiner les conditions concrètes dans lesquelles une alternative peut être mobilisée.

L'écosystème institutionnel du numérique en santé (schéma 1) permet précisément d'éclairer cette question. La Délégation au numérique en santé (DNS) assure le pilotage d'ensemble des chantiers de transformation du numérique en santé[99], tandis que l'Agence du Numérique en Santé (ANS)

[96] CNIL (2019, 31 janvier). *Délibération n° 2019-008 du 31 janvier 2019 portant avis sur un projet de loi relatif à l'organisation et à la transformation du système de santé (demande d'avis n° 19001144).* Légifrance. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038142154/

[97] CNIL (2024). *Avis sur la Plateforme des données de santé.* https://www.cnil.fr/fr/les-principaux-avis-et-recommandations-de-la-cnil-sur-la-plateforme-des-donnees-de-sante

[98] CNIL (2024). *Avis sur la Plateforme des données de santé.* https://www.cnil.fr/fr/les-principaux-avis-et-recommandations-de-la-cnil-sur-la-plateforme-des-donnees-de-sante

[99] Délégation au numérique en santé. (2024). *Qu'est-ce que la Délégation au numérique en santé (DNS) ?* Ministère de la Santé et de la Prévention. esante.gouv.fr – Qu'est-ce que la DNS ?

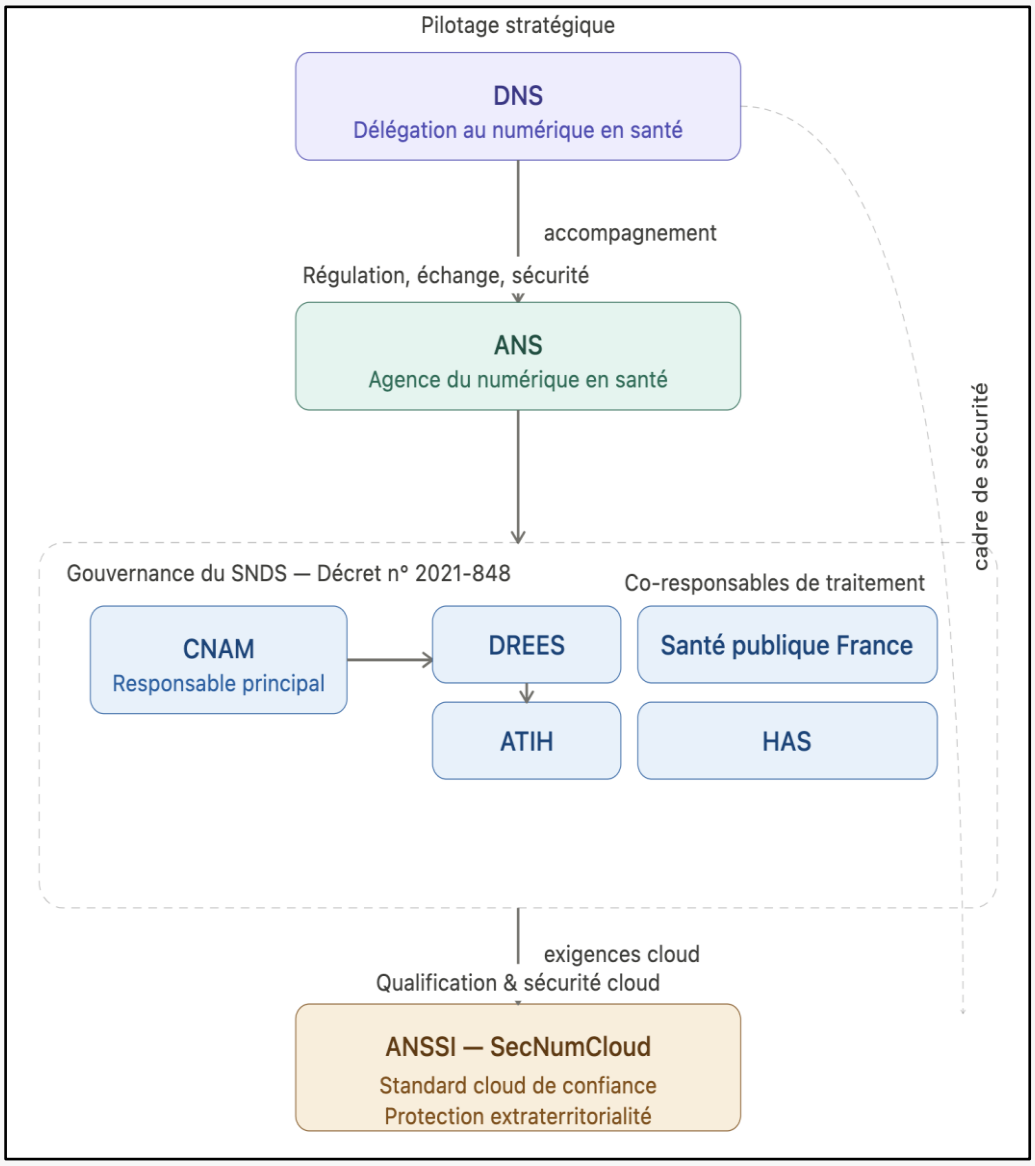
accompagne les acteurs du secteur et participe à la structuration de règles communes de régulation, d'échange et de sécurité[100]. Parallèlement, la CNAM occupe une place structurante dans la gouvernance du SNDS en tant que responsable de traitement principal, aux côtés de la Direction de la Recherche, des Études, de l'Évaluation et des Statistiques (DREES), de Santé publique France, de l'Agence Technique de l'Information sur l'Hospitalisation (ATIH) et de la Haute Autorité de Santé (HAS), le cadre réglementaire précisant les rôles respectifs des responsables de traitement et les modalités de fonctionnement du système[101]. Dès lors, l'existence d'offres alternatives compatibles avec ces exigences permet de déplacer l'analyse : la **vulnérabilité apparaît aussi comme une question de substituabilité effective**, c'est-à-dire de disponibilité d'offres de remplacement juridiquement, techniquement et opérationnellement adaptées aux contraintes propres aux données de santé sensibles.

[100] Délégation au numérique en santé [DNS], & Agence du Numérique en Santé [ANS]. (2025, June 24). *13ème Conseil du Numérique en Santé (CNS)* https://esante.gouv.fr/sites/default/files/media_entity/documents/20250624_cns_presentation.pdf

[101] République française. (2021, June 29). *Décret n° 2021-848 du 29 juin 2021 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ». Journal officiel de la République française*, n° 0150, texte n° 63. Légifrance. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043715694

SCHÉMA 1

L'écosystème institutionnel français du numérique en santé[102]



[102] (auto-produit, Valentine Schmitz)

2. Acteurs alternatifs : OVHcloud

À cet égard, l'exemple de OVH cloud illustre concrètement ce que recouvre la notion de substituabilité effective. En tant qu'acteur européen proposant des offres qualifiées SecNumCloud, OVH cloud répond aux exigences identifiées par l'ANSSI, en ce qu'il échappe au champ d'application de l'extraterritorialité du droit et relève exclusivement des juridictions de l'Union européenne[103]. Son existence au sein de l'écosystème démontre que **la vulnérabilité juridique identifiée n'est pas structurellement irréductible** : elle procède aussi d'un choix d'infrastructure, lequel peut, sous certaines conditions techniques et opérationnelles, être révisé.

Pour autant, la disponibilité formelle d'une alternative **ne suffit pas à garantir une substituabilité réelle**. Encore faut-il que cette alternative soit opérationnellement compatible avec les contraintes propres à un système de la taille et de la complexité du SNDS, en termes de capacité d'hébergement, de continuité de service, d'intégration aux outils existants et de coût de migration. C'est précisément à l'articulation entre ces dimensions juridiques, techniques et économiques que se joue, en définitive, le degré de dépendance effective du secteur de la santé à l'égard d'acteurs soumis à des droits extraterritoriaux.

D. Justice

Si le secteur de la santé illustre la vulnérabilité juridique liée à l'extraterritorialité, le secteur de la justice en révèle une dimension supplémentaire : celle d'une **criticité opérationnelle** et **régalienne** qui renforce encore l'exigence de maîtrise des infrastructures numériques.

Les systèmes d'information judiciaires supportent en effet des activités touchant au contentieux pénal, à l'exécution des peines, aux situations d'urgence et, plus largement, au fonctionnement quotidien du service public de la justice. Cette spécificité est reconnue par le ministère de la Justice qui inscrit la sécurité numérique dans une logique de maîtrise du risque, de gouvernance et de gestion des incidents à l'échelle de l'ensemble de ses services[104]. Elle l'est également dans la politique ministérielle de

[103] Bureau d'Enquêtes et d'Analyses des Risques Industriels. (2022). *Rapport d'enquête sur l'incendie du 10 mars 2021 à Strasbourg dans les locaux de la société OVHcloud*. Ministère de la Transition écologique. https://www.igedd.developpement-durable.gouv.fr/rapport-d-enquete-sur-l-incendie-du-10-mars-2021-a-a3660.html

[104] Ministère de la Justice. (2026). *Politique ministérielle de sécurité numérique*. https://www.justice.gouv.fr/sites/default/files/2026-02/Annexe_PMSN_2026.pdf

défense et de sécurité, qui rappelle que le ministre de la Justice est tenu d'assurer la **continuité de l'activité pénale ainsi que l'exécution des peines en toutes circonstances**, ce qui confère aux infrastructures numériques du ministère une importance opérationnelle particulière[105].

La première vulnérabilité est donc informationnelle. Les systèmes de la justice traitent des données à caractère hautement confidentiel, notamment dans le champ pénal. Le Sénat souligne ainsi que les données de connexion constituent des données personnelles soumises à des exigences de protection renforcée dans le cadre de l'enquête et de la procédure pénale, non pas au sens des catégories particulières de données définies à l'article 9 du RGPD[106], mais en raison de leur **portée probatoire et de leur sensibilité contextuelle**, ce qui illustre plus largement la densité informationnelle des données manipulées dans ce secteur[107]. À cette sensibilité intrinsèque s'ajoute le fait que la numérisation croissante des procédures, des échanges et des outils accentue l'exposition globale du ministère au risque numérique, en multipliant les dépendances entre applications, infrastructures et partenaires.

La deuxième vulnérabilité est **opérationnelle**. Dans la justice, une indisponibilité prolongée peut affecter la tenue des audiences, le traitement des contentieux urgents, la conduite des procédures pénales ou encore l'exécution des décisions. Cette exigence de continuité justifie que les systèmes d'information judiciaires soient appréhendés comme des infrastructures critiques. Le guide d'homologation du ministère confirme d'ailleurs que les démarches de sécurité doivent être adaptées à la criticité propre de chaque système et qu'elles concernent aussi bien les applications

---

[105] Ministère de la Justice. (2016). *Arrêté portant approbation de la politique ministérielle de défense et de sécurité*.
https://www.justice.gouv.fr/sites/default/files/migrations/textes/art_pix/JUST1624217A.pdf

[106] ***Chapitre IX - RGPD relatif aux dispositions relatives à des situations particulières de traitement,*** *Article 85 -* **Traitement et liberté d'expression et d'information** 1. Les États membres concilient, par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement et le droit à la liberté d'expression et d'information, y compris le traitement à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire. 2. Dans le cadre du traitement réalisé à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire, les États membres prévoient des exemptions ou des dérogations au chapitre II (principes), au chapitre III (droits de la personne concernée), au chapitre IV (responsable du traitement et sous-traitant), au chapitre V (transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales), au chapitre VI (autorités de contrôle indépendantes), au chapitre VII (coopération et cohérence) et au chapitre IX (situations particulières de traitement) si celles-ci sont nécessaires pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information. 3. Chaque État membre notifie à la Commission les dispositions légales qu'il a adoptées en vertu du paragraphe 2 et, sans tarder, toute disposition légale modificative ultérieure ou toute modification ultérieure les concernant. https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=fr

[107] Sénat. (2023). *Données de connexion dans l'enquête pénale* [rapport].
https://www.senat.fr/rap/r23-110/r23-1109.html

métiers que les socles techniques, tels que les annuaires, les postes de travail, les dispositifs de sauvegarde et les archivages[108]. Cela montre que la vulnérabilité de la justice ne dépend pas seulement des applications visibles, mais de toute une chaîne technique dont la défaillance peut se propager.

La troisième vulnérabilité est **organisationnelle** et **stratégique**. La Cour des comptes[109] met en évidence que la modernisation engagée ne se réduit pas à l'acquisition d'outils mais implique des choix d'architecture, de gouvernance, de pilotage budgétaire et de ressources humaines, qui conditionnent directement la robustesse des systèmes et leur capacité d'évolution. Dans cette perspective, la vulnérabilité peut aussi être comprise comme une difficulté à reprendre la main sur des systèmes devenus complexes, interdépendants ou insuffisamment maîtrisés.

Enfin, la justice présente une vulnérabilité **juridique** et **de souveraineté** particulièrement nette. La doctrine de l'État dite « Cloud au centre » fait du cloud le principe applicable aux nouveaux projets numériques, mais elle articule cette orientation avec un impératif de souveraineté et de protection des données sensibles. La DINUM précise ainsi que les données sensibles de l'État doivent relever soit du cloud interne interministériel, soit d'un cloud commercial de confiance disposant de la qualification SecNumCloud et d'une immunité à l'égard des réglementations extraterritoriales[110]. Dès lors, par cohérence avec la nature des missions judiciaires, les systèmes d'information les plus sensibles du ministère devraient relever d'offres internes ou qualifiées SecNumCloud, précisément parce que la vulnérabilité de la justice ne se réduit pas au risque cyber au sens strict, mais inclut aussi la dépendance à un environnement juridique extra-européen tout comme pour le domaine de la santé.

[108] Ministère de la Justice. (2025). *Guide d'homologation de la sécurité numérique des systèmes d'information relevant du ministère de la Justice.* https://www.justice.gouv.fr/sites/default/files/2025-03/Guide-homologation_V2.pdf
[109] Cour des comptes. (2022). *Point d'étape du plan de transformation numérique du ministère de la justice.* https://www.ccomptes.fr/sites/default/files/2022-01/20220126-plan-transformation-numerique-justice-.pdf
[110] Délégation interministérielle au numérique. (n.d.). Cloud au centre : la doctrine de l'État. Numérique.gouv.fr. https://numerique.gouv.fr/offre-accompagnement/cloud-administrations/la-doctrine-de-letat/ & Direction interministérielle du numérique. (s. d.). *Le cloud commercial.* numerique.gouv.fr. https://numerique.gouv.fr/offre-accompagnement/cloud-administrations/le-cloud-commercial/ & Délégation interministérielle au numérique (DINUM). (2021.). *Doctrine cloud de l'État.* https://www.numerique.gouv.fr/sinformer/espace-presse/le-gouvernement-annonce-sa-strategie-nationale-pour-le-cloud/

E. Défense

Dans le champ de la défense, la vulnérabilité associée au cloud ne peut être réduite à la seule question de la cybersécurité technique. Elle renvoie plus largement à des **enjeux de souveraineté numérique**, de **maîtrise des infrastructures critiques** et de **dépendance** stratégique vis-à-vis de prestataires extérieurs. Toutefois, ces vulnérabilités s'observent moins dans une hypothétique compromission directe des systèmes opérationnels militaires (domaine hautement spécifique et peu documenté publiquement) que dans deux espaces plus tangibles : l'administration numérique du **ministère des Armées** et l'écosystème industriel de la Base industrielle et technologique de défense (**BITD**).

Premièrement, le ministère des Armées lui-même constitue un acteur numérique exposé. Au-delà des systèmes strictement opérationnels, le ministère repose sur un ensemble d'infrastructures numériques administratives nécessaires à son fonctionnement quotidien tels que les ressources humaines, les achats, la logistique, la communication, la gestion documentaire ou encore le traitement de données organisationnelles. Le Commissariat au numérique de défense (CND), chargé depuis 2025 du pilotage de cette stratégie, indique explicitement que l'architecture cloud du ministère repose sur une segmentation différenciée selon le niveau de sensibilité des usages. Concrètement, le ministère dispose d'un cloud privé pour les environnements les plus critiques, complété par des solutions de cloud de confiance pour des usages moins sensibles[111]. Cette doctrine souligne le besoin de différencier les usages selon leur niveau de sensibilité, mais la dépendance à des prestataires externes demeure une question stratégique dès lors que certaines fonctions essentielles reposent sur des infrastructures non entièrement maîtrisées.

La question de la doctrine française du cloud souverain (SecNumCloud), dans le cas du ministère des Armées, revêt une importance particulière. Même lorsque les données concernées ne relèvent pas du secret opérationnel, une dépendance excessive à des fournisseurs soumis à des juridictions extérieures peut créer une vulnérabilité structurelle en matière de **disponibilité**, de **confidentialité** ou de **continuité de service**[112].

[111] Ministère des Armées – Commissariat au numérique de défense. (2025). *Le Cloud*. defense.gouv.fr. https://www.defense.gouv.fr/cnd/nos-missions/enjeux-du-commissariat-au-numerique-defense/cloud

[112] https://cyber.gouv.fr/enjeux-technologiques/cloud/

Deuxièmement, cette vulnérabilité apparaît avec davantage d'acuité encore au sein de la **BITD**. Les entreprises de la BITD concentrent des actifs stratégiques majeurs allant de la propriété intellectuelle sensible, des données industrielles, des plans de systèmes d'armes, des programmes duals à des informations relatives à la chaîne d'approvisionnement militaire. Or, cet écosystème constitue une **cible privilégiée d'attaques cyber**. En 2025, l'ANSSI souligne la persistance d'attaques par rançongiciel visant des entités industrielles stratégiques, illustrant la vulnérabilité durable du tissu industriel français[113]. Cette exposition est amplifiée par la structure même de la BITD, largement composée de PME aux capacités de cybersécurisation limitées. La Commission des finances de l'Assemblée nationale recense entre 500 et 550 atteintes caractérisées par an visant ses entités, dont 80 % ciblent précisément ces maillons vulnérables[114]. Effectivement, la Commission de la défense consacrée aux défis de la cyberdéfense formait un diagnostic similaire et appelait dès 2024 à renforcer les exigences de cybersécurité imposées aux entreprises de défense et à leurs sous-traitants dans le cadre des marchés publics[115].

L'enjeu ici dépasse la protection individuelle des entreprises concernées. Dans un environnement militaire fortement interdépendant, **la vulnérabilité d'un sous-traitant peut devenir celle de l'ensemble de la chaîne capacitaire**. Les attaques dites de rebond, consistant à compromettre un acteur périphérique pour atteindre une cible stratégique, illustrent particulièrement cette logique systémique. Dès lors, la dépendance au cloud dans le secteur de la défense ne doit pas être envisagée uniquement sous l'angle de la performance technologique ou du coût économique, mais également comme **une question de résilience industrielle et de continuité stratégique.**

Enfin, à l'échelle plus large de l'appareil sécuritaire français, le renouvellement du contrat entre la **DGSI et Palantir** rappelle que les dépendances technologiques à des fournisseurs étrangers peuvent, lorsqu'elles s'installent durablement, dépasser leur caractère initialement transitoire[116]. Si ce cas relève du renseignement intérieur davantage que de

[113] https://cyber.gouv.fr/enjeux-technologiques/cloud/

[114] Plassard, C. (2025, 16 juillet). *Rapport d'information n° 1757 sur la guerre économique* (Rapport de la Commission des finances de l'économie générale et du contrôle budgétaire). Assemblée nationale. https://www.assemblee-nationale.fr/dyn/17/rapports/cion_fin/l17b1757_rapport-information

[115] Le Hénanff, A. & Mathieu, F. (2024, 17 janvier). *Rapport d'information n° 2068 sur les défis de la cyberdéfense* (Mission flash, Commission de la défense nationale et des forces armées). Assemblée nationale. https://www.assemblee-nationale.fr/dyn/16/rapports/cion_def/l16b2068_rapport-information

[116] Palantir Technologies. (2025, 15 décembre). *Palantir Announces Renewal of Multi-Year Contract with the DGSI* [Communiqué de presse]. Palantir Investor Relations.

la défense au sens stricte, il illustre néanmoins une **tension persistante entre efficacité opérationnelle immédiate et autonomie stratégique de long terme**

F. Secteur privé : des vulnérabilités convergentes entre banques, assureurs et PME

Après avoir étudié les vulnérabilités propres aux secteurs publics régaliens, il convient d'élargir l'analyse au secteur privé. Celui-ci n'est pas seulement utilisateur du cloud : il en devient progressivement dépendant. Banques, assureurs et petites et moyennes entreprises rencontrent des formes différenciées mais structurellement convergentes de vulnérabilité, mêlant dépendance technique, coût de sortie, exposition juridique, asymétrie d'information et perte de maîtrise stratégique. Si les enjeux de souveraineté paraissent a priori réservés aux acteurs publics, ils concernent en réalité l'ensemble des entités qui externalisent des données sensibles vers des infrastructures soumises à des droits extraterritoriaux.

1. Le secteur bancaire : entre impératif d'innovation et dépendance critique

Le secteur bancaire illustre particulièrement la tension entre la nécessité économique du cloud et les risques structurels qui en découlent. Les banques ont largement adopté des architectures hybrides, mobilisant le cloud public pour les services clients, tels que les applications mobiles, personnalisation par l'intelligence artificielle, accélération du *time-to-market*, tout en conservant des infrastructures sur site ou en cloud privé pour les systèmes cœur et les données les plus sensibles (Nortain & Darchy, 2025). Cette hybridation traduit une tentative de concilier agilité opérationnelle et maîtrise des risques dans un environnement réglementaire exigeant.

Le principal obstacle à une migration fluide reste la dette technique héritée des architectures "*legacy*" ou lié au "organitional path dependence"[117]. Nombre de grandes banques ont procédé à des migrations dites "*lift & shift*". Celles-ci consistent à **transférer les applications vers le cloud sans refonte de leur architecture**, produisant des **résultats décevants** (performances

https://investors.palantir.com/news-details/2025/Palantir-Announces-Renewal-of-Multi-Year-Contract-with-the-DGSI/

[117] (Gilbert, C. G. (2008). Organizational path dependence: Opening the black box. *Academy of Management Review, 33*(4), 975–994. https://doi.org/10.5465/AMR.2009.44885978)

sous-optimales, coûts d'exploitation supérieurs à l'hébergement initial, et dette technique déplacée mais non résolue)[118]. La **gouvernance financière** représente un autre facteur de friction. Le modèle de facturation à la consommation, propre au cloud, est structurellement incompatible avec les cycles budgétaires annualisés des grandes institutions, conduisant à des dérives de **coûts non anticipées**[119].

Ces difficultés opérationnelles s'inscrivent dans un contexte réglementaire désormais très contraignant. Entré en application le 17 janvier 2025, le règlement européen DORA (*Digital Operational Resilience Act*)[120] rebâtit l'ensemble du cadre de résilience numérique du secteur financier. L'Europe impose désormais des standards harmonisés à l'ensemble de l'écosystème financier. Ainsi, la **cybersécurité** n'est plus l'affaire des informaticiens, mais celle des **conseils d'administration**, et la **résilience numérique** devient un **impératif stratégique** au même titre que la solvabilité ou la liquidité. DORA impose aux entités financières une vision systémique de leurs dépendances technologiques, avec des **obligations spécifiques de gouvernance**, de **plans de continuité**, de suivi permanent des prestataires TIC critiques et **d'audit**. Il exige en particulier la tenue d'un registre des contrats avec les prestataires, la démonstration de scénarios de substitution, et l'élaboration de plans de réversibilité pour toute fonction critique externalisée. L'ACPR et la BCE examinent désormais avec une attention particulière la qualité des registres d'externalisation, la robustesse des contrats avec les prestataires critiques et l'effectivité des plans de réversibilité, sanctionnant les établissements défaillants.

Cette évolution réglementaire est significative au regard de l'analyse développée dans les chapitres précédents. Là où la doctrine « **Cloud au centre** » posait la question de la souveraineté comme contrainte à gérer, **DORA la transforme en obligation justiciable**. Le Comité de stabilité financière a publié en décembre 2024 une boîte à outils pour la gestion et la supervision des risques, jugeant que les dépendances vis-à-vis des tiers se sont accrues ces dernières années dans le cadre de la numérisation du secteur financier[121].

[118] Nortain, A., & Darchy, R. (2025, 13 juin). Comment les banques doivent migrer efficacement vers le cloud. *Zenika*. https://www.zenika.com/
[119] Nortain, A., & Darchy, R. (2025, 13 juin). Comment les banques doivent migrer efficacement vers le cloud. *Zenika*. https://www.zenika.com/
[120] Parlement européen et Conseil de l'Union européenne. (2022). *Règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier (DORA)*, du 14 décembre 2022. *Journal officiel de l'Union européenne*, L 333.
[121] (Banque centrale européenne (BCE), *Décisions du Conseil des gouverneurs de la BCE (autres que les décisions relatives à la fixation des taux d'intérêt) – Novembre 2024*, 29 novembre 2024,

2. Les PME : vulnérabilité silencieuse et asymétrie d'information

Si le secteur bancaire dispose de ressources réglementaires et humaines pour appréhender les risques liés au cloud, les petites et moyennes entreprises se trouvent dans une **situation structurellement plus précaire**. L'étude de Bourliataux-Lajoinie et al. (2025), fondée sur vingt entretiens avec des cadres supérieurs d'entreprises commerciales, industrielles et de haute technologie, met en évidence des comportements d'adoption du cloud largement déterminés par la simplicité d'usage et la gratuité apparente des offres, au détriment de toute évaluation des risques de souveraineté ou de confidentialité. La facilité d'utilisation au sens du modèle TAM de Davis (1989) prime sur la sécurité des échanges. Des pratiques aussi répandues que le recours à Google Drive ou Dropbox pour partager des dossiers sensibles, ou l'utilisation d'un même terminal personnel pour les activités privées et professionnelles, illustrent la porosité entre sphères privée et publique qui résulte de cette adoption non maîtrisée[122].

Cette vulnérabilité se double d'une **asymétrie d'information structurelle**. **Les PME ne disposent généralement pas des compétences internes** pour évaluer où transitent leurs données, dans quels centres d'hébergement elles sont stockées, ni sous quel régime juridique elles se trouvent placées. Les coûts liés à la mauvaise connaissance des risques du cloud (perte de gouvernance sur le système d'information, sous-estimation des coûts de changement de fournisseur, méconnaissance des obligations du RGPD) ne sont généralement pas pris en compte par les acteurs concernés[123]. La **valeur économique du cloud est minimisée au regard de sa valeur d'usage**, au prix d'une délégation implicite et non négociée de la maîtrise des données vers les fournisseurs de solutions.

Ce phénomène ne se limite pas aux entreprises commerciales ordinaires. Des sociétés disposant d'un patrimoine scientifique et technique sensible (laboratoires de recherche, entreprises de haute technologie) continuent de recourir à des solutions de type Dropbox ou Google Drive, en dépit des recommandations de sécurité de l'ANSSI, au **motif que les alternatives**

disponible sur le site de la Banque centrale européenne : Décisions du Conseil des gouverneurs de la BCE – novembre 2024).

[122] Bourliataux-Lajoinie, S., David, M., Legrand, V., & Dercourt, C. (2025). Comprendre les enjeux du Cloud Souverain dans les PME, une lecture des pratiques via la théorie de l'agence. *Annales des Mines – Gérer & Comprendre*, n° 162, pp. 13–25. https://doi.org/10.3917/geco1.162.0014

[123] Bourliataux-Lajoinie, S., David, M., Legrand, V., & Dercourt, C. (2025). Comprendre les enjeux du Cloud Souverain dans les PME, une lecture des pratiques via la théorie de l'agence. *Annales des Mines – Gérer & Comprendre*, n° 162, pp. 13–25. https://doi.org/10.3917/geco1.162.0014

souveraines sont perçues comme une contrainte imposée plutôt qu'une protection nécessaire[124]. Cette logique rejoint la notion de *lock-in*, c'est-à-dire que la familiarisation précoce avec des interfaces grand public crée des habitudes d'usage difficiles à déloger par la seule réglementation.

[124] Bourliataux-Lajoinie, S., David, M., Legrand, V., & Dercourt, C. (2025). Comprendre les enjeux du Cloud Souverain dans les PME, une lecture des pratiques via la théorie de l'agence. *Annales des Mines – Gérer & Comprendre*, n° 162, pp. 13–25. https://doi.org/10.3917/geco1.162.0014 & Entretien avec le professeur Frédéric Marty

Risques et vulnérabilités

À RETENIR

- L'analyse conduite dans ce chapitre montre que la vulnérabilité associée au cloud ne réside pas dans la technologie elle-même, mais dans les conditions dans lesquelles son externalisation affecte la capacité effective de gouvernance de l'acteur qui en demeure juridiquement, opérationnellement ou stratégiquement responsable. **Le cloud n'est pas intrinsèquement vulnérabilisant ; le risque apparaît lorsque l'externalisation entraîne une perte de maîtrise sur les infrastructures et services numériques concernés.**

- Cette approche permet de comprendre pourquoi des secteurs pourtant très différents présentent des vulnérabilités similaires. Dans les domaines régaliens, cette dissociation entre responsabilité et contrôle revêt une intensité particulière dès lors que l'État demeure garant de missions dont la continuité, la confidentialité ou l'intégrité ne peuvent être interrompues sans affecter l'exercice même de la puissance publique. Dans le secteur de la santé, l'enjeu révèle les limites d'une approche purement territoriale de la protection des données lorsque la dépendance juridique subsiste à travers la structure du fournisseur. Dans la justice, la vulnérabilité tient moins à la seule menace cyber qu'au fait qu'une défaillance technique ou contractuelle pourrait entraver directement l'exécution d'une mission régalienne. Dans la défense, enfin, cette logique se prolonge à l'échelle systémique. La dépendance ne se concentre pas uniquement dans les infrastructures centrales, mais peut émerger dans les chaînes industrielles, les sous-traitants ou les services périphériques, transformant une fragilité locale en vulnérabilité stratégique élargie. Le secteur privé présente le même écart entre externalisation et contrôle effectif, mais de façon inégale. Les grandes institutions financières bénéficient désormais d'un cadre qui les oblige à rester responsables de leurs prestataires, tandis que les PME se retrouvent souvent à déléguer des fonctions essentielles, faute de moyens pour négocier ou évaluer ce à quoi elles s'engagent.

- Ces constats appellent toutefois plusieurs nuances. D'une part, **la dépendance au cloud n'est ni uniforme ni nécessairement irréversible**. Le niveau de vulnérabilité varie selon la sensibilité des usages, les choix d'architecture retenus, les exigences contractuelles imposées et l'existence d'alternatives effectivement mobilisables. D'autre part, **toute dépendance ne relève pas d'un enfermement intentionnel**. Une part importante des vulnérabilités identifiées procède de décisions techniques rationnelles prises à un instant donné, dont les effets cumulatifs deviennent visibles seulement à mesure que l'environnement technique, réglementaire ou stratégique évolue. C'est précisément ce caractère progressif qui rend ces vulnérabilités particulièrement difficiles à appréhender.

- **Dès lors, l'enjeu n'est peut-être pas tant de déterminer si le cloud constitue en lui-même un risque, que de comprendre à partir de quel seuil une externalisation initialement maîtrisée cesse d'être un choix d'organisation pour devenir une dépendance structurelle**. C'est dans cette transformation progressive du confort opérationnel en contrainte stratégique que se situe la question centrale des politiques de remédiation.

Recommandations

Levier Technique et Architectural

Généraliser la conteneurisation et rejeter les architectures fermées : L'usage de la conteneurisation (standards ouverts type Docker) doit devenir la norme impérative pour tout nouveau développement public. Il est recommandé d'interdire explicitement l'utilisation de bases de données non compatibles SQL ou de services d'exécution serverless propriétaires pour les systèmes centraux de l'État, afin d'encapsuler l'application dans des environnements portables, agnostiques du fournisseur cloud.

Déployer systématiquement l'orchestration multi-cloud : Afin de prévenir le verrouillage technologique, il est essentiel de découpler le code applicatif de l'infrastructure sous-jacente. Nous recommandons l'adoption généralisée de couches d'abstraction open source (telles que Crossplane ou Dapr) permettant de limiter le basculement entre fournisseurs à un simple changement de configuration. Cette réversibilité stratégique autorise le recours ponctuel à un hyperscaler si l'offre européenne manque de maturité sur certains services, tout en garantissant un rapatriement sans friction ni surcoût de code dès qu'une alternative souveraine devient compétitive.

Automatiser la conformité via l'Infrastructure-as-Code et le Policy-as-Code : Pour s'assurer que l'abstraction architecturale ne soit pas compromise par des erreurs manuelles, l'infrastructure doit être intégralement versionnée sous forme de code. Nous recommandons de coupler ces outils à des mécanismes de Policy-as-Code permettant de traduire les contraintes de souveraineté en règles logicielles exécutables automatiquement dès le déploiement des projets.

Refondre la formation académique et promouvoir les communs numériques : Le verrouillage technologique s'enracinant dès la formation des ingénieurs, une restructuration de l'enseignement supérieur européen en informatique nous semble primordiale. Nous recommandons de limiter la pénétration des programmes universitaires sponsorisés par les hyperscalers, afin de recentrer les cursus sur les fondamentaux des systèmes distribués agnostiques et de l'orchestration multi-cloud. En complément, il est recommandé d'intégrer massivement le catalogue des solutions open source (OSS) de l'UE dans les cursus et les administrations, afin de forger une culture de l'ingénierie immunisée contre le verrouillage.

Instaurer des certifications européennes et des formations décisionnelles obligatoires : Pour contrer la valeur marchande des certifications propriétaires, nous recommandons la création de certifications européennes alternatives de très haut niveau, portées par des consortiums académiques et l'Institut Européen d'Innovation et de Technologie (EIT). Par ailleurs, il est également recommandé d'imposer aux acheteurs publics, DSI et RSSI des modules de formation continue obligatoires portant spécifiquement sur la géopolitique de la donnée, le calcul des coûts de réversibilité et la cartographie des alternatives technologiques européennes.

Recommandations

Levier Financier et Industriel

Cibler les financements publics sur le continuum Cloud-Edge : Face à l'impossibilité de rattraper les hyperscalers américains sur les services IaaS généralistes à court terme, la stratégie européenne doit reposer sur une sélectivité asymétrique. Il est recommandé d'investir massivement, via Horizon Europe ou les fonds de relance, dans les ruptures technologiques de la prochaine décennie, notamment l'Edge Computing, l'IA et le quantique. Des projets comme l'IPCEI-CIS doivent sanctuariser la création d'intergiciels open source fédérant des ressources hétérogènes.

Instaurer des quotas souverains dans la commande publique : La commande publique doit muer en outil stratégique de politique industrielle. Pour se conformer aux règles de l'OMC et du droit européen tout en atteignant cet objectif, il est recommandé d'intégrer les exigences d'immunité extraterritoriale comme critères d'éligibilité techniques absolus dans les cahiers des charges. Pour les données strictement régaliennes et critiques (OIV, OSE), l'Article 346 du TFUE doit être mobilisé de manière ciblée, en qualifiant ces infrastructures de marchés de défense et de sécurité, ce qui autorise légalement la restriction des appels d'offres.

Créer un Fonds Cloud Souverain Européen conditionnant l'émancipation technologique : Afin de combler le déficit capacitaire, il est recommandé de créer un véhicule financier macro-structurel calqué sur le Fonds Européen de la Défense (FED). En outre, tout financement public ou octroi de marché public visant des solutions de "cloud de confiance" hybrides doit être strictement assorti d'une feuille de route contraignante de réinternalisation logicielle, afin d'éviter le sovereign-washing et de garantir une véritable réduction de la dépendance aux licences extra-européennes.

Recommandations

Levier Réglementaire

Imposer des standards de résilience et d'immunité extraterritoriale dans la commande publique : La doctrine “Cloud au Centre” doit évoluer pour intégrer une exigence de souveraineté opérationnelle et juridique. Nous recommandons d'ériger les exigences de souveraineté du référentiel SecNumCloud 3.2 de l'ANSSI, en standard par défaut pour les données publiques. Ces exigences doivent constituer le socle minimal et non négociable de la position française lors des négociations du schéma de certification européen (EUCS), afin de garantir une protection absolue de nos données sensibles face aux injonctions juridiques d'États tiers.

Affirmer un mandat politique européen explicite : Il est recommandé qu’un arbitrage politique au niveau du Conseil européen tranche explicitement en faveur de critères d’immunité extraterritoriale contraignants, selon plusieurs niveaux en fonction de la sensibilité des données. Nous recommandons de converger les certifications nationales existantes (SecNumCloud, BSI C5, ENS) autour d'un socle EUCS commun. Une logique de coordination européenne est requise afin de parler d'une seule voix dans les négociations avec les puissances numériques tierces.

Instituer un régime optionnel européen libéré des contraintes nationales : S’appuyant sur le précédent EU Inc. proposé par la Commission Européenne en mars 2026, l’idée est de créer un 28ème régime européen optionnel afin de permettre d'avoir des acteurs européens pouvant se développer pour offrir des solutions équivalentes ou rivales avec les acteurs clouds actuels, dans l'offre ou l'innovation.

Levier Sociétal

Généraliser l'éducation à l'hygiène numérique : La méconnaissance des risques liés au cloud non souverain s'installe dès les premiers usages numériques, bien avant toute décision professionnelle. Il est recommandé de généraliser des programmes d'éducation à la sécurité numérique dès le lycée, sur le modèle du Passeport de Prévention numérique de l'ANSSI, afin de sensibiliser les futurs citoyens sur l’hygiène numérique et la protection et traçabilité des données personnelles.

2025-2026

1ère édition

RAPPORT ANNUEL

Les Dépendances

L'énergie française à l'heure de la souveraineté

La question du cloud souverain apparaît comme **un enjeu structurant pour la politique industrielle et numérique, au niveau français ou européen.** Alors que les infrastructures cloud deviennent un support essentiel du fonctionnement de l'économie de la donnée, **la dépendance aux fournisseurs technologiques étrangers soulève de nombreuses questions** quant à la capacité de la France et de l'Union européenne à garantir la protection de ses infrastructures numériques et données stratégiques.

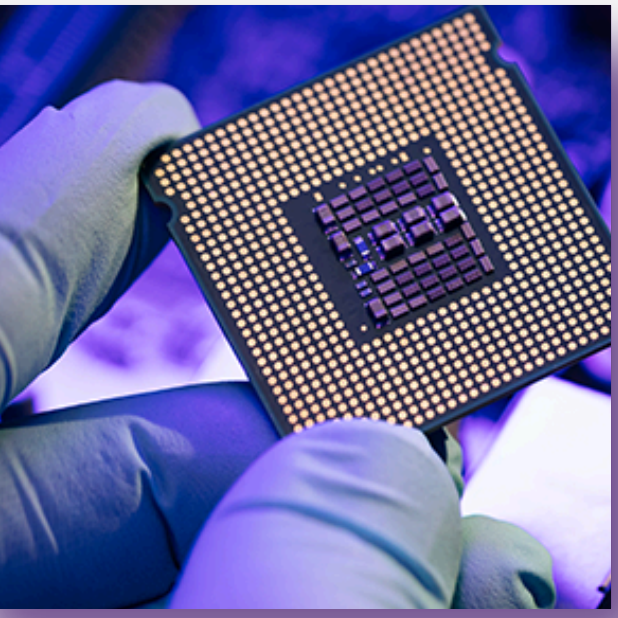


PHOTO ©/UFLYPRO / ADOBE STOCK

De ce fait, **ce rapport produira un état des lieux des dépendances auxquelles la France fait face aujourd'hui,** ainsi que l'efficacité des solutions apportées. Puis, dans un second temps, se penchera sur **les possibilités pour un cloud souverain ou de confiance pour renforcer la souveraineté digitale et l'autonomie de la France** en vue de ces dépendances.

2025-2026

CGE

1ère édition