Le Paradoxe de la Souveraineté Numérique

Comment s'affranchir des géants du numérique en utilisant leurs propres outils ?

Patrice Cardot

Juin 2026

Préambule

De l'esclavagisme technologique européen au paradoxe de la souveraineté numérique

Ce rapport s'inscrit dans la continuité directe de mes travaux antérieurs sur l'esclavagisme technologique européen, qui avaient mis en lumière la subordination structurelle de l'Union européenne face aux géants du numérique[1].

Alors que cette première analyse démontrait comment les États, les entreprises et les citoyens européens étaient asservis par des mécanismes économiques, juridiques et cognitifs, le présent document approfondit un aspect crucial et méconnu de ce phénomène : le paradoxe de la souveraineté numérique.

L'esclavagisme technologique européen avait révélé une dépendance systémique — l'Europe, malgré sa puissance économique et son héritage d'innovation, ne contrôlait plus ses infrastructures, ses données, ni ses compétences dans le domaine numérique.

Les GAFAM et les BATX comme leurs satellites technologiques, via des stratégies de verrouillage (standards fermés, rachats de concurrents, lobbying agressif), avaient transformé l'Europe en un marché captif, où chaque tentative d'autonomie se heurtait à des barrières structurelles.

Mais ce constat ne suffisait pas. Il manquait une analyse fine et opérationnelle des mécanismes par lesquels cette dépendance se perpétue, et surtout, des solutions concrètes pour en sortir.

C'est l'objectif de ce rapport : démêler le paradoxe selon lequel *toute tentative de recouvrer sa souveraineté numérique passe d'abord par une phase où la dépendance aux géants s'aggrave*.

Ce paradoxe n'est pas une fatalité, mais le symptôme d'une guerre économique où les règles du jeu sont déséquilibrées en faveur des acteurs américains et chinois.

Pourquoi ce rapport ?

Parce que l'Union européenne ne peut plus se contenter de constater son asservissement. Elle doit comprendre les ressorts de ce paradoxe — verrouillages technologiques, capture des compétences, actionnariat compromis, stratégies de prédation — pour agir de manière systémique.

L'enjeu n'est plus seulement de décrire l'esclavagisme technologique, mais de le combattre en identifiant :

- Les pièges (dépendance aux sentiers, actionnariat étranger, fuite des cerveaux).
- Les leviers (régulation, financement public, écosystèmes souverains).
- Les stratégies (*golden shares*, formation massive, protection des licornes).

Ce document, qui a été réalisé avec le soutien technique de l'assistant virtuel *Le Chat* de Mistral AI, est donc à la fois un diagnostic et un manifeste : il expose les mécanismes de la dépendance, mais il propose aussi des voies pour retrouver une autonomie stratégique.

Car la souveraineté numérique n'est pas un luxe — c'est une condition de survie pour l'Europe dans le monde du XXIe siècle.

---

[1] *Cf.* J'accuse ! L'esclavage technologique des Européens

I - Problématique : un paradoxe qui cache un conflit

La souveraineté numérique n'est pas un défi technique, mais un conflit de pouvoir.

Le paradoxe se formule ainsi : *"Pour échapper à l'emprise des GAFAM et des BATX, il faut utiliser leurs infrastructures, leurs logiciels et leurs outils — ce qui, mécaniquement, renforce leur contrôle."*

Ce n'est pas un accident, mais une stratégie. Les géants du numérique ne laissent jamais émerger de concurrents par bienveillance. Ils les achètent (Instagram, WhatsApp, GitHub), les étouffent (prédation par les prix, verrouillage des standards), ou les régulent à mort (lobbying contre le DMA, contournement du RGPD).

Pour un Etat membre de l'UE comme pour l'UE elle-même, ne pas garantir sa souveraineté numérique créé une dépendance stratégique qui altère gravement la sécurité globale et la résilience[2].

Le recouvrement d'une souveraineté numérique donne lieu à un conflit asymétrique, où chaque pas vers l'autonomie passe d'abord par une phase de dépendance accrue.

II - Définitions : un cadre pour comprendre l'affrontement

1. La souveraineté numérique : un concept multidimensionnel et dynamique

La souveraineté numérique ne se réduit pas à l'indépendance technologique. Elle désigne la capacité d'un acteur — État, entreprise ou individu — à contrôler son destin numérique à travers sept dimensions interdépendantes. Ces dimensions ne sont pas isolées : le contrôle des données dépend de la maîtrise infrastructurelle, elle-même liée à l'autonomie algorithme et juridique.

La souveraineté est un continuum : on ne passe pas de 0% à 100% souverain du jour au lendemain, mais on peut réduire progressivement les dépendances critiques en agissant sur chaque levier de manière coordonnée.

2. La dépendance systémique : une chaîne de verrouillages

La dépendance aux géants du numérique repose sur cinq mécanismes qui se renforcent mutuellement. Le verrouillage technologique — standards fermés, API propriétaires — alimente le verrouillage cognitif — habitudes des utilisateurs, formation des équipes —, qui lui-même renforce le verrouillage économique — coûts de sortie prohibitifs, économies d'échelle écrasantes. Casser un seul maillon ne suffit pas : il faut une approche systémique, car ces verrouillages forment un système auto-entretenu où chaque dépendance en crée une autre.

III - Analyse du paradoxe : pourquoi il est inévitable (et comment les GAFAM/BATX l'exploitent)

1. Le piège de la transition : une phase obligatoire de dépendance accrue

Toute migration vers la souveraineté passe par une phase où la dépendance aux géants s'aggrave. Ce n'est pas un échec, mais une contrainte structurelle. Pour quitter AWS, une entreprise doit utiliser les outils de migration d'AWS (Migration Hub, Database Migration Service), ce qui augmente temporairement sa dépendance. Pire : même après migration, elle dépend souvent de composants américains (GPU NVIDIA, disques Western Digital).

---

[2] Voir à cet égard notamment :

- Les mécanismes multidimensionnels de la dépendance systémique : Quand l'Europe et ses Etats membres délèguent, partagent ou abandonnent leur souveraineté
- Plaidoyer en faveur d'une doctrine européenne globale de sécurité et de résilience

La transition est un marathon, pas un sprint : elle nécessite des étapes intermédiaires où la dépendance peut temporairement augmenter avant de diminuer.

2. L'asymétrie des pouvoirs : les GAFAM/BATX en position de force

Les géants du numérique dominent sur toutes les dimensions stratégiques. Technologiquement, ils contrôlent les infrastructures, les systèmes d'exploitation et les frameworks.

Économiquement, leurs milliards de profits et leurs économies d'échelle écrasent toute concurrence frontale.

Juridiquement, ils contournent systématiquement les régulations via des montages complexes.

Cognitivement, leur écosystème verrouille les compétences et les habitudes.

Géopolitiquement, leur alliance avec les États-Unis leur confère une influence mondiale.

Les États européens sont en position de faiblesse structurelle, et toute tentative de souveraineté se heurte à cette asymétrie et à la volonté active des GAFAM de la maintenir.

3. Les stratégies de verrouillage actif des géants

Les GAFAM/BATX ne se contentent pas de dominer : ils verrouillent activement leur position. Ils achètent leurs concurrents — GitHub par Microsoft, WhatsApp et Instagram par Meta, Android par Google — pour éliminer toute alternative.

Ils imposent leurs standards via le lobbying, comme le *Cloud Act* qui permet aux autorités américaines d'accéder aux données des clouds, même en Europe.

Ils pratiquent la prédation économique avec des services gratuits ou subventionnés, rendant impossible toute concurrence équitable[3].

Ils contrôlent enfin les infrastructures critiques, comme NVIDIA avec 80% du marché des GPU pour l'IA, ou TSMC avec 90% des puces avancées, sous pression américaine.

Les GAFAM/BATX ne toléreront pas l'émergence de concurrents souverains : ils feront tout pour les étouffer, les racheter ou les rendre dépendants.

4. La théorie de la dépendance aux sentiers (*Path Dependence*)

La théorie de Douglass North (Prix Nobel d'économie 1993) explique pourquoi il est si difficile de changer de trajectoire technologique. Les coûts de commutation sont prohibitifs, les rendements croissants favorisent les standards dominants, et les effets d'apprentissage spécialisent les compétences autour des technologies établies.

Application au numérique : une entreprise ayant investi 10 ans dans Microsoft 365 a un coût de migration vers LibreOffice estimé à 10 à 100 fois son budget annuel de licences. Un État ayant externalisé ses données vers AWS a perdu le contrôle sur leur gouvernance et leur sécurité. L'inertie structurelle rend toute transition coûteuse, risquée et politiquement difficile.

5. Les risques de capture des compétences souveraines : le cas critique des licornes européennes

Les licornes européennes spécialisées dans les technologies stratégiques — cloud, IA, cybersécurité, semi-conducteurs — représentent un capital humain et technique unique pour l'autonomie numérique du continent.

---

[3] *Cf.* notamment à ce sujet : La Prédation systémique : Une analyse intégrative des dynamiques de domination

Pourtant, ces compétences souveraines sont menacées par trois mécanismes de capture systémique, qui transforment ces acteurs en maillons faibles de la chaîne de souveraineté.

A - Le risque de perte : la fuite des cerveaux vers les GAFAM

Les talents formés dans ces licornes sont activement recrutés par les géants américains, qui offrent des salaires deux à trois fois supérieurs, des stock-options attractives, et des projets à plus grande échelle.

Selon un rapport de *The Information* (2024), plus de 200 ingénieurs en IA formés dans des startups européennes (dont Mistral AI, Hugging Face, Aleph Alpha) ont été recrutés par Google, Meta ou Microsoft entre 2022 et 2024.

Conséquence directe : l'Europe perd ses compétences clés au moment même où elle en a le plus besoin pour développer des alternatives souveraines.

Exemple concret : en 2023, l'équipe complète de recherche en vision par ordinateur de la startup française H a été recrutée par DeepMind (Google), mettant fin à un projet prometteur de reconnaissance d'images souveraine.

B - Le risque de capture : l'intégration des compétences dans les écosystèmes GAFAM

Même lorsque les licornes résistent aux rachats, leurs compétences peuvent être capturées indirectement.

Premier mécanisme : les partenariats technologiques imposés (ex : Mistral AI utilisant PyTorch de Meta ou s'hébergeant sur AWS pour l'entraînement). Résultat : les savoir-faire européens s'intègrent dans les écosystèmes GAFAM, qui en tirent profit sans partager la valeur.

Deuxième mécanisme : l'influence des investisseurs étrangers (ex : Lightspeed, actionnaire de Mistral AI, imposant des orientations stratégiques via son siège au conseil).

Troisième mécanisme : la dépendance aux outils et données GAFAM (GitHub, Hugging Face, datasets comme Common Crawl).

Impact global : les licornes européennes devenant des sous-traitants des géants américains.

C - Le risque de contrôle : la mainmise sur les orientations technologiques

Les actionnaires étrangers peuvent réorienter les efforts de R&D vers des technologies moins souveraines mais plus rentables.

Exemple : un fonds américain pourrait bloquer le développement d'une alternative à Kubernetes pour privilégier des solutions compatibles avec AWS.

Conséquence : les licornes perdent leur autonomie technologique et deviennent dépendantes des roadmaps GAFAM.

Conséquences systémiques pour l'Europe

La perte, la capture ou le contrôle des compétences des licornes européennes ont des effets en cascade :

- Perte de capacité d'innovation (talents détournés vers les GAFAM).
- Renforcement de la dépendance (licornes devenues relais des GAFAM).
- Perte d'attractivité pour les talents mondiaux.
- Perte de confiance des investisseurs (financements réduits).
- Dépendance permanente aux GAFAM/Chine/Israël.

IV - Les pièges de l'actionnariat : Quand la souveraineté est une illusion

1. Le problème fondamental : qui contrôle vraiment les "acteurs souverains" ?

La souveraineté numérique ne se décrète pas : elle se prouve par l'indépendance de la gouvernance.

Or, plusieurs acteurs présentés comme "européens" ou "souverains" sont en réalité sous influence étrangère via leur actionnariat. Un actionnaire étranger, surtout américain ou chinois, peut imposer des décisions stratégiques — choix des infrastructures, partenariats technologiques, localisation des données — qui compromettent la souveraineté revendiquée. Pire, certains fonds d'investissement ont des obligations légales de maximiser les profits, même au détriment de l'intérêt national.

2. Analyse par acteur : qui possède vraiment les "champions européens" ?

OVHcloud : une souveraineté menacée par l'actionnariat international

OVHcloud, souvent cité comme le fer de lance du cloud souverain européen, a une structure actionnariale problématique. Depuis 2016, KKR (fonds américain) et *TowerBrook* (fonds britannique) détiennent une part significative du capital. Bien que l'entreprise reste majoritairement contrôlée par son fondateur, Octave Klaba, ces fonds étrangers ont un droit de regard sur les décisions stratégiques. En 2020, KKR a même augmenté sa participation, ce qui soulève des questions sur l'autonomie réelle d'OVHcloud.

Risque concret : des clauses contractuelles imposées par ces actionnaires pourraient obliger OVHcloud à utiliser des infrastructures ou des services américains, ou à partager des données avec des entités sous juridiction étrangère. Sans contrôle public ou *golden shares*, la souveraineté d'OVHcloud reste fragile.

Mistral AI : un fleuron européen... financé par des fonds américains

Mistral AI incarne l'espoir d'une IA souveraine européenne, mais son actionnariat révèle une dépendance inquiétante. Lors de sa levée de fonds de 385 millions d'euros en juin 2024, Mistral AI a accueilli *Lightspeed Venture Partners*, un fonds de capital-risque américain, comme investisseur principal. *Lightspeed*, basé à Menlo Park en Californie, a ainsi obtenu un siège au conseil d'administration de Mistral AI.

Conséquence : un acteur américain a désormais un pouvoir de décision sur une entreprise présentée comme le champion de l'IA européenne.

Risque stratégique : *Lightspeed* pourrait influencer les choix technologiques de Mistral AI, par exemple en poussant à l'utilisation d'infrastructures AWS ou de GPU NVIDIA, ou en bloquant des partenariats avec des acteurs souverains. Sans garanties juridiques fortes, Mistral AI pourrait devenir un "cheval de Troie" où les données et les modèles européens seraient indirectement contrôlés par des intérêts américains.

Scaleway (Iliad/Free) : une infrastructure française, mais des composants étrangers

Scaleway, filiale du groupe Iliad (Free), est souvent cité comme une alternative souveraine à AWS. Pourtant, son modèle économique repose sur des composants étrangers. Iliad utilise massivement des équipements réseau Huawei (Chine) et des GPU NVIDIA (USA) pour ses data centers.

Problème : même avec un actionnariat 100% français, l'infrastructure dépend de fournisseurs étrangers, ce qui crée une dépendance technologique critique.

Risque : en cas de tension géopolitique (ex : embargo américain sur les GPU), Scaleway pourrait se retrouver incapable d'opérer sans ces composants. La souveraineté infrastructurelle nécessite un contrôle de toute la chaîne de valeur, pas seulement du capital.

Gaia-X : Le Projet Européen de Cloud Souverain... Infiltré par les GAFAM

Gaia-X, présenté comme l'alliance européenne pour un cloud souverain, souffre d'un paradoxe criant : Amazon, Google et Microsoft en sont membres via leurs filiales européennes. Ces géants américains participent aux groupes de travail et influencent les standards techniques du projet.

Conséquence : Gaia-X risque de devenir un cheval de Troie où les GAFAM définissent les règles du jeu en leur faveur, tout en bénéficiant du label "européen".

Exemple concret : en 2023, des membres de Gaia-X ont protesté contre la participation des GAFAM, arguant qu'elle sapait la crédibilité du projet. Sans exclusion des acteurs non-européens, Gaia-X ne peut pas garantir une vraie souveraineté.

S3NS : Un modèle à suivre ?

S3NS (*Secure SuperCloud for National Security*) est un projet français de cloud 100% public, porté par l'État et des banques publiques comme la BPI. Son actionnariat est entièrement contrôlé par des entités françaises, sans participation étrangère.

Avantage : les décisions stratégiques — localisation des données, choix des infrastructures, partenariats — ne peuvent pas être influencées par des intérêts étrangers.

Leçon : la vraie souveraineté passe par un actionnariat 100% national ou public, avec des garanties juridiques contre toute ingérence extérieure.

V - Les mécanismes de capture : Comment l'actionnariat étranger compromet la souveraineté

1. Le droit de regard sur les décisions stratégiques

Un actionnaire étranger, même minoritaire, peut imposer des vetos sur des décisions clés via des clauses contractuelles ou des droits de vote renforcés.

Exemple : un fonds américain pourrait bloquer un partenariat entre Mistral AI et un data center européen souverain, au profit d'AWS.

2. Les obligations de rentabilité

Les fonds d'investissement ont une obligation fiduciaire : maximiser les profits pour leurs investisseurs.

Conséquence : ils peuvent pousser à des choix technologiques moins chers mais moins souverains (ex : utiliser AWS plutôt que OVHcloud). Risque : la souveraineté devient un coût plutôt qu'un objectif.

3. Les clauses de sortie et les rachats

Les actionnaires étrangers peuvent exiger une vente de l'entreprise à un concurrent (ex : un GAFAM) pour réaliser leur investissement.

Exemple historique : en 2011, Skype (créé par des Européens) a été racheté par Microsoft pour 8,5 Md$, mettant fin à son indépendance. Sans protections juridiques, les "champions européens" peuvent être vendus au plus offrant.

4. L'accès aux données et aux technologies

Un actionnaire étranger peut exiger un accès aux données ou aux modèles d'IA développés par l'entreprise, sous prétexte de "due diligence" ou de "valorisation de l'investissement".

Exemple : en 2020, TikTok a été accusé de transférer des données européennes vers la Chine via son actionnariat chinois (ByteDance).

Risque : même sans contrôle majoritaire, un actionnaire étranger peut compromettre la confidentialité des données.

VI - Solutions concrètes : comment garantir une vraie Souveraineté ?

1. *Golden Shares* (Actions spéciales)

Principe : L'État ou une institution publique détient une action spécifique qui lui donne un droit de veto sur les décisions stratégiques (ex : choix des infrastructures, localisation des données, partenariats technologiques).

Exemple : En France, l'État détient une golden share dans EDF et Airbus, lui permettant de bloquer des décisions contraires à l'intérêt national.

Application possible : OVHcloud et Mistral AI pourraient adopter ce modèle pour bloquer toute influence étrangère sur leurs choix technologiques.

2. Financement 100% public et/ou européen

Principe : Éviter les fonds étrangers en se finançant via des banques publiques (BPI, BEI), des subventions européennes, ou des fonds souverains nationaux.

Exemple : S3NS est financé par l'État français et la BPI, sans participation étrangère.

Avantage : Aucun actionnaire étranger ne peut influencer les décisions.

Limite : Les fonds publics sont limités et peuvent ralentir la croissance. Solution : Combiner financement public et fonds européens souverains (ex : fonds souverain européen pour l'IA).

3. Audits indépendants et transparence

Principe : Imposer des audits réguliers par des organismes indépendants (ANSSI, CNIL, cour des comptes européenne) pour vérifier que :

- Les données restent localisées en Europe.
- Les infrastructures utilisées sont souveraines (pas de GPU NVIDIA, pas de cloud AWS).
- Les décisions stratégiques ne sont pas influencées par des intérêts étrangers.

Exemple : La CNIL pourrait auditer Mistral AI pour vérifier que aucune donnée européenne n'est transférée vers les USA via son actionnariat américain.

Outil : Créer un label "Souveraineté Vérifiée" pour les entreprises passant ces audits.

4. Contrôle public des acteurs clés

Principe : Nationaliser partiellement ou prendre une participation majoritaire publique dans les acteurs stratégiques (cloud, IA, semi-conducteurs).

Exemple : L'État français pourrait prendre une participation dans Mistral AI pour bloquer toute influence étrangère et garantir que les modèles d'IA restent souverains.

Modèle : Airbus (coentreprise publique/privée) montre qu'un contrôle partagé peut fonctionner tout en restant compétitif.

5. Interdiction des rachats par les GAFAM

Principe : Bloquer légalement tout rachat d'un acteur européen souverain par un GAFAM ou un fonds étranger.

Exemple : La loi européenne sur les investissements étrangers (2019) permet déjà de bloquer des rachats stratégiques. À étendre aux acteurs du numérique.

Application : Mistral AI et OVHcloud devraient être classés comme "actifs stratégiques", interdisant tout rachat par des entités non-européennes.

6. Actionnariat salarié et citoyen

Principe : Ouvrir le capital aux salariés et aux citoyens européens via des fonds dédiés ou des obligations souveraines.

Exemple : Linux Foundation est financée par des contributions de la communauté, ce qui limite l'influence des grands acteurs.

Avantage : Réduit la dépendance aux fonds étrangers et ancré l'entreprise dans l'écosystème européen.

VII - Études de cas : Le paradoxe en action (et les réponses stratégiques)

Cas 1 : OVHcloud vs. AWS – Résister par la niche et le droit, mais avec un actionnariat fragile

OVHcloud, leader européen du cloud souverain, illustre à la fois les succès et les limites d'une stratégie de souveraineté. Pour migrer vers OVHcloud, les entreprises doivent souvent passer par AWS, utilisant les outils de migration du géant américain, ce qui augmente temporairement leur dépendance. Pire, même après migration, elles dépendent souvent de composants américains comme les GPU NVIDIA ou les disques Western Digital.

Stratégie d'OVHcloud : l'entreprise mise sur le RGPD et la conformité réglementaire européenne pour attirer les clients sensibles aux données. Elle a aussi noué des partenariats avec l'État français, créant une demande captive via des contrats publics. Mais son actionnariat reste un point faible : depuis 2016, KKR (fonds américain) et TowerBrook (fonds britannique) détiennent une part significative du capital.

Risque : ces actionnaires pourraient influencer les décisions pour privilégier des solutions moins souveraines mais plus rentables.

Leçon : la souveraineté cloud est possible, mais elle nécessite un écosystème protégé — régulation, demande publique, ET un actionnariat contrôlé.

Chiffres clés (2025-2026) : OVHcloud compte 1,6 million de clients et a réalisé un chiffre d'affaires de 764 millions d'euros en 2025, avec une prévision de 850 millions d'euros en 2026 (source : rapport annuel OVHcloud 2025). AWS, de son côté, affiche plus de 100 millions de clients et un chiffre d'affaires de 90 milliards de dollars en 2025, avec une estimation de 100 milliards en 2026 (source : Amazon Q4 2025). Ratio : 1 euro investi chez OVHcloud correspond à 100 euros de chiffre d'affaires pour AWS, illustrant l'asymétrie économique massive entre les acteurs européens et américains.

Cas 2 : Mistral AI – Contourner les verrouillages par l'Open Source, mais avec un actionnariat américain

Mistral AI incarne l'espoir d'une IA souveraine européenne, mais son actionnariat pose question. Pour entraîner ses modèles, l'entreprise doit louer des GPU NVIDIA (contrôlés par les USA) et utiliser des frameworks américains (PyTorch, TensorFlow).

Stratégie de Mistral AI : elle mise sur l'open source radical en publiant ses modèles et leurs poids, créant ainsi un écosystème indépendant. Elle développe aussi des partenariats avec des data centers européens (OVHcloud, Scaleway) pour réduire sa dépendance aux clouds américains.

Mais son financement est problématique : lors de sa levée de 385 millions d'euros en juin 2024, Mistral AI a accueilli *Lightspeed Venture Partners*, un fonds américain, comme investisseur principal. *Lightspeed* a obtenu un siège au conseil d'administration, ce qui lui donne un pouvoir de décision sur une entreprise présentée comme le champion de l'IA européenne.

Risque stratégique : ce fonds pourrait influencer les choix technologiques de Mistral AI, par exemple en poussant à l'utilisation d'infrastructures AWS ou en bloquant des partenariats avec des acteurs souverains.

Leçon : l'open source permet une souveraineté algorithmique, mais la souveraineté infrastructurelle et décisionnelle nécessite un actionnariat contrôlé.

Chiffres clés (2025-2026) : Le coût d'entraînement de GPT-4 est estimé entre 60 et 100 millions de dollars (source : *The Information*, 2023). Celui de Mistral-8x22B est estimé entre 10 et 20 millions de dollars (source : Mistral AI, 2025). NVIDIA contrôle environ 80% du marché des GPU pour l'IA (source : *Mercury Research*, 2025), et Mistral AI dépend à 100% de ces GPU pour entraîner ses modèles, ce qui crée une dépendance technologique critique.

Cas 3 : Linux – La Souveraineté par la Collaboration, mais avec des Contributeurs Américains

Linux est le système d'exploitation open source le plus utilisé au monde, avec 100% des supercalculateurs et 90% des serveurs cloud l'utilisant (source : *TOP500* et *Cloud Market*, 2025). Pourtant, son écosystème dépend encore des géants.

Le paradoxe : Linux permet une souveraineté logicielle grâce à son code ouvert, mais ses principaux contributeurs sont des entreprises américaines comme Red Hat/IBM, Google et Intel. Les distributions les plus populaires (Ubuntu, Fedora) dépendent aussi de financements américains.

Stratégie de Linux : son modèle de développement distribué limite les points de contrôle uniques, et la Linux Foundation tente de diversifier ses sources de financement. Mais les utilisateurs dépendent souvent de matériel américain (Intel, NVIDIA), ce qui crée une dépendance infrastructurelle.

Leçon : l'open source permet une souveraineté collective, mais pas une souveraineté totale sans contrôle du matériel, des infrastructures ET de la gouvernance.

Cas 4 : Le RGPD – Une Régulation forte, mais contournée et affaiblie par les lobbyistes

Le RGPD, entré en vigueur en 2018, est la régulation la plus avancée au monde en matière de protection des données. Pourtant, les GAFAM le contournent systématiquement.

Le paradoxe : le RGPD interdit les transferts de données vers des pays sans protection adéquate, comme les États-Unis. Pourtant, les entreprises européennes doivent utiliser des services comme AWS, Google Cloud ou Microsoft 365, qui transfèrent les données vers les USA via des mécanismes comme les *Standard Contractual Clauses* (SCC) combinés à des mesures supplémentaires.

Stratégie européenne : la CNIL a infligé des amendes record à Meta (1,2 milliard d'euros entre 2023 et 2025), et le SecNumCloud impose des exigences strictes pour les clouds souverains. Mais les GAFAM contournent ces règles via des montages juridiques complexes et un lobbying intensif à Bruxelles.

Leçon : la régulation est nécessaire, mais insuffisante sans volonté politique d'application ET sans alternatives souveraines crédibles.

Chiffres clés (2025-2026) : Selon l'ANSSI, 60 à 70% des données européennes sont stockées sur des serveurs américains (source : *ANSSI*, 2025). La part des entreprises européennes pleinement conformes au RGPD est estimée à environ 30% (source : *Gartner*, 2025). Seulement 10% des transferts de données vers les USA respectent pleinement le RGPD, malgré les amendes (source : *CNIL*).

VIII - L'impact de l'IA : un nouveau champ de bataille

1. L'IA comme outil de domination accélérée

L'intelligence artificielle, et en particulier les *Large Language Models* (LLM), aggravent considérablement le paradoxe en introduisant de nouvelles formes de dépendance.

D'abord, les modèles *foundation* comme GPT-4 coûtent entre 60 et 100 millions de dollars à entraîner (source : *The Information*), un investissement que seuls les GAFAM et quelques startups bien financées peuvent se permettre.

Ensuite, NVIDIA contrôle environ 80% du marché des puces pour l'IA (source : *Mercury Research*, 2025), et les États-Unis peuvent interdire l'export de ces puces, comme ils l'ont fait pour la Chine en 2023.

Enfin, les GAFAM ont accès à 100 fois plus de données que les autres acteurs (source : *The Economist*, 2024), ce qui leur confère un avantage compétitif insurmontable pour les nouveaux entrants.

*Résulta*t : l'IA crée une nouvelle forme de dépendance, plus profonde que le cloud ou les logiciels, car elle touche à la fois aux infrastructures, aux données et aux compétences.

2. L'IA comme outil de souveraineté... mais avec des pièges

L'IA peut aussi aider à résoudre le paradoxe, mais attention à ne pas tomber dans de nouveaux pièges.

Par exemple, des outils comme *DependenSee* ou *CloudMapper* permettent d'automatiser les audits de dépendance, réduisant ainsi les coûts et les risques de migration. Cependant, ces outils sont souvent développés par des entreprises américaines, ce qui crée une nouvelle dépendance.

De même, *GitHub Copilot* (Microsoft) ou *Kubernetes* (Google) peuvent accélérer le développement d'alternatives souveraines, mais ils verrouillent les utilisateurs dans leurs écosystèmes.

Conclusion : l'IA peut être un outil de souveraineté, mais il faut éviter de tomber dans le piège de la dépendance aux outils des GAFAM, en privilégiant des alternatives européennes ou open source avec un actionnariat contrôlé.

IX - Pistes de résolution : une stratégie systémique, offensive et protégée

1. Accepter le Paradoxe... et le Gérer avec un actionnariat maîtrisé

Le paradoxe n'est pas une contradiction insurmontable, mais une tension dialectique qui nécessite une approche pragmatique et offensive.

D'abord, il faut engager un désenclavement progressif et ciblé : réduire les dépendances critiques — cloud, IA, données sensibles — en commençant par les secteurs stratégiques comme la santé, la défense, l'éducation, l'énergie et l'administration.

Par exemple, migrer les données de santé vers des clouds souverains comme OVHcloud ou Scaleway, en s'appuyant sur un calendrier réaliste et des garanties contractuelles, permet de limiter les risques tout en progressant vers l'objectif.

Ensuite, il faut bifurquer technologiquement en développant des alternatives souveraines — open source, infrastructures locales — et en les protégeant via un actionnariat contrôlé (golden shares, financement public). Mistral AI pourrait ainsi limiter l'influence de Lightspeed en introduisant une golden share détenue par l'État français.

Enfin, une hybridation contrôlée et temporaire est possible : utiliser les outils des géants de manière tactique, avec des garde-fous stricts comme des contrats imposant des clauses de sortie faciles et des pénalités en cas de non-respect. *Exemple* : utiliser AWS pour la transition vers OVHcloud, mais uniquement si OVHcloud garantit un actionnariat 100% européen à terme.

La réappropriation des compétences est tout aussi cruciale. Il faut former les talents — en IA, cloud, cybersécurité, droit du numérique — et créer des écosystèmes souverains via des partenariats entre universités, laboratoires et entreprises.

Par exemple, former 10 000 ingénieurs en IA souveraine d'ici 2030, comme le prévoit l'UE, en s'assurant que ces talents travaillent pour des entreprises à actionnariat européen, éviterait une fuite des cerveaux vers les GAFAM.

2. Stratégies concrètes par acteur

Pour les États

Réguler les Géants du Numérique avec des sanctions dissuasives

Les États doivent interdire les clouds étrangers pour les données sensibles, via des labels comme SecNumCloud en France. Ils doivent aussi taxer les revenus des GAFAM pour financer des alternatives locales, comme la taxe GAFA en France. Exiger la localisation des données — pas de stockage aux USA ou en Chine pour les données européennes — est une autre priorité. Enfin, il faut sanctionner les contournements avec des amendes proportionnelles au chiffre d'affaires mondial (ex : 10% du CA pour Meta en cas de non-respect du RGPD).

Mais ces mesures ne suffisent pas sans contrôle de l'actionnariat : les États doivent aussi classer les acteurs stratégiques (Mistral AI, OVHcloud) comme "actifs nationaux", interdisant tout rachat par des entités non-européennes.

Investir dans les infrastructures souveraines avec un actionnariat public

Les États doivent financer massivement les data centers souverains comme OVHcloud, Scaleway et 3DS Outscale, avec un budget de 10 milliards d'euros par an pour l'UE. Ils doivent aussi développer des supercalculateurs européens via EuroHPC et Jean Zay en France, pour l'entraînement des LLM. Pour les réseaux, il faut privilégier des acteurs européens comme Nokia et Ericsson pour la 5G/6G. Enfin, pour les semi-conducteurs, il faut renforcer STMicroelectronics et contrôler les partenariats avec TSMC pour éviter toute dépendance aux États-Unis ou à la Chine. Dans tous ces cas, l'État doit exiger un actionnariat majoritaire européen ou public pour garantir la souveraineté.

Promouvoir l'Open Source avec des garde-fous juridiques

Les États doivent financer des acteurs comme Mistral AI, Linux ou Nextcloud, mais sans dépendre des GAFAM.

Obliger les administrations à utiliser des logiciels open source est une autre mesure clé.

Créer une Fondation Européenne pour l'Open Source, indépendante des intérêts américains, permettrait de coordonner les efforts et d'éviter la capture par les géants. *Exemple* : la Linux

Foundation est aujourd'hui financée en partie par des GAFAM ; une fondation européenne 100% publique éviterait ce problème.

Construire des coalitions pour éviter l'isolement

Au niveau national, les partenariats public-privé (États + entreprises + universités) comme les initiatives de *spin off* et *de spin-in* « transferts défense/sécurité <-> entreprises technologiques civiles » sont aussi essentiels pour accélérer l'innovation. Il revient à l'Etat de les favoriser.

Les États doivent également former des alliances entre pays européens (UE + Royaume-Uni + Suisse + Norvège) pour mutualiser les ressources.

Enfin, une coopération Sud-Sud (Afrique + Amérique Latine + Asie) permettrait de réduire la domination USA/Chine et de créer un marché alternatif pour les technologies souveraines.

Pour les Entreprises

Auditer les dépendances et l'actionnariat

Les entreprises doivent identifier leurs dépendances critiques — cloud, logiciels, IA, données — et évaluer les risques associés : coût de sortie, perte de données, conformité RGPD. Elles doivent aussi auditer leur actionnariat : qui sont les investisseurs ? Ont-ils des liens avec les GAFAM ? Prioriser les migrations en commençant par les données sensibles et les secteurs stratégiques est une autre étape clé. *Exemple* : une entreprise utilisant AWS pour des données de santé doit migrer en urgence vers un cloud souverain à actionnariat européen vérifié.

Adopter une approche hybride et sécurisée

Les entreprises peuvent mixer cloud souverain et cloud public, mais uniquement avec des clauses de sortie strictes (ex : migration gratuite vers un autre cloud). Le multi-cloud — éviter la dépendance à un seul fournisseur — est une autre stratégie pertinente. Enfin, l'open core — utiliser des versions open source + services payants souverains — permet de réduire les coûts tout en restant indépendant. Mais dans tous les cas, il faut vérifier que les fournisseurs ont un actionnariat contrôlé.

Développer des alternatives internes avec un financement souverain

Les entreprises doivent créer des outils open source pour remplacer les solutions propriétaires, former leurs employés aux alternatives souveraines, et participer à des communautés open source indépendantes des GAFAM. *Exemple* : plutôt que d'utiliser GitHub (Microsoft), une entreprise peut contribuer à GitLab (qui a une version open source) ou à Gitea (100% open source). Mais il faut aussi s'assurer que ces alternatives ne sont pas contrôlées par des fonds étrangers.

Exiger la transparence et des garanties juridiques

Les entreprises doivent auditer les contrats avec leurs fournisseurs, négocier des clauses de sortie faciles (ex : migration gratuite vers un autre cloud), et exiger des certifications comme SecNumCloud ou ISO 27001. Elles doivent aussi vérifier que leurs fournisseurs — cloud, IA, logiciels — ont un actionnariat souverain, sans influence étrangère.

Pour les Citoyens

Choisir des alternatives souveraines et vérifiées

Les citoyens peuvent opter pour des alternatives souveraines dans leur vie quotidienne.

Pour le moteur de recherche, Qwant (France) est une option, tout comme SearX (open source). Pour la messagerie, Olvid (France) ou Matrix (open source) sont préférables à WhatsApp (Meta).

Pour le cloud, OVHcloud ou Scaleway (à condition de vérifier leur actionnariat) sont meilleurs que AWS ou Google Drive. Pour l'IA, Mistral AI (France) est une alternative à ChatGPT, mais il faut rester vigilant sur son actionnariat.

Pour le système d'exploitation, Linux (Ubuntu, Debian) ou /e/OS (France) sont préférables à Windows ou macOS.

Enfin, pour la bureautique, LibreOffice ou OnlyOffice sont des alternatives à Microsoft 365.

Sensibiliser et Éduquer

Les citoyens doivent comprendre les enjeux de la souveraineté numérique, former leurs enfants à l'utilisation d'outils souverains, et soutenir les projets *open source* via des dons ou des contributions. *Exemple* : contribuer à Linux ou Mistral AI permet de renforcer les alternatives souveraines.

X - Scénarios futurs : des futurs possibles, mais inégaux

Scénario 1 : Domination totale des GAFAM/BATX (Probabilité : 40%)

Description : Les géants renforcent leur emprise via l'IA, le cloud et les données, en écrasant toute concurrence et en capturant les acteurs européens via leur actionnariat.

Facteurs clés : l'échec des régulations (DMA, AI Act contournés par les GAFAM), le manque d'alternatives crédibles (Mistral AI et OVHcloud ne reçoivent pas assez de soutien et restent sous influence étrangère), l'adoption massive de l'IA des GAFAM (les entreprises et États renoncent à développer leurs propres solutions), et la guerre économique (les GAFAM achètent ou étouffent tous les concurrents émergents).

Conséquences : perte totale de souveraineté pour les États et entreprises, surveillance de masse généralisée via l'IA et le cloud, mais innovation rapide — bien que contrôlée par les USA et la Chine.

Scénario 2 : Équilibre des Pouvoirs (Probabilité : 35%)

Description : Coexistence tendue entre géants et alternatives souveraines, grâce à une régulation forte, des investissements massifs et un actionnariat contrôlé.

Facteurs clés : le succès des régulations (DMA, AI Act efficaces avec des sanctions dissuasives et l'interdiction des rachats par les GAFAM), l'émergence d'alternatives crédibles (Mistral AI, OVHcloud, RISC-V reçoivent un soutien public massif et protègent leur actionnariat), l'adoption d'une approche hybride (les États et entreprises mixent souveraineté et outils des GAFAM avec des garde-fous stricts), et la coopération internationale (UE + Royaume-Uni + Suisse unissent leurs forces).

Conséquences : souveraineté partielle pour les États et entreprises, diversité des solutions (moins de monopoles), mais complexité accrue (multi-écosystèmes) et coûts plus élevés (pas d'économies d'échelle).

Scénario 3 : Fragmentation numérique (Probabilité : 20%)

Description : Le monde numérique se fragmente en blocs (USA, Chine, UE, Russie), avec peu d'interopérabilité.

Facteurs clés : la montée des nationalismes numériques (chaque bloc impose ses propres standards), l'échec des standards ouverts (les GAFAM et les acteurs chinois refusent de collaborer), et les guerres commerciales et sanctions (les USA interdisent les puces NVIDIA à la Chine, qui développe ses propres alternatives).

Conséquences : souveraineté totale pour chaque bloc, mais perte d'interopérabilité (silos technologiques), ralentissement de l'innovation (moins de collaboration) et guerre technologique (cyberattaques, espionnage).

Scénario 4 : Révolution Open Source (Probabilité : 5%)

Description : L'open source domine le monde numérique, grâce à une coalition mondiale et un actionnariat souverain.

Facteurs clés : le succès des modèles open source (Mistral, Llama, RISC-V deviennent des standards avec un actionnariat 100% européen ou public), l'adoption massive par les États et entreprises (les gouvernements imposent l'open source et financent massivement les acteurs souverains), le financement durable (fonds publics, dons, modèles économiques innovants), et la protection contre les GAFAM (les États interdisent les rachats et taxent les géants pour financer l'open source).

Conséquences : souveraineté pour tous (États, entreprises, citoyens), innovation accélérée (collaboration mondiale), réduction des coûts (pas de monopoles), mais manque de soutien commercial (modèles économiques à inventer).

XII - Conclusion : Le paradoxe est gérable, mais la guerre est inévitable

Le paradoxe de la souveraineté numérique n'est pas une contradiction logique, mais une tension dialectique qui révèle la profondeur des asymétries de pouvoir dans l'économie numérique mondiale.

Les GAFAM/BATX ne laisseront pas émerger de concurrents par bienveillance : ils les combattront par tous les moyens — rachats, lobbying, prédation économique, contrôle des infrastructures.

Pire encore, même les acteurs présentés comme "souverains" — OVHcloud, Mistral AI — peuvent être compromis par leur actionnariat, qui donne à des fonds américains ou britanniques un pouvoir de décision sur des choix stratégiques.

La résolution du paradoxe passe par quatre piliers, appliqués de manière systémique, offensive ET protégée :

Désenclavement progressif : Réduire les dépendances critiques — cloud, IA, données — en ciblant les secteurs stratégiques, avec des garanties sur l'actionnariat des fournisseurs.

Bifurcation technologique : Identifier, notamment au moyen d'instruments puissants de veille et d'intelligence technique et scientifique, ainsi que de programmes appropriés de recherche stratégique de caractère spéculatif, financer et développer des alternatives souveraines — open source, infrastructures locales — et les protéger via un actionnariat contrôlé (golden shares, financement public, audits indépendants).

Hybridation contrôlée : Utiliser les outils des géants de manière tactique et temporaire, avec des garde-fous stricts (contrats, clauses de sortie, certifications) ET une sortie planifiée vers des alternatives souveraines à actionnariat européen.

Réappropriation des compétences : Former massivement les talents (10 000 ingénieurs d'ici 2030, clauses de non-délocalisation) et s'assurer qu'ils travaillent pour des entreprises à actionnariat européen, pour éviter la fuite des cerveaux et la dépendance cognitive. Créer des écosystèmes souverains et attractifs (salaires compétitifs, projets ambitieux, reconnaissance internationale). Renforcer la coopération européenne (mobilité des talents, partage des connaissances, projets communs). Sensibiliser les talents aux défis de la souveraineté (campagnes sur l'importance stratégique, fierté européenne).

Protéger les compétences souveraines des licornes européennes **:** *golden shares*, financements publics, interdiction des rachats par des tiers non européens.

La clé du succès réside dans l'équilibre : ni dépendance totale (risque de perte de souveraineté), ni autarcie totale (risque d'isolement et de retard technologique).

Mais surtout, elle réside dans le contrôle : sans maîtrise de l'actionnariat, la souveraineté n'est qu'une illusion.

La souveraineté numérique est un marathon, pas un sprint. Les acteurs qui comprennent ce paradoxe, anticipent les stratégies des GAFAM/BATX et de leurs satellites technologiques, protègent leur actionnariat ET agissent de manière systémique et offensive seront ceux qui prévaudront dans l'économie numérique de demain.

"La souveraineté, c'est comme la liberté : ça ne se donne pas, ça se prend. Et dans le monde numérique, ça se prend par des actes concrets : désenclaver, bifurquer, hybrider (temporairement), réapproprier — et surtout, contrôler qui vous possède."

Annexes techniques

1. Architectures techniques et dépendances systémiques

OVHcloud : une infrastructure européenne avec des composants critiques étrangers

OVHcloud repose sur une stack logicielle open source (OpenStack pour l'orchestration, Kubernetes pour la « conteneurisation »[4], Ceph pour le stockage distribué) déployée dans des data centers situés en France, Allemagne, Pologne et Royaume-Uni.

Problème systémique : malgré cette localisation européenne, l'infrastructure matérielle dépend de composants américains (GPU NVIDIA pour les services d'IA, disques Western Digital pour le stockage) et de réseaux utilisant des équipements Huawei (Chine) pour certaines interconnexions.

Conséquence : une dépendance technologique cachée persiste même après migration, car les fournisseurs de matériel (NVIDIA, WD) et les outils de gestion (ex : outils de monitoring souvent développés par des éditeurs américains) restent sous contrôle étranger.

Solution partielle : OVHcloud développe des partenariats avec des fabricants européens (ex : collaboration avec SiPearl pour des puces souveraines), mais la chaîne d'approvisionnement reste majoritairement extra-européenne.

Mistral AI : une souveraineté algorithmique limitée par des dépendances infrastructurelles

Mistral AI utilise une architecture distribuée pour l'entraînement de ses modèles : les GPU NVIDIA H100 (indispensables pour le calcul intensif) sont loués via des data centers partenaires (OVHcloud, AWS, GCP) ou des clusters dédiés.

Stack logicielle : *PyTorch* (Meta) pour le framework, *Hugging Face Transformers* pour les bibliothèques, et des outils internes pour l'optimisation. Dépendance critique : 100 % des GPU sont de NVIDIA, et les frameworks dominants (*PyTorch, TensorFlow*) sont développés par des GAFAM.

Paradoxe technique : Mistral AI publie ses modèles en open source (souveraineté algorithmique), mais ne contrôle pas l'infrastructure (dépendance aux GPU et aux clouds).

Piste de résolution : développement de frameworks européens (ex : contributions à JAX de Google, mais avec des alternatives open source) et partenariats avec des fabricants de puces souveraines (ex : SiPearl, Intel IDM 2.0 en Europe).

Scaleway : une approche hybride avec des verrouillages matériels

Scaleway (Iliad) combine des serveurs standard x86 (Intel, AMD) et des accélérateurs GPU (NVIDIA) dans ses data centers français.

Architecture réseau : utilisation de matériel Huawei pour les routeurs et switches, et de solutions open source (Open vSwitch, BGP) pour la gestion du trafic.

---

[4] La conteneurisation est une technologie qui isole une application et ses dépendances dans un conteneur léger et portable, permettant de :

- L'exécuter de manière cohérente sur n'importe quel environnement (cloud, serveur, machine locale).
- Éviter les conflits entre applications ou avec le système hôte.
- Déployer et mettre à l'échelle rapidement (ex : Docker, Kubernetes).

Analogie : comme une boîte de transport qui contient tout ce dont l'application a besoin (code, bibliothèques, configurations), sans dépendre de l'ordinateur sous-jacent.

Problème systémique : la dépendance aux fournisseurs de matériel (NVIDIA pour les GPU, Huawei pour le réseau) crée un risque de rupture d'approvisionnement en cas de tensions géopolitiques.

Solution envisagée : diversification vers des fournisseurs européens (ex : puces RISC-V, équipements réseau Nokia) et stockage stratégique de composants critiques.

2. Tableaux comparatifs techniques

Comparatif des dépendances infrastructurelles des clouds souverains

Acteur	Localisation data centers	Stack logicielle	Matériel serveur	Matériel réseau	GPU IA	Certifications
OVHcloud	FR/DE/PL/UK	OpenStack, Kubernetes	Intel, AMD	Huawei, Cisco	NVIDIA (USA)	SecNumCloud 3.2, ISO 27001
Scaleway	FR	OpenStack, Kubernetes	Intel, AMD	Huawei	NVIDIA (USA)	SecNumCloud (en cours)
AWS	Mondial	Propriétaire	Intel, AMD, Graviton	Cisco, Juniper	NVIDIA (USA)	ISO 27001, SOC 2
S3NS	FR (100 % public)	OpenStack	Européen (cible)	Européen (cible)	Européen (cible)	SecNumCloud 3.2

Comparatif des frameworks d'IA et de leurs dépendances

Framework	Développeur	Licence	Dépendances matérielles	Écosystème	Souveraineté possible
PyTorch	Meta (USA)	BSD	GPU NVIDIA (CUDA)	Large (GAFAM)	Non
TensorFlow	Google (USA)	Apache 2.0	GPU NVIDIA, TPU Google	Large (GAFAM)	Non
JAX	Google (USA)	Apache 2.0	GPU NVIDIA, TPU Google	Croissant	Partielle (open source)
Flux (Apple)	Apple (USA)	Propriétaire	GPU Apple Silicon	Fermé	Non
Poplar (Graphcore)	Graphcore (UK)	Propriétaire	IPU Graphcore	Spécialisé	Oui (matériel UK)

3. Schémas d'architecture et de dépendance

Schéma 1 : Chaîne de dépendance lors d'une migration cloud vers un acteur souverain

```
graph LR
    A[Entreprise] -->|1. Hébergement initial| B[AWS/Google Cloud]
    B -->|2. Outils de migration| C[AWS Migration Hub]
    C -->|3. Transfert progressif| D[OVHcloud/Scaleway]
```

D -->|4. Dépendances résiduelles| E[GPU NVIDIA]

D -->|4. Dépendances résiduelles| F[Disques Western Digital]

E -->|Contrôlés par| G[USA]

F -->|Contrôlés par| G

D -->|5. Outils de gestion| H[OpenStack/Kubernetes]

H -->|Développé par| I[Communauté open source + éditeurs]

I -->|Influence| J[GAFAM]

Explication : Ce schéma illustre comment une migration vers un cloud souverain ne supprime pas toutes les dépendances. Les étapes 4 et 5 montrent que l'infrastructure matérielle (GPU, disques) et les outils de gestion (même open source) peuvent rester sous influence étrangère.

Schéma 2 : Architecture technique de Mistral AI et ses verrouillages

graph TD

A[Mistral AI] -->|1. Entraînement| B[Cluster GPU]

B -->|2. Matériel| C[GPU NVIDIA H100]

C -->|3. Contrôle| D[USA : NVIDIA + Cloud Act]

A -->|4. Frameworks| E[PyTorch/TensorFlow]

E -->|5. Développeur| F[Meta/Google USA]

A -->|6. Données| G[Datasets publics/privés]

G -->|7. Stockage| H[AWS/GCP/OVHcloud]

H -->|8. Localisation| I[Europe/USA]

A -->|9. Publication| J[Modèles open source]

J -->|10. Utilisation| K[Communauté mondiale]

Explication : Mistral AI contrôle l'algorithme (via l'open source) mais pas l'infrastructure (GPU NVIDIA, frameworks GAFAM, stockage potentiellement aux USA). Le verrouillage est systémique : même avec une souveraineté algorithmique, les dépendances matérielles et logicielles persistent.

Schéma 3 : Cartographie des verrouillages technologiques dans l'écosystème IA européen

graph TD

A[Modèle IA européen] -->|1. Dépend au framework| B[PyTorch/TensorFlow]

B -->|2. Développé par| C[GAFAM USA]

A -->|3. Nécessite des GPU| D[GPU NVIDIA]

D -->|4. Contrôlé par| E[USA : NVIDIA + export controls]

A -->|4. Utilise des outils| F[Hugging Face, Weights & Biases]

F -->|5. Hébergé sur| G[AWS/GCP]

G -->|6. Soumis à| E

A -->|7. Données d'entraînement| H[Datasets]

H -->|8. Stocké sur| G

H -->|9. Provenance| I[USA/UE/Autres]

Explication : Ce schéma montre tous les points de verrouillage dans la chaîne de valeur de l'IA : frameworks, matériel, outils, stockage, et données. Chaque dépendance renforce le contrôle des GAFAM sur l'écosystème européen.

4. Glossaire des concepts techniques clés

Cloud Act : loi américaine de 2018 qui oblige les entreprises américaines (et leurs filiales) à transmettre les données stockées à l'étranger aux autorités US, même sans mandat local.

Impact technique : toute entreprise utilisant AWS, Google Cloud ou Azure doit considérer que ses données peuvent être accessibles par les USA, même si elles sont physiquement en Europe.

SecNumCloud : label de sécurité français (ANSSI) pour les services cloud, avec trois niveaux (1 : base, 2 : renforcé, 3.2 : souveraineté maximale).

Exigences clés : localisation des données en France, contrôle exclusif par des entités françaises, et audits *ré*guliers.

Acteurs certifiés : OVHcloud (niveau 3.2), Outscale, Scaleway (en cours).

Path Dependence **(Dépendance aux sentiers)** : concept économique (Douglass North) expliquant comment les choix technologiques passés (ex : adoption de Windows, AWS) verrouillent les organisations dans une trajectoire, rendant les changements coûteux et risqués.

Application au cloud : migrer de AWS vers OVHcloud peut coûter 10 à 100 fois le budget annuel de cloud, à cause des coûts de réécriture des applications, de la reformation des équipes, et des risques de compatibilité.

GPU **(*Graphics Processing Unit*)** : processeur spécialisé dans le calcul parallèle, indispensable pour l'entraînement des modèles d'IA.

Problème systémique : NVIDIA contrôle 80 % du marché (source : Mercury Research 2025), et ses GPU (ex : H100, A100) sont optimisés pour ses propres bibliothèques (CUDA), créant un verrouillage technique (difficile d'utiliser d'autres GPU sans réécrire le code).

Framework d'IA : bibliothèque logicielle (ex : *PyTorch, TensorFlow*) qui simplifie le développement des modèles d'IA.

Dépendance critique : les frameworks dominants sont développés par les GAFAM (PyTorch par Meta, TensorFlow par Google), et optimisés pour leurs infrastructures (ex : TensorFlow avec les TPU de Google).

Conséquence : même en utilisant un framework open source, les performances sont meilleures sur les infrastructures des GAFAM.

Standard Contractual Clauses **(SCC)** : clauses contractuelles types de la Commission européenne pour encadrer les transferts de données vers des pays tiers (ex : USA).

Limite technique : les SCC ne protègent pas contre le *Cloud Act*, car elles sont subordonnées aux lois américaines (ex : *FISA, Cloud Act*) qui priment sur les contrats privés.

5. Analyse systémique des verrouillages technologiques

A - La chaîne de dépendance dans le cloud

Le verrouillage cloud repose sur **quatre couches interdépendantes** :

Couche 1 : Matérielle

GPU/TPU : NVIDIA (80 % du marché) et Google (TPU) contrôlent les accélérateurs indispensables pour l'IA.

Disques/SSD : Western Digital, Seagate, Samsung (tous sous influence USA/Corée du Sud) dominent le stockage.

Réseau : Cisco, Juniper, Huawei (USA/Chine) fournissent les équipements d'interconnexion.

Conséquence : même avec un cloud européen, l'infrastructure matérielle reste dépendante.

Couche 2 : Logicielle

Hyperviseurs : VMware (USA), KVM (open source mais dominé par Red Hat/IBM USA).

Orchestration : Kubernetes (développé par Google, maintenant CNCF).

Stockage distribué : Ceph (open source, mais contributions majeures de Red Hat/IBM).

Conséquence : les outils de gestion du cloud sont souvent développés ou contrôlés par les GAFAM.

Couche 3 : Données

Localisation : les GAFAM stockent les données où ils veulent (ex : AWS peut répliquer des données européennes aux USA).

Format : les données sont souvent verrouillées dans des formats propriétaires (ex : bases de données Amazon RDS).

Transfert : les coûts de sortie (*egress fees*) peuvent être prohibitifs (ex : 0,12 $/Go pour AWS).

Conséquence : migrer ses données d'un cloud GAFAM vers un cloud souverain coûte cher et prend du temps.

Couche 4 : Écosystème

Services managés : les GAFAM proposent des services intégrés (ex : AWS Lambda, Google BigQuery) qui verrouillent les utilisateurs.

Certifications : les certifications sectorielles (ex : HIPAA pour la santé) sont souvent plus faciles à obtenir avec les GAFAM.

Support : le support 24/7 et les SLA (Service Level Agreements) des GAFAM sont difficiles à égaler pour les acteurs souverains.

Conséquence : les avantages écosystémiques des GAFAM compensent souvent leurs inconvénients (coût, souveraineté).

B - Solution systémique : pour briser ces verrouillages, il faut agir sur toutes les couches simultanément :

- *Matérielle* : développer des puces souveraines (ex : SiPearl, RISC-V).
- *Logicielle* : utiliser des alternatives open source (ex : OpenStack, Kubernetes).
- *Données* : exiger des clauses de sortie gratuite et des formats ouverts.
- *Écosystème* : créer des partenariats publics-privés pour offrir des services comparables.

Dernière mise à jour : 3 juin 2026

Sources :

- ANSSI (2025), *Rapport sur la souveraineté numérique et la localisation des données*
- CNIL (2025), *Sanctions RGPD et transferts de données vers les États-Unis*
- CJUE, *Arrêts sur le Privacy Shield (2020) et les Standard Contractual Clauses*
- Mercury Research (2025), *Parts de marché des GPU pour l'IA*
- The Information (2023-2025), *Coûts d'entraînement des LLM (GPT-4, Mistral-8x22B)*
- Rapports parlementaires français et européens (2024-2026), *Stratégies de souveraineté numérique*
- Études académiques : Zuboff (*L'Âge du capitalisme de surveillance*), Stiegler (*La Société automatique*), North (*Institutions, Institutional Change and Economic Performance*)
- Lightspeed Venture Partners (2024), *Investissement dans Mistral AI*
- KKR et TowerBrook (2016-2026), *Participation dans OVHcloud*