Cloud et dépendances numériques : vers une autonomie stratégique européenne

Par Frédéric Tatout et Louis Cougouille – 22 avril 2026.

Table des matières

I/ Le Cloud : de quoi s'agit-il ?

L'informatique en nuage (« cloud ») combine un réseau à haut débit, une grande puissance de calcul, et la capacité à s'abstraire de leur matérialité.

Le concept est antérieur au Web 2.0 du début de la décennie 2010, qui a permis son émergence par[1] :

- L'Internet à haut débit partout (ADSL et fibre),
- la mutualisation de serveurs, permettant de cumuler une grande capacité de calcul,
- la virtualisation, une innovation qui permet d'accéder aux ressources de stockage et de calcul de manière flexible, sans devoir se préoccuper de leur matérialité,

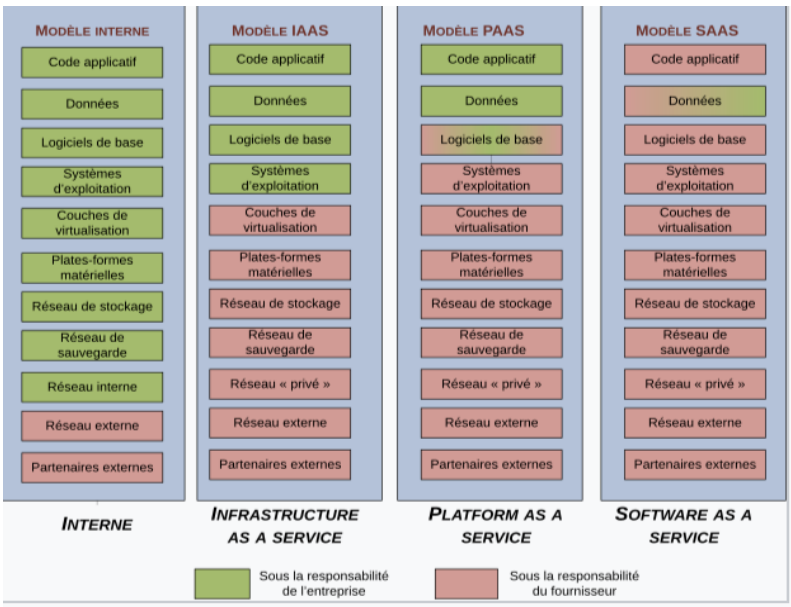
Depuis, le Cloud est devenu un modèle d'organisation incontournable.

Le web 2.0 a vu éclore des offres commerciales proposant aux entreprises clientes ***d'accéder aux ressources informatiques dont elles ont strictement besoin à chaque instant, et de ne payer que leur consommation effective, avec à la clé un gain financier conséquent et la décharge des activités de gestion associées[2].***

Le bouquet de services peut dépasser largement l'accès à de la puissance de calcul et à du stockage, comme précisé ci-dessous - Crédit : wikipédia (ici).

[1] Les deux premiers aspects ont hérité de deux décennies de normalisation et de R&D, notamment en calcul de haute performance

[2] plus besoin d'investir dans un parc de machines répondant au maximum du besoin en ressource



Cette représentation des différents modèles de service montre comment les responsabilités sont théoriquement réparties suivant les modèles internes, IaaS, PaaS, SaaS.

L'accès aux serveurs peut être local, s'ils sont sur le site de l'entreprise (« on premises »). Mais dans la majorité des cas il se fait via Internet : les données sont stockées dans l'immenses fermes de serveurs, sans restriction géographique a priori, ce qui pose des problématiques de dépendance que nous verrons plus bas.

L'abaissement des barrières financières et en compétences a boosté l'innovation dans le numérique et conduit en moins de 10 ans à une restructuration profonde de la chaîne de valeur du numérique.

- pour les utilisateurs, les enjeux de flux de données et d'accès aux capacités de traitement ont (de manière schématique) remplacé les problématiques d''acquisition et de gestion de parc[3] ;
- en parallèle, les géants du numérique des années 2000 ont été supplantés par les GAFAM[4].

On peut faire une analogie avec la seconde révolution industrielle née du remplacement (typiquement dans les entreprises textiles) de la force motrice d'une seule machine à vapeur (ou un gros moteur) avec ses nombreuses poulies, par un réseau d'alimentation électrique qui alimente des moteurs plus petits, autonomes, chacun montés sur une machine. La vague d'innovations liée à cette évolution s'est étendue sur un demi-siècle. Celle du Cloud, conduisant au « Big data », n'aura duré en gros qu'une décennie.

Cette révolution du numérique a débouché sur l'ubérisation[5] et ouvert la voie à deux autres mutations en cours du numérique :

- celle du *No code* qui permet (en principe) de s'affranchir de toute compétence en informatique pour automatiser quasiment tout comme présenté ici ;
- celle des modèles pré entraînés à partir d'immenses quantités de données, accessibles en ligne en langage naturel (le prompt)[6], comme des LLM (ChatGPT, Claude, etc.).

De manière structurelle, *en irrigant quasiment tous les pans de l'économie physique, structurés initialement par domaines de spécialité pyramidaux* (typiquement, un intégrateur et une sous-traitance plus ou moins éparse), ***le Cloud permet son réagencement par catégories d'usages en accroissant la prééminence de la donnée***. C'est ainsi que des startups comme Tesla, Uber ou SpaceX / Starlink ont pu s'arroger le leadership en attaquant d'emblée leur cœur de cible à partir de 4 leviers : maîtrise de la donnée, accès direct à la clientèle, verticalisation industrielle et force d'impact financière. Les circuits de financement puissants ont été déterminants dans cette réussite aux Etats-Unis (fonds privés et DARPA) comme en Chine (bras financier de l'Etat soutenu par la masse énorme de l'épargne des citoyens).

Les tentatives nationales et européennes pour tenter de recréer un acteur du Cloud local ne pouvaient qu'échouer face à l'écrasante supériorité technologique et financière des GAFAM ; non pas que les compétences technologiques soient déficientes en Europe, loin de là. Mais deux verrous opérationnels se posaient au minimum : celui du passage à l'échelle (scalabilité) et l'incapacité à proposer un écosystème de

[3] Ici : ordinateurs et logiciels.
[4] En 2000 : IBM, HP, Alcatel, SAP, etc. Depuis : GAMA (Google, Amazon, META, Apple), liste à laquelle il est d'usage d'ajouter un M pour Microsoft qui est resté un géant : ce sont les GAFAM devenus GAMAM, et en Chine : Baidu, Alibaba, Tencent, Xiaomi (les BATX).
[5] Avec des leaders emblématiques comme Uber, Netflix, Airbnb, Tesla, etc.
[6] Les autres les plus connus en Occident sont : BERT, BLOOM d'origine française, LlaMA, MISTRAL (français), Gemini, Grok.

services complet. En France, des initiatives comme CloudWatt et Numergy ont ainsi échoué, en raison de la taille limitée du marché national, de choix technologiques discutables (comme l'adoption prématurée par CloudWatt de la virtualisation réseau OpenContrail en 2012) et d'une stratégie commerciale inadaptée. Par exemple, CloudWatt a initialement lancé une offre de stockage sans solution de calcul associée, ne répondant pas aux attentes réelles du marché. En Europe, l'initiative au départ franco-allemande GAIA-X a accouché de 3 niveaux de labels, après de longues péripéties.

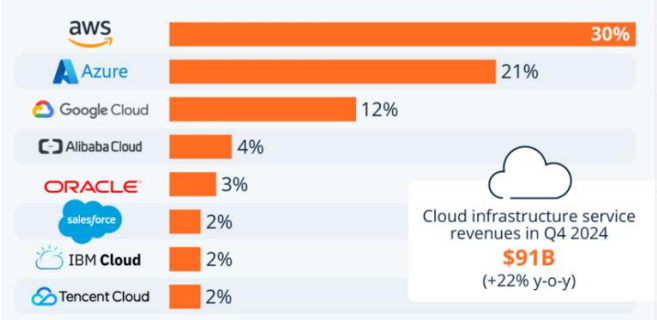
AWS est à la fois un précurseur et un cas d'école. Comme il émane du système d'information interne d'Amazon et de son approche self-service et API-first entre ses Business Units, il est né avec une grande longueur d'avance. A contrario, il aurait été impossible pour un « pure player » de petite taille comme OVH de proposer un bouquet d'offre attractif sans nouer des partenariats : au départ, surtout avec des acteurs anglo-saxons, à présent en majorité avec des acteurs français et européens. Comme les fournisseurs de « Cloud de confiance » français et européens, il s'est également appuyé sur des briques de logiciels libres (cf. plus bas).

Parts de marché des leaders (France en 2025 et monde en 2024)

Parts de marché du cloud en France en 2025

Fournisseur	Part de marché estimée (2025)
Amazon Web Services (AWS)	~30-35%
Microsoft Azure	~25-30%
Google Cloud	~10-15%
OVHcloud	~5-10%
Oracle Cloud	~3-5%
Autres	~10-15%

Source : Statista[7]



2/ Effets sur l'environnement

Sur le plan environnemental, on peut noter deux effets importants.

Premièrement, à parc installé équivalent, la mutualisation des ressources permet de mieux amortir les capacités installées (comme, en transport, le co-voiturage et la mutualisation des flottes automobiles) et de moins consommer par unité de calcul réalisé, du fait du rajeunissement du parc. Ayant suivi la restructuration de la chaîne de valeur évoquée plus haut, ce fut un **ajustement transitoire, d'impact positif**.

En regard, l'***effet rebond est inévitable.*** Il s'explique par plusieurs facteurs, notamment la banalisation progressive de toutes les ressources, dont les prix baissent ; les méthodes de mise en œuvre, sous forme modulaire et avec un travail de plus en plus réduit d'optimisation[8] ; et par extension, les effets des mutations induites. Il en résulte des gaspillages de plus en plus massifs de ressources planétaires. La croissance des infrastructures de cloud est aujourd'hui portée par l'essor fulgurant de l'IA et se traduit par une consommation massive d'énergie, d'eau et de terres rares, avec des investissements records dans les data centers (620 milliards de dollars en 2026, quatre fois plus qu'en 2023). Les GPU, cœurs des Large Language Models (LLMs), nécessitent des métaux rares et une pureté extrême, dopant la demande en silicium, cuivre et terres rares, avec un risque de pénuries et de conflits d'usage. La consommation électrique des data centers, boostée par l'IA, pourrait tripler d'ici 2030, représentant jusqu'à 1 500 TWh/an – l'équivalent de trois fois la production française. Les émissions de CO_2 de ces infrastructures pourraient dépasser celles de la France, tandis que leur soif en eau (5 000 milliards de litres en 2023) menace les ressources locales.

[7] https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/
[8] Exemple : il est souvent bien plus coûteux et fastidieux d'effacer les disques durs que de les recopier et empiler.

La croissance du marché mondial se fait donc à un rythme effréné et ne va pas s'arrêter de sitôt : **l'effet rebond, aux impacts délétères, est donc voué à perdurer**, sauf à être infléchi ou stoppé par une crise mondiale, une mutation des paradigmes de développement, une rupture technologique ou une réglementation effective des marchés.

Aujourd'hui, la majorité des modèles d'IA reposent sur des architectures gourmandes en énergie (GPU et LLM), mais **des alternatives émergent**. Des acteurs comme DeepSeek[9] ont prouvé qu'il est possible d'entraîner des modèles performants avec moins de ressources. Mistral AI[10], de son côté, se distingue par une transparence sur son impact environnemental et une consommation électrique divisée par quatre par rapport à la moyenne du secteur. Côté hardware, NVIDIA, bien que dominant, voit sa position remise en question par des concurrents comme AMD (avec ses puces Instinct MI300X), Intel (qui prépare des puces moins énergivores grâce à une gravure innovante), et même des géants du cloud comme Google, Amazon et OpenAI, qui développent leurs propres puces pour réduire leur dépendance et optimiser leurs coûts.

Parmi d'autres pistes prometteuses, les "world models" (modèles du monde) gagnent du terrain : ces architectures, défendues par des figures comme Yann LeCun (ex-Meta, désormais à la tête d'AMI Labs à Paris) ou Fei-Fei Li (World Labs), visent à modéliser la physique et les interactions du monde réel, permettant une compréhension causale et une planification bien plus efficace que les LLM actuels. En 2025-2026, des projets comme Marble (World Labs) ou Genie 3 (DeepMind) ont montré qu'il était possible d'entraîner des IA capables de simuler des environnements complexes, avec des applications en robotique ou en simulation industrielle, tout en réduisant la dépendance aux données massives et aux calculs énergivores.

La régulation et la souveraineté technologique accélèrent aussi la transition. En Europe, la directive sur l'efficacité énergétique impose désormais aux data centers de valoriser leur « chaleur fatale » et de respecter des normes strictes (PUE ≤ 1,4, récupération d'énergie, audits obligatoires). La France, avec son mix nucléaire bas-carbone, attire des projets de méga-centres (comme celui de Mistral AI en Essonne ou de Data4 dans le Nord), mais sous condition de sobriété et d'innovation. Ces cadres légaux, couplés à la montée en puissance de modèles open-source et souverains, pourraient infléchir la courbe de la surconsommation à condition que l'effet rebond (où les gains d'efficacité entraînent une hausse globale des usages) soit maîtrisé par des choix politiques et industriels ambitieux.

3/ Quels enjeux de souveraineté ?

a/ Souveraineté numérique : entre gestion des dépendances et ambiguïtés d'un concept

La notion de souveraineté, souvent mobilisée dans le débat public, gagne à être reformulée en termes plus opérationnels de dépendance et de gestion du risque. Dans des écosystèmes technologiques complexes et globalisés comme le cloud, la recherche d'une indépendance totale apparaît hors d'atteinte. L'enjeu réel consiste plutôt à **optimiser un ratio entre le coût et le niveau de dépendance**, dans une logique de réduction des risques (« de-risking »). Cette approche marque une inflexion nette par rapport à une période où l'ouverture des marchés et la recherche d'efficacité économique primaient dans un contexte géopolitique plus stable.

Elle conduit à distinguer les dépendances acceptables de celles qui sont critiques, susceptibles d'affecter la continuité des activités, l'intégrité des données ou l'autonomie de décision, et à y répondre par des arbitrages concrets : internalisation de certaines briques ou processus stratégiques, diversification des fournisseurs, redondance et multi-sourcing. Dans le cloud, cela se traduit notamment par des approches

[9] DeepSeek est un laboratoire chinois d'intelligence artificielle fondé en 2023, spécialisé dans le développement de grands modèles de langage (LLM) et d'architectures d'IA optimisées pour l'efficacité énergétique.
[10] Mistral AI est un laboratoire français d'intelligence artificielle fondé en 2023, spécialisé dans le développement de grands modèles de langage (LLM) performants, ouverts et éco-responsables.

multi-cloud, le recours à des standards ouverts favorisant la réversibilité ou la capacité de ré-internalisation de certains services critiques.

Cette logique s'inscrit dans un mouvement plus large de sécurisation des dépendances à l'échelle des politiques publiques. Les travaux sur les minerais et matériaux critiques illustrent cette approche : il ne s'agit pas de sortir des chaînes de valeur mondiales mais de limiter les vulnérabilités en identifiant les points de fragilité, en diversifiant les sources et, lorsque pertinent, en reconstituant des capacités nationales ou européennes.

Dans le même esprit, les travaux de la Commission d'enquête parlementaire sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France (« Commission Latombe ») fait apparaître la nécessité de dépasser une vision purement juridique de la souveraineté pour adopter une analyse systémique des dépendances, qui intègre les dimensions techniques, industrielles et opérationnelles (cf. notamment audition de Dominique Luzeaux). Elle conduit à une approche de cartographie des risques, de hiérarchisation des priorités et de plans d'action ciblés articulant régulation, politique industrielle et organisation des chaînes d'approvisionnement.

Dans cette perspective, le cloud s'inscrit dans une problématique plus large de gestion des dépendances stratégiques, appelant des réponses graduées, pragmatiques et coordonnées à l'échelle européenne.

Le terme souveraineté est parfois galvaudé. Dans son acception politique classique, il renvoie à un principe d'autorité suprême d'un État ou d'un prince, historiquement associé à des prérogatives quasi exclusives sur un territoire et ses résidents. Cette conception est largement mise en cause à l'ère d'Internet et des infrastructures numériques distribuées.

L'expression « cloud souverain » apparaît dès lors comme un oxymore, le cloud impliquant par nature un transfert de données vers des capacités de stockage administrées par des tiers. Le cloud privé désigne simplement un usage exclusif de ressources, tandis que le cloud *on premises* reste marginal.

La notion de contrôle exclusif par un seul acteur est en outre difficilement soutenable au regard de la complexité des architectures cloud, reposant sur des écosystèmes d'acteurs multiples, et de la réalité des cyberattaques, y compris à des fins de cyberespionnage, qui touchent même les principaux opérateurs.

Un consensus minimal existe néanmoins dans une approche européenne : un « cloud souverain » désigne une infrastructure où **les données sont hébergées et gérées sur le territoire d'un État membre de l'Union européenne, sous juridiction locale appliquant le droit européen**, afin de limiter les risques d'ingérence extérieure. Il convient toutefois de ne pas en faire un concept de repli : **l'enjeu relève davantage d'autonomie et d'indépendance stratégique** que de souveraineté au sens strict.

b/ Qu'attendre en pratique des fournisseurs de Cloud ? («construire la confiance»)

Il faut pouvoir s'appuyer sur des éléments de confiance en pratique, qui s'articule au niveau de la relation et du terrain ; sur ce dernier, par un ensemble d'exigences doublé des preuves de leur respect.

On peut distinguer quatre types d'exigences fondamentales.

i/ **La première concerne la relation contractuelle**. Compte tenu de la taille respective des GAFAM et des entreprises clients, c'est déjà un résultat notable d'aboutir à

- une négociation équilibrée ;
- un prix raisonnable et prévisible ;
- l'auditabilité de l'offre ;
- la possibilité de rompre la relation contractuelle sans avoir à subir des pertes financières ou des tâches d'une envergure disproportionnée (voire des pertes sèches d'actifs informationnels).

ii/ **La seconde concerne la cybersécurité** sur laquelle l'offre du fournisseur doit être crédible face à la menace des cyberattaques de sophistication croissante, de plus en plus souvent diligentées ou mandatées par des officines étrangères dotées de ressources financières et de compétences très importantes.

Cette crédibilité s'appuie sur des éléments d'assurance de sa capacité à protéger efficacement les données de son client, celles régies par des enjeux de métier (par exemple processus, procédés vitaux de l'entreprise) comme celles sensibles car régies par un droit spécifique : données individuelles (RGPD), de santé (HDS), sujettes à d'autres réglementations spécifiques (DORA dans la sphère banque et finances, NIS2, etc.). Une vigilance s'impose sur les modalités fluctuantes de l'accord-cadre entre l'Europe et les Etats-Unis relatif aux données individuelles : devenue caduque, la convention *Safe Harbour* a été remplacée par la convention *Data Privacy Shield*, à son tour invalidée puis remplacée par le Data Privacy Framework. Pour les données non régies par un droit spécifique, des vides juridiques existent. Cela concerne notamment le secret des affaires et les données critiques opérationnelles ou stratégiques, dont il faut éviter le partage non maîtrisé, la perte d'intégrité (corruption) et la perte pure et simple.

iii/ La troisième, la capacité à se conformer à des exigences environnementales solides est un troisième élément qui pose des problématiques, liées notamment à des approches obsolètes et à l'opacité de la plupart des acteurs[11].

Iv/ La quatrième, l'exigence de réversibilité ou la capacité à récupérer ses actifs (données, applications, matériels) dans le but de changer de fournisseur ou de ré-internaliser tout ou partie de son Système d'Information et ce, sans coût prohibitif. Les solutions open source jouent un rôle crucial dans cette démarche, car elles garantissent l'interopérabilité (par exemple, via Kubernetes ou OpenStack) pour éviter le vendor lock-in, et proposent des formats ouverts qui facilitent les migrations.

Le CIGREF a publié deux documents consignant ces aspects en détail : « Trusted cloud reference document » (10.2023) et « CCTP : Achat de services de cloud public PAAS dans un environnement de confiance » (03.2024).

c/ Se prémunir d'ingérences étrangères ?

Rien ne permet de se prémunir contre l'interruption d'un service commercial à la demande du pays d'accueil du fournisseur. En outre, il est facile pour un fournisseur de service Cloud d'exercer une pression sur un client, en menaçant de couper le service, par exemple au moment de la renégociation de clauses – d'autant plus s'il est en position dominante.

Nous avons déjà évoqué les problématiques de données personnelles, dont la résolution très imparfaite donne lieu à des débats nourris, notamment en santé.

Une autre vulnérabilité tient à l'application de certaines lois à l'extérieur des frontières des pays des fournisseurs (extraterritorialité). Certaines lois de sécurité ou de renseignement peuvent obliger des fournisseurs étrangers à scruter ou recueillir, parfois en masse, des données de leurs clients français. ***Le cloud est en première place de ce risque qui renvoie à la réalité crue de possibles opérations d'espionnage[12].***

Aux Etats-Unis, deux réglementations sont en jeu :

- section 702 du Foreign Intelligence Surveillance Act (FISA) : elle autorise les agences américaines de renseignement à collecter des informations sans mandat. Le Congrès américain l'a prolongé de 2 ans en avril 2024.
- décret « Enhancing Safeguards for United States Signals Intelligence Activities », signé par le président Biden en octobre 2023. Il établit un principe de proportionnalité de la surveillance des données, certes, mais contestable.

Les acteurs chinois comme Alibaba (peu présents en Europe) sont tenus à respecter l'article 7 de la loi de collecte d'information du 27 juin 2017 rénovée le 27 avril 2018 : comme toutes les autres organisations et

[11] Recours notamment à des schémas de compensation s empruntant des circuits complexes ou difficiles à tracer sur le long terme.

[12] A ce titre : Guide du MEDEF et de l'AFEP, rédigé avec le Service de l'information stratégique et de la sécurité économiques (Sisse), créé en 2016 pour assurer la protection des actifs stratégiques de l'économie française face aux menaces étrangères.

les citoyens chinois ils doivent soutenir, assister et coopérer avec les autorités d'intelligence nationales « dans le respect de la loi », une expression souvent à géométrie variable en Chine.

Ces réglementations permettent de couvrir en principe des opérations d'espionnables sous couvert de la *discovery procedure* aux Etats-Unis.

La nouvelle doctrine américaine sous Trump (2025-2026) accentue encore ces risques. Son administration a renforcé les mesures protectionnistes et les contrôles sur les données hébergées par des acteurs étrangers, notamment via :

- L'extension des pouvoirs du Committee on Foreign Investment in the United States (CFIUS), qui peut désormais bloquer des transactions ou des services cloud jugés sensibles, même pour des entreprises européennes.
- Des restrictions accrues sur les transferts de données vers des pays considérés comme « à risque » (Chine, Russie, etc.), avec des sanctions possibles pour les fournisseurs qui ne s'y conformeraient pas.
- Une interprétation plus agressive de l'extraterritorialité, où les autorités américaines peuvent exiger l'accès à des données stockées hors des États-Unis, sous peine de représailles commerciales (ex. : amendes, exclusion des marchés).

En l'absence d'un acteur de confiance national, une remédiation consiste à ne retenir que les fournisseurs de Cloud (ou solution de confiance) à capitaux majoritairement français – en pratique à obliger des leaders du Cloud à créer une filiale à capitaux majoritairement français (ou du moins européens).

Encore faut-il préciser ce que l'on entend par des données sensibles. Cf. la Directive interministérielle de juin 2023 concernant les solutions hébergées par le Cloud pour les ministères, qui propose une très longue liste[13] qu'il sera nécessaire de préciser pour chaque système ou usage.

d/ Comment attester qu'un prestataire répond à ces attentes ?

L'ANSSI a instauré la qualification SecNumCloud (https://cyber.gouv.fr/secnumcloud-pour-les-fournisseurs-de-services-cloud), dont le niveau High + porte l'exigence capitalistique évoquée plus haut. Ce cadre permet à des acteurs français de proposer des offres enrichies de compétences et capacités au niveau voulu et « sûres »[14], moyennant un surcoût lié à la mise en place de l'organisation, du volet technologique[15] et à la certification de l'offre. On notera que GAIA-X intègre également cette condition dans son label de niveau 3, le plus élevé[16].

A noter que SecNumCloud est avant tout un dispositif de cybersécurité, et non un instrument de politique industrielle. SecNumCloud repose sur un processus d'évaluation technique rigoureux et standardisé, visant à garantir un haut niveau de sécurité pour des usages sensibles du cloud. Le référentiel impose notamment des exigences fortes pour protéger les données contre les cyberattaques, les accès internes abusifs et certains risques juridiques, dont l'extraterritorialité du droit. Il garantit ainsi que seul un prestataire européen contrôle les données, même lorsque des technologies non européennes sont utilisées. En

---

[13] « *Ces données d'une sensibilité particulière recouvrent :Les données qui relèvent de secrets protégés par la loi, notamment au titre des articles L.311-5 et L.311-6 du code des relations entre le public et l'administration (par exemple, les secrets liés aux délibérations du Gouvernement et des autorités relevant du pouvoir exécutif, à la défense nationale, à conduite de la politique extérieure de la France, à la sûreté de l'Etat, aux procédures engagées devant les juridictions ou encore le secret de la vie privée, le secret médical, le secret des affaires qui comprend le secret des procédés, des informations économiques et financières et des stratégies commerciales ou industrielles); Les données nécessaires à l'accomplissement des missions essentielles de l'État, notamment la sauvegarde de la sécurité nationale, le maintien de l'ordre public et la protection de la santé et de la vie des personnes.* »

[14] (S3NS https://www.s3ns.io/ Thales 90% des parts sociales, Google Cloud 10% ; BleuCloud https://www.bleucloud.fr/ Orange, CapGemini et Azure, etc.)

[15] « vaccinées » par rapport à la menace juridique évoquée plus haut, sous réserve de traiter le volet technique.

[16] https://gaia-x.eu/wp-content/uploads/files/2021-11/Gaia-X%20Labelling%20Framework_0.pdf https://docs.gaia-x.eu/policy-rules-committee/compliance-document/24.11/criteria_cloud_services/#P5.1.5 voir notamment critères P. 5.1.5. et P.5.1.6.

revanche, SecNumCloud ne vise pas à supprimer toutes les dépendances technologiques ni à organiser la souveraineté industrielle, qui relèvent d'autres politiques publiques.

A titre d'exemple, Thales dispose d'une structure pour identifier les failles informatiques des produits duaux, des méthodes et des capacités pour fiabiliser les composants sourcés. Dans le cadre de S3NS, les rôles sont répartis de la manière suivante : Google propose les mises à jour des services et les innovations (solution Google Cloud), tandis que Thales les fiabilise :

- composants physiques : retrait des drivers pour accéder au code natif ou même directement à la puce (« composant nu »), puis ajout d'une pile logique de confiance.
- logiciels : remplacement des APIs, installation de middleware fiabilisé et de briques de sécurité (crypto) certifiées ANSSI. Les « backdoors » restent parmi les risques résiduels que même le recours à du logiciel libre ne peut complètement éliminer.
- tout le personnel qui intervient est dûment habilité.

L'Europe pour sa part propose le schéma de certification de cloud de confiance, l'EUCS (EU Cloud Services Scheme, (https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme), mais son instauration au plan réglementaire invalidera le dispositif SecNumCloud, ce qui aura un impact certain puisque la Commission Européenne rechigne à adopter la clause capitalistique sous la pression politique américaine et celle des lobbies industriels[17].

Est-il concevable que l'Europe reste dans cette posture compte-tenu de la situation géopolitique actuelle ?

Tout d'abord, il n'est plus très crédible d'invoquer l'idée que les leaders étrangers à l'Europe seraient immunisés contre une attaque cyber majeure (Cf. violations massives chez Oracle18), dont nous savons qu'une part importante concerne des opérations d'ingérence et de vol de propriété intellectuelle.

Le contexte du Cloud présente une analogie intéressante avec celui d'une habitation en co-propriété. On peut en effet rappeler que la souscription d'une assurance multi-risques habitation n'est pas légalement obligatoire en France. Pour un propriétaire logeant dans sa maison, isolée de tout et qui n'y inviterait personne, l'intérêt peut en être discuté. Mais dans une co-propriété, ne pas en souscrire semble déraisonnnable puisque, par exemple, un incendie démarrant chez soi peut faire des victimes chez ses voisins. Et plusieurs situations l'imposent, comme signer un contrat de location, acheter une habitation, si le règlement de copropriété l'impose, par une société de syndic dans le cadre de ses mandats.

De même, le fournisseur d'un Cloud doit veiller à ce qu'une tierce partie, cliente ou non, n'empiète pas sur les droits et la sphère informationnelle d'aucun autre. S'il n'en est pas capable, alors la puissance publique doit pouvoir suppléer à son impuissance. C'est précisément ce à quoi vise un dispositif de certification réglementaire.

Ainsi, l'Europe doit prendre la mesure de ses responsabilités, tant au plan moral que pratique en adoptant un dispositif de certification réglementaire suffisamment solide. La situation actuelle pose de manière plus nette la nécessité d'un rééquilibrage entre les enjeux de sécurité européens et ceux du libre-échange invoqué par les Etats-Unis et les leaders du Cloud. Vu le peu de cas fait par l'administration Trump des accords de libre-échange, la prise de politique, qui pouvait sembler incommensurable, apparaît désormais mineure.

---

[17] https://www.cio-online.com/actualites/lire-eucs-la-certification-cloud-europeenne-qui-menace-de-desarmer-secnumcloud-15856.html : (12.09.2024) « ***Tout en soulignant l'incertitude juridique qui entoure encore le dossier, la CSNP, composée de sept députés, sept sénateurs et trois personnalités nommées par le ministre de l'Économie, estime que « l'adoption de l'EUCS, qu'il intègre ou non le niveau High+, rendrait caduque le référentiel SecNumCloud », la norme européenne étant appelée à se substituer aux référentiels nationaux, dont SecNumCloud en France. Sans oublier des difficultés d'application des articles relatifs à la protection des données stratégiques et sensibles sur le cloud que renferme la loi SREN. Sous la pression des lobbys de l'industrie de la tech américaine, le secrétaire d'Etat Anthony Blinken a envoyé, en septembre 2023, une note à Ursula von der Layen, la présidente de la Commission de Bruxelles, avertissant que l'inclusion de ces dispositions « pourrait nuire aux relations bilatérales économiques et sécuritaires » entre les deux blocs. »***

[18] https://oracle.developpez.com/actu/370688/Oracle-poursuivi-en-justice-suite-a-deux-violations-massives-de-donnees-sur-le-cloud-accusee-de-negligence-notamment-a-cause-de-l-absence-d-un-chiffrement-adequat-l-entreprise-ne-les-aurait-pas-signale/

De fait, l'EUCS a bien failli être adopté sans la clause relative au contrôle de capital, mais ce dossier a été réouvert suite aux dernières évolutions politiques aux US, ce qui a donné naissance à l'initiative Cloud and AI Development Act (CADA) visant à renforcer les capacités de cloud et de calcul nécessaires au développement de l'IA en Europe, notamment en facilitant l'implantation de data centers et l'investissement dans les infrastructures numériques. CADA relève principalement d'une logique de politique industrielle et de développement d'infrastructures tandis que les versions récentes du schéma EUCS en font un instrument exclusivement centré sur les exigences de cybersécurité applicables aux services cloud et ne comportant donc plus de clause de contrôle du capital ou de souveraineté.

CADA vient ainsi compléter l'EUCS : alors que l'EUCS définit un cadre de confiance et de cybersécurité pour les services cloud, CADA vise à développer les capacités industrielles et les infrastructures cloud nécessaires en Europe, en particulier pour soutenir l'essor de l'IA dans une logique de « souveraineté ». CADA vise à rendre possible, dans l'Union, des offres « EU-based » pour des usages publics hautement critiques : ce n'est plus une étiquette, c'est une stratégie d'infrastructure.

e/ Quelles approches privilégier dans la situation actuelle ?

i/ Nos responsables politiques doivent empêcher l'Union Européenne de continuer à se soumette au bon vouloir des lobbies des USA sur le projet EUCS. En ce sens, l'initiative CADA qui complète l'EUCS est bienvenue.

ii/ **Il convient de considérer le cloud, et en particulier ses couches basses (socle matériel et services de compute et réseaux IaaS) plus que jamais comme aussi stratégique que les réseaux électriques ou les télécoms** :

- **Le cloud n'est pas un marché réellement concurrentiel : il est captif.** Les coûts de sortie ne sont pas principalement financiers : ils sont organisationnels, opérationnels, cognitifs (re-platforming, dépendances à des services managés, outillage, gestion des identités, observabilité, data pipelines, etc.). Cette captivité réduit l'intensité concurrentielle effective, même si la concurrence existe théoriquement. Dit autrement : on n'est plus dans un marché "contestable" au sens classique.
- **Le risque systémique est devenu difficilement assurable.** Une défaillance majeure (technique, cyber, juridique, géopolitique) peut affecter simultanément des milliers d'acteurs. Le risque est corrélé et donc peu diversifiable, ce qui met en tension les mécanismes de couverture privés. Cela rapproche le cloud d'autres secteurs où l'on a dû inventer des cadres publics (ou quasi-publics) pour traiter des risques systémiques.
- **La liberté contractuelle s'érode sous l'asymétrie de pouvoir.** La négociation est souvent limitée, la réversibilité coûteuse, l'auditabilité imparfaite, et la menace de coupure (ou de durcissement unilatéral) est crédible du fait de la dépendance. Là encore, sans jugement moral : l'asymétrie est structurelle. Or, lorsqu'une relation contractuelle devient structurellement déséquilibrée, on bascule fréquemment vers des logiques de concession, obligation de service, régulation des conditions d'accès et de sortie.
- **Le cloud est devenu une condition d'accès à la concurrence.** C'est peut-être le point le plus important : pour une PME, une startup, une ETI, l'accès à une infrastructure cloud stable et neutre conditionne la capacité même à entrer sur certains marchés (scalabilité, sécurité, conformité, time-to-market). Dès lors, l'infrastructure n'est plus un simple service : elle devient un "ticket d'entrée" à la compétition économique. Quand l'infrastructure conditionne la concurrence, la question de sa neutralité devient centrale.
- **L'intervention publique n'a pas besoin d'être totale : elle peut être minimale, ciblée, "en couches". On peut imaginer une approche où seule la couche socle (certaines briques fondamentales : interconnexion, identité, chiffrement, services de base, exigences de réversibilité, transparence environnementale, etc.) fait l'objet d'un régime plus contraignant, sans chercher à "nationaliser**

le cloud" ni à empêcher l'innovation sur les couches hautes. Cette logique par couches ressemble beaucoup à ce qui a été fait ailleurs : concurrence sur les services, neutralisation/régulation du réseau.

L'Union Européenne dispose déjà d'un certain nombre d'outils pour avancer dans cette direction : le Digital Markets Act (DMA) pour imposer l'interopérabilité et sanctionner les pratiques anticoncurrentielles, le fonds pour la souveraineté numérique (10 milliards d'euros) pour financer des alternatives européennes, et le règlement sur la résilience des infrastructures critiques (CER) pour encadrer les data centers stratégiques. Une approche ciblée sur les secteurs vitaux (santé, énergie, défense) permettrait d'imposer des obligations d'hébergement local, des audits de souveraineté et une diversification des fournisseurs, tout en s'inspirant des modèles éprouvés de service public (tarifs régulés, préférence européenne dans les marchés publics). Les solutions open source (Kubernetes, OpenStack) et les normes communes (comme celles promues par Gaia-X) sont essentielles pour briser le *vendor lock-in* et assurer la réversibilité des données. Enfin, une volonté politique forte, combinant subventions, sanctions et coordination entre États membres, est indispensable pour transformer le cloud en une infrastructure publique résiliente, à l'image de ce qui a été fait pour l'électricité (ex : ENTSO-E) ou les télécommunications.

iii/ Au niveau pratique et technique, bien plus que l'infrastructure, **l'écueil porte sur l'absence d'un écosystème national ou européen intégré d'acteurs du logiciel, capable de fournir et maintenir un ensemble de composants logiciels permettant de déployer une offre crédible**.

En effet, si Google venait à se retirer par exemple de S3NS (ou Microsoft de BLEU), cette offre disparaîtrait. La domination des acteurs nord-américains repose sur le fait de disposer d'une **pile (« stack ») logicielle complète, propriétaire, robuste, allant du stockage sécurisé aux outils collaboratifs en passant par l'IA, et compétitive.**

Plutôt qu'ériger des murailles réglementaires qui, soit avantageront les GAFAM, parce qu'il leur sera facile d'y satisfaire, soit les détournera du marché européen (ou pire, comme le propose le RN, des taxes du type à la bande passante), il faut donc **accompagner la progression des acteurs nationaux et européens dans leurs efforts pour créer l'écosystème souhaitable**.

Ces acteurs en France sont nombreux :
- l'ANSSI, qui propose des briques logicielles de confiance[19], des spinoffs de la défense ;
- les capacités en recherche théorique et appliquée avec des acteurs puissants comme l'INRIA et le CEA et leurs nombreuses spinoffs. A titre d'exemple, l'INRIA a été l'un des principaux instigateurs de Scilab, un logiciel de calcul reconnu mondialement.
- des entreprises comme OVHcloud, Scaleway, Outscale, NumSpot[20], Clever Cloud, Scalingo, Ionos, Leaseweb, Aruba, Oodrive, etc. qui avancent dans la certification SecNumCloud de leurs offres cloud
- des acteurs de la cybersécurité comme Thales (qui a racheté Gemalto), Atos, CapGemini, et ceux apparus depuis 2010 (Wallix, Tehtris, HarfangLab, Sekoia, PrimX, Sentryo, Prove & Run, Quarkslab, etc.)
- en IA Mistral AI, des acteurs de l'Edge computing et edge AI comme Axelera, etc.
- toute une panoplie d'utilisateurs (notamment licornes) dans des domaines comme les fintech, la santé, le marketing, le e-commerce, etc.

iii/ Dans le cadre des services administratifs, la DINUM a fédéré des objectifs communs à tous les ministères, y compris celui des Armées, des méthodes et un recours à un ensemble de briques logicielles libres. Elle a passé sur ce dernier volet un accord avec son homologue en Allemagne pour promouvoir

[19] https://github.com/orgs/ANSSI-FR/repositories?type=all – par exemple https://github.com/ANSSI-FR/eurydice
[20] monté par La Poste, Dassault Systèmes, Bouygues Télécom et la Banque des Territoires

la **création de communs numériques**. Enfin elle instaure une approche de mutualisation puissante de l'identité numérique par le biais de monidénum, dont une version pro vient de sortir. **Cette approche par la fédération de ressources et de pratique, la création de « communs », étendue à d'autres états-membres, est un excellent début**, même si elle ne peut être développée qu'au cas par cas, du moins dans un premier temps. Par exemple les pays nordiques ont adopté un identifiant unique, de sorte que l'approche monidenum n'y est pas pertinente.

Par rapport au début des années 2000, les personnes en charge des projets et des structures porteuses sont bien mieux gréées en termes de RH, compétences et moyens, et mieux préparées à mutualiser les approches et partager les bonnes pratiques.

iv/ En complément aux référentiels spécifiques au Cloud, il sera utile de généraliser cette approche concernant les applications spécifiques et le middleware par exemple de sécurisation – ou sur ce domaine exiger des composants répondant à des exigences attestées par exemple selon un schéma ISO 15408, de préférence sous maîtrise de l'ANSSI ou l'ENISA.

v/ Sur un plan général les leviers de confiance, alliée à des formes d'autonomie conférées par la création de communs, sont

- des labels et des standards conformes aux réglementations européennes et à nos valeurs (éthique de l'IA – la dimension environnementale étant appelée à devenir un levier de plus en plus fort) – selon un effort à moduler finement.
- des approches fédératives et mutualisant des ressources logicielles libres ou open source.
- Des pratiques adaptées d'achats publics (cf. paragraphe spécifique à ce sujet, qui s'applique au numérique).
- Le suivi à bon rythme des progrès technologiques (exemples kubernetes, qbo.io va balayer vmware ce qui va simplifier la stack).

Quelques éléments de perspective en conclusion

Nous nous sommes limités ici à un objectif consistant essentiellement à assurer une relation contractuelle équilibrée avec les fournisseurs extra-européens et à réduire à un niveau raisonnable la vulnérabilité, notamment à des manœuvres essentiellement de nature politique pour compromettre les données confiées par les entreprises françaises et européennes (en l'occurrence via des artifices de nature juridique).

Dans le contexte présent, où la précieuse césure entre pouvoirs politique et juridique se désagrège Outre-Atlantique, où les mutations géostratégiques s'accélèrent et où la Chine et les USA sont dans une course éperdue aux investissements en IA, le niveau considéré comme raisonnable doit être réévalué, le cas échéant, en temps utile ou périodiquement.

Ce contexte contribue aussi à réduire le coût politique d'un renforcement au niveau souhaité par la France des labels européens en cours de finalisation. Il est donc essentiel qu'une impulsion politique soit donnée pour que cela ait lieu en profitant de la fenêtre d'opportunité qui se présente.

Le chemin vers un niveau d'autonomie sensiblement plus fort sera très long, si l'on en prolonge le tableau jusqu'au composant clé de la capacité de calcul, le processeur ou la carte graphique.

Mais dans plusieurs domaines, la France a réussi à surmonter progressivement son retard technologique ou industriel et une bonne part de ses vulnérabilités, par rapport au scénario extrême d'un refus de fourniture par un acteur étranger.

Dans le nucléaire civil, l'impulsion de l'Etat a été cruciale, en s'appuyant sur des compétences étrangères (Westinghouse). Dans celui de la signature électronique, cela fut principalement grâce à l'initiative privée :

création de Certplus (JV Gemplus, France Telecom et VeriSign, le leader international de ce domaine), puis intégration à Keynectis en 2004, sous la houlette de Thierry Dassault[21] avec l'encouragement de l'Etat. ***Ces deux exemples illustrent le rôle crucial de la confiance entre le secteur privé et les instances publiques, voire le pouvoir politique*** (cas du nucléaire civil – un tel scénario de constitution de capacité en bloc paraissant impossible à renouveler dans le contexte économique actuel).

L'essor de l'industrie aérospatiale soviétique jusqu'à la chute du Mur de Berlin (quasiment sans ordinateurs) montre qu'une forte détermination politique peut faire des miracles. La Chine est bien parvenue à se passer des ingénieurs de l'Union Soviétique, et dans divers domaines, à rattraper l'Occident (parfois tardivement - carte à puce, avion C919, etc. et pas toujours : finesse de gravure de composants).

Donc (même si l'on peut regretter l'absence d'un « Airbus du numérique ») l'Europe et la France n'ont pas à rougir des échecs répétés de recréer un « GAFAM européen » mais il s'agit maintenant d'***acter que c'était un projet irréaliste et de convenir que les deux « questions de fond » concernent plutôt la manière de :***

- ***Formuler des objectifs et proposer des approches de rattrapage réalistes,***
- ***anticiper (prévenir, ralentir et préparer) le rattrapage industriel par la Chine.***

En effet, chaque fois que l'Asie rattrape l'Occident, cela fragilise nos industries. Quand c'est le fait de la Chine, cela peut mettre nos industries en péril de mort[22]. Le tableau ci-dessous présente quelques exemples (des exceptions existent, comme Nexans, rescapé de GEC-Alsthom).

Technologie	**Période (décennie)**	**Brevets d'origine**	**processus de transfert / clés du leadership chinois (ou exemples)**	**Conséquence**
Ecrans plats / cristaux liquides	Fin années 90	CEA	Thomson vend sa dernière usine de téléviseurs à Singapour. Transferts technologiques à la RPC, via Taïwan.	Disparition (toute l'Europe)
Batteries au lithium	Années 2000	SAFT / HEF	JV en Chine	
Cellules photovoltaïques	2010		Energie électrique fournie à prix dérisoire.	
Véhicule électrique	2015	BYD	Commande de 50000 bus électriques par la province de Guangdong à BYD, quand Heuliez s'en voit commander 30.	Fragilisation importante
Big Data / Cloud	> 2015	Monde entier	Vallée du Cloud (Guizhou). Energie quasi gratuite, climat tempéré et cavernes fraîches	Fragilisation (production et R&D)
Recherche médicale	2010	Monde entier	(2014 SANOFI ouvre un premier centre de R&D à Shanghaï). La France souffre de l'éloignement des outils de production de médicaments et de réactifs.	Poursuite du processus de fragilisation
omique	2010	BGI (1999 / 2007) iCarbonX (2015)	2010 : BGI achète 128 machines Illumina (1,5 M$ garantis par China Develoment Bank).	Autonomisation de la R&D chinoise dans le secteur médical

L'IA bouleversera à terme quasiment tous les secteurs de l'économie. L'ingénierie et la fabrication (robots – dont la Chine est le premier utilisateur au monde) seront parmi les plus impactés, ce qui met en jeu notre compétitivité et la pérennité de nos industries à horizon 2035 ou avant. Le Cloud n'apparaît ainsi que comme un volet préalable d'une immense confrontation technologique. Il est temps de tirer le constat de nos échecs dans ce domaine et de rassembler une volonté déterminée sur des démarches ambitieuses et réalistes,

[21] Keynectis a intégré en 2015 DocuSign, basé en Californie ; mais entre-temps une offre nationale et européenne avait émergé

[22] Cela tient au fait qu'en plus de la taille de son économie, celle-ci fonctionne au gré d'incitations gouvernementales massives et de bulles financières.

comme celles proposées ci-dessus et en misant sur l'IA de manière pragmatique, sans trop focaliser sur les LLM propriétaires actuels : Cf. Deepseek[23] ou article ci-dessous.

Dans cette perspective, il est rassurant de pouvoir constater le dynamisme des ingénieurs et chercheurs nationaux dans les systèmes d'IA (Hugging Face, rachetée par un acteur US ; Yann Le Cun, directeur scientifique de l'IA chez META, à présent citoyen américain et revenu en France ; Mistral AI et en défense Helsing) et européens (en Allemagne Aleph Alpha et par extension Deepl). Est-ce satisfaisant ? Assurément non si les meilleurs partent outre-Atlantique, notamment chez des leaders qui reposent sur leurs acquis, leur puissance financière et leurs alliés politique.

Pour en revenir au volet important des composants électroniques utilisés dans le Cloud et pour l'IA, il renvoie notamment aux enjeux d'indépendance dans le domaine du calcul à haute performance, auquel on peut rattacher dans une perspective peut-être plus lointaine le volet des ordinateurs quantiques.

Il est clair que l'économie européenne souffre d'une relation déséquilibrée par rapport à ses partenaires commerciaux US, taïwanais, coréens et chinois. Elle dispose toutefois d'un quasi-monopole sur les technologies de photolithogravure de composants. En effet, l'acteur hollandais ASML (à l'origine une JV avec Philips) est le seul capable de produire des machines recourant à l'extrême ultraviolet (EUV) nécessaires pour graver les composants les plus puissants[24]. Son chiffre d'affaires est passé de 13 M$ à 30 M$ entre 2018 et 2023[25]. Le président Trump a tenté en 2018 de bloquer la vente de machines ASML à la Chine continentale, sans réel succès. Mais plus récemment, suite notamment à une affaire d'espionnage par un ancien employé chinois d'ASML, le gouvernement hollandais s'est aligné sur les attentes américaines et exerce désormais directement le contrôle des licences d'exportation.

En outre, il existe encore quelques pôles industriels conséquents en Europe : celui de Dresde, qui a attiré Global Foundries (US) et le leader taïwanais TSMC[26] ; celui de Münich (Infineon, spinoff de Siemens) ; et celui autour de Grenoble (ST Micro), dont l'attractivité pourrait ne pas être aussi forte, à la lumière des incertitudes sur la mégafab conjointe STMi-Global Foundries[27]. Par ailleurs, STMicro reste focalisé sur des marchés de niche (notamment transport). Mais de manière générale, l'Europe investit très peu, bien trop peu, sur l'innovation dans l'industrie des composants électroniques. Examinons le secteur des composants clé du calcul à haute performance, indispensables pour mener des recherches à la pointe en IA et dans plusieurs secteurs industriels. Après la triade NVidia, AMD et Intel, se profilent AWS, Alphabet, Alibaba, IBM, Huawei, etc. L'europe reste quasiment inexistante. Il fallait examiner, il y a peu, des domaines connexes comme la vision artificielle, pour trouver des acteurs tels que la fabless hollandaise Axelera AI, fondée en 2021, qui commercialise la puce Metis[28] (68 m$ de capital levé en 2024, 62 m$ en 2025, 140 employés, « des dizaines de clients »[29]). Kalray, une startup filiale du CEA, ambitionne de produire une puce sécurisée pour des plateformes autonomes.

L'Europe a lancé l'initiative European Processor Initiative (EPI)[30], en phase 2 avec notamment Axelera AI et SiPearl[31], une startup en grande partie française qui a bouclé un tour de table de 90 m€[32] en avril 2023 pour

---

[23] Un très bon interview de son fondateur Liang Wenfeng https://www.chinatalk.media/p/deepseek-ceo-interview-with-chinas : *What we lack in innovation is definitely not capital, but a lack of confidence and knowledge of how to organize high-density talent for effective innovation.*

[24] La puissance de calcul d'une puce se traduisant en effet en nombre de circuits élémentaires qu'elle contient, autrement dit en densité surfacique ou volumique, étroitement liée à la finesse du trait de gravure.

[25] Source : wikipedia

[26] https://www.courrierinternational.com/article/allemagne-tsmc-inaugure-sa-premiere-usine-de-puces-en-europe-un-somptueux-cadeau-de-l-ue_221364

[27] https://www.usinenouvelle.com/article/en-isere-globalfoundries-est-il-en-train-de-lacher-stmicroelectronics-pour-sa-megafab-a-crolles.N2210430

[28] https://axelera.ai/ai-accelerators/metis-m2-ai-acceleration-card

[29] https://www.ecinews.fr/fr/axelera-lance-metis-une-carte-edge-pour-lia-en-memoire/

[30] https://cordis.europa.eu/article/id/442363-building-europe-s-high-performance-computing-capabilities/fr

[31] https://sipearl.com/joint-projects-european-processor-initiative

[32] https://www.usinenouvelle.com/article/la-start-up-sipearl-leve-90-millions-d-euros-pour-accelerer-la-commercialisation-d-un-microprocesseur-europeen.N2119136

produire un chiplet pour l'IA. Ces deux projets ambitionnent d'apporter une indépendance technologique à l'Europe , avec pour SiPearl une promesse de performance énergétique très ambitieuse.

Depuis sa création en 2019, SiPearl a été forcée, peut-être faute d'une capitalisation suffisante, à relancer un cycle de développement qui l'a retardée de 2 ans. Etant parvenue semble-t-il à rattraper le rythme du marché, elle a lancé en été 2025 la production des premiers échantillons de sa puce de première génération, Rhéa 1. Les générations 2 et 3 suivront moyennant une levée de 200 m€ espérée en Série B. Il aura ainsi fallu une décennie pour qu'émerge enfin un acteur européen crédible du composant pour l'IA. Le développement d'Axelera AI a été plus rapide : fondée en 2021), elle vient de boucler une levée de 250 mUSD et aurait 500 clients[33].

L'initiative EPI est au cœur d'EuroHPC Joint Undertaking (J.U)[34] (soutien financier total de l'ordre de 500 m€[35]). L'Euro HPC J.U vient de lancer le projet successeur DARE[36], dont la phase 1, sur 3 ans, recevra un financement maximum de 240 m€. Les « tickets » européens de subventions publiques sont donc de l'ordre du demi-milliard d'euros sur 2 ou 3 ans.

Parallèlement, Aux Etats-Unis,

- Joe Biden et Donald Trump se sont clairement relayés dans l'industrie du composant : Chips & Science Act (août 2022) avec un potentiel de 280 MUSD à la clé, dont 52MUSD de subventions aux implantations sur le territoire américain (l'acteur taïwanais TSMC étant particulièrement visé) ; annonce en mars 2026 d'un prolongement à 100 M$ pour renforcer la présence de TSMC ;
- 500 MUSD investis dans l'IA aux Etats-Unis en 2025, dont 215 dans des startups et 60 dans la construction de datacenters.

Au niveau mondial les volumes prévisionnels d'achats en matériels et infrastructures sont considérables : Mc Kinsey (7 TUSD en infrastructures pour le numérique dans son ensemble) ; Gartner (1,5 MUSD en 2025), tandis que Bain & Co, plus pondéré en raison des incertitudes sur le succès des modèles d'affaires, augure une forte hausse des tarifs au fil de la structuration du marché.

En tout état de cause, l'émergence d'un écosystème industriel du cloud et du calcul en Europe souffrira de la faiblesse des investissements, parallèlement à une hémorragie financière accrue générée par ses dépendances, en plus des enjeux d'autonomie développés ci-dessus. Une politique d'investissement vers l'écosystème local du cloud apparaît indispensable – nous en avons abordé quelques aspects – .

Cette politique d'investissement devra être ciblé et étendue à l'IA, une thématique plus complexe en raison notamment de ses évolutions extrêmement rapides, de son ancrage cognitif puissant et au-delà, de tous les enjeux de pouvoir qu'elle porte. Elle pourra faire l'objet d'une autre fiche.

L'effet d'un investissement bien ciblé permettra de verrouiller la maîtrise de technologies clé à volume financier limité, et c'est probablement la seule approche réaliste dans la mesure une politique d'investissement à l'image de celles de la Chine et des Etats-Unis est inconcevable à l'heure actuelle.

Une condition de succès est que la main d'œuvre spécialisée dans les domaines considérés ne soit pas aspirée notamment vers ces deux pays.

Une politique d'achats publics liée notamment à des projets structurants (base de données confiance pour la médecine de précision – exemple le Health Data Hub – ; initiatives sur les communs numériques en lien avec l'histoire et la mémoire ; architectures de confiance pour les services critiques ; etc.) est indispensable. La présentation plus précise de quelques domaines concernés, parmi les multiples que l'on pourrait énumérer, pourrait faire l'objet d'une étude spécifique.

[33] https://www.afp.com/fr/infos/axelera-ai-obtient-plus-de-250-millions-de-dollars-pour-la-croissance-commerciale
[34] https://eurohpc-ju.europa.eu/3-new-ri-projects-boost-digital-sovereignty-europe-2022-02-03_en
[35] https://eurohpc-ju.europa.eu/system/files/2023-06/Decision%2010.2023.-%202nd%20Amendment%20WP%202023.pdf
https://www.europarl.europa.eu/cmsdata/269929/EuroHPC%20JU_RBFM%202022.pdf
[36] https://eurohpc-ju.europa.eu/advancing-european-sovereignty-hpc-risc-v-2025-03-06_en

En complément, l'orientation vers ces secteurs (ou des secteurs d'application), par exemple, d'une partie des fonds des assurances, pourrait jouer un rôle de facilitation. On pourrait envisager de l'associer à une réglementation pour promouvoir des actions d'adaptation face aux catastrophes naturelles climatiques dans le contexte du réchauffement, prenant appui sur des technologies à fort contenu numérique – sur un périmètre global, et non pas limité aux fermes de serveurs, ce qui lancerait une dynamique économique – . Il se trouve que l'impulsion donnée pendant des décennies par la Commission Européenne sur les thématiques d'adaptation face aux catastrophes naturelles, a fait naître un ensemble de capacités et de compétences qui constitue un terreau fertile.