# LA SOUVERAINETÉ DU CLOUD EUROPÉEN

Les capacités humaines, économiques, technologiques
et industrielles qui déterminent l'autonomie numérique de l'Europe



FRANCK MEVENGUE

# La souveraineté du cloud européen

*Les capacités humaines, économiques, technologiques et industrielles qui déterminent l'autonomie numérique de l'Europe*



Franck Mevengue

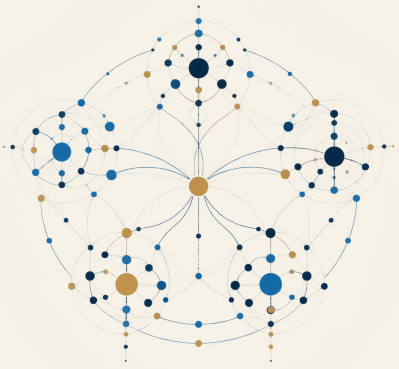
# Note au lecteur

Ce livre distingue ce que les sources permettent d'établir, ce qui demeure partiellement documenté, ce qui relève d'une hypothèse plausible, et ce qui reste ouvert. Les limites empiriques sont exposées dans le texte lorsqu'elles conditionnent le raisonnement. Elles ne sont pas dissimulées pour renforcer une conclusion.

LANGAGE GRAPHIQUE

## Le motif Nœuds

Traits pleins : relations documentées. Traits pointillés : hypothèses ou trajectoires. Ce motif ne porte aucune donnée empirique.



Motif signature Nœuds (illustration conceptuelle).

# Préface

L'Europe numérise ses administrations, ses industries et ses services publics à une vitesse qui laisse peu de place à l'illusion. Une part croissante du calcul, du stockage et des applications repose désormais sur des infrastructures opérées par un petit nombre d'acteurs mondiaux. Ce déplacement n'est pas un détail technique. Il redéfinit ce qu'une organisation peut encore maîtriser, substituer ou reconstruire lorsqu'un incident, un contrat ou une tension géopolitique vient rappeler la fragilité d'une dépendance.

Le cloud, souvent réduit à une question d'hébergement, est devenu une infrastructure économique et stratégique. Il concentre des enjeux de coût, de compétences, de réversibilité, d'industrie et d'institutions. Une approche exclusivement juridique, qui se contenterait de localiser des données ou de signer des clauses, laisse hors champ l'essentiel : qui sait vraiment opérer, sortir, industrialiser et contrôler. Une approche exclusivement commerciale, qui comparerait des catalogues de prix sans périmètre équivalent, confondrait avantage tarifaire et autonomie.

Ce livre propose un autre fil. Il traite la souveraineté du cloud européen comme un **degré de capacités interdépendantes** (humaines, économiques, technologiques, industrielles et institutionnelles) face à des dépendances jugées critiques. La thèse n'annonce pas une souveraineté déjà acquise. Elle invite à examiner, chapitre après chapitre, ce que les sources permettent d'établir, ce qui demeure plausible, et ce qui reste ouvert.

Le lecteur trouvera ici des distinctions plus que des slogans : adoption et souveraineté, localisation et contrôle, prix catalogue et coût total, obligation juridique et migration testée, financement et industrialisation. Ces distinctions ne ferment pas le débat. Elles le rendent possible.

La lecture demandée est critique. Là où les séries manquent, où une expérience n'a pas été menée, ou où une évaluation causale reste hors de portée, le texte le dit. La solidité d'un essai technologique se mesure aussi à ce qu'il refuse d'inventer.

# Mot de l’auteur

Ce livre est né d’une question simple dans sa formulation et exigeante dans ses conséquences : que reste-t-il de la maîtrise lorsque le numérique s’appuie sur des infrastructures partagées, souvent situées hors du périmètre direct de celui qui les utilise ?

J’ai choisi de traiter ensemble l’école et les laboratoires, les prix et le coût total, les standards et la réversibilité, l’industrie et la commande publique. Non pour tout confondre, mais parce que les dépendances cloud deviennent critiques précisément là où ces dimensions se croisent. Une formation sans accès réel aux environnements, un contrat sans sortie testée, un financement sans offre industrialisée : chaque maillon isolé peut donner l’illusion du progrès.

Le projet s’est construit avec un appareil de sources et d’affirmations, et avec la discipline de distinguer faits, estimations, interprétations et hypothèses. Certaines propositions restent volontairement au statut d’hypothèse de travail. Ce n’est pas une faiblesse cachée : c’est une règle de lecture.

Le lecteur peut utiliser cet ouvrage comme une carte de distinctions, comme une méthode pour lire un indicateur ou une annonce politique, ou comme un cadre pour poser des priorités de recherche. Il ne trouvera ni classement général des fournisseurs, ni validation scientifique globale décrétée par la seule composition du livre.

Je remercie par avance ceux qui liront avec exigence, corrigent une formulation, signalent une limite, ou refusent une conclusion trop large. Un essai sur la souveraineté cloud ne mérite d’exister que s’il reste réfutable.

# Table des matières

Note au lecteur . . . . . iii
Préface . . . . . iv
Mot de l'auteur . . . . . v
Introduction . . . . . 1

**I Le cloud, la souveraineté et les dépendances . . . . . 5**

1 Le cloud comme infrastructure économique et stratégique . . . . . 6
2 Que signifie réellement la souveraineté cloud ? . . . . . 13
3 Cartographier les dépendances critiques . . . . . 18

**II Capital humain et formation . . . . . 24**

4 Former dès l'école : culture numérique et informatique . . . . . 25
5 Universités, laboratoires et infrastructures pédagogiques . . . . . 30
6 Former, certifier et conserver les compétences opérationnelles . . . . . 34

**III Économie des choix cloud . . . . . 37**

7 Comparer stockage, calcul et réseau à périmètre équivalent . . . . . 38
8 Comprendre le coût total de possession . . . . . 45
9 Expérimenter, migrer et réduire les coûts de sortie . . . . . 51

**IV Technologies, industrie et résilience . . . . . 56**

10 Logiciels libres, standards et interopérabilité . . . . . 57
11 Data centers, semi-conducteurs, énergie et chaînes d'approvisionnement . . . . 61
12 Cybersécurité, résilience et maîtrise opérationnelle . . . . . 66

**V Recherche, marchés et concurrence . . . . . 71**

13 Recherche, financement, startups et industrialisation . . . . . 72
14 Commande publique et politique industrielle . . . . . 76
15 Adoption, concurrence, coopération et effets de réseau . . . . . 81

**VI Mesure, scénarios et autonomie . . . . . 86**

16 Construire un tableau de bord des capacités et dépendances . . . . . 87
17 Scénarios européens, arbitrages et politiques possibles . . . . . 92
18 Vers une autonomie cloud progressive, mesurable et réaliste . . . . . 96
Conclusion . . . . . 100
Épilogue . . . . . 102

# Introduction

Imaginez une organisation qui annonce avoir « migré au cloud ». Les serveurs locaux ont disparu. Les factures mensuelles ont remplacé les amortissements. Les équipes travaillent plus vite. Pourtant, personne ne sait encore combien coûterait une sortie complète, qui répondrait à un incident grave hors heures ouvrables, ni si les compétences nécessaires pour basculer vers un autre fournisseur existent réellement dans l'équipe. Ce scénario n'est pas une preuve empirique. C'est une situation typique. Il montre pourquoi la souveraineté cloud ne se réduit pas à une case cochée sur un contrat d'hébergement.

Ce livre part d'une observation simple : le cloud est devenu une infrastructure économique et stratégique, pas seulement un choix d'outil informatique. Lorsqu'une part croissante du calcul, du stockage et des logiciels repose sur des opérateurs tiers, les questions de dépendance, de coût, de compétences et de capacité industrielle cessent d'être périphériques. Elles deviennent politiques au sens large : elles concernent ce qu'une société, une administration ou une entreprise peut encore maîtriser, substituer ou reconstruire.

## 1 Pourquoi le terme « souveraineté cloud » prête à confusion

Le mot souveraineté évoque d'abord le pouvoir d'un État. Appliqué au cloud, il a glissé vers un vocabulaire flottant. Tantôt il désigne la localisation des données en Europe. Tantôt la nationalité d'un fournisseur. Tantôt une certification. Tantôt une ambition industrielle. Ces usages ne sont pas équivalents. Les confondre transforme le débat en slogans.

Ce livre n'utilise pas « souveraineté cloud » comme une norme juridique européenne déjà établie, ni comme un score unique. Il s'agit d'un **cadre analytique** : un degré de capacités face à des dépendances jugées critiques. Ce cadre distingue, sans les fusionner, la localisation, la propriété, le contrôle opérationnel, l'autonomie industrielle, la réversibilité technique et les leviers institutionnels. Une organisation peut être conforme à une exigence de localisation et rester incapable de sortir. Elle peut acheter chez un fournisseur européen et dépendre de composants, de compétences ou de plateformes hors d'Europe. L'inverse est aussi possible : une dépendance envers un acteur non européen n'est pas automatiquement critique si la substituabilité, les délais et les impacts restent gérables.

## 2 Thèse et limites

La thèse centrale de l'ouvrage est la suivante. La souveraineté du cloud européen résulte du développement progressif de capacités humaines, économiques, technologiques, industrielles et institutionnelles interdépendantes, dont la combinaison permet de réduire les dépendances critiques envers les acteurs non européens.

Cette proposition n'affirme pas que l'Europe a déjà atteint une souveraineté cloud complète. Elle n'affirme pas qu'il faut tout relocaliser, ni que tout fournisseur européen est plus sûr, moins cher ou plus souverain. Elle n'affirme pas que l'open source garantit automatiquement la réversibilité, qu'une certification prouve une compétence opérationnelle transférable, qu'une obligation juridique démontre une migration réussie, ni qu'une hausse de financements prouve une industrialisation effective.

La thèse est une **hypothèse structurante** à examiner chapitre après chapitre. Certaines parties du raisonnement reposent sur des faits bornés et traçables. D'autres restent des mécanismes plausibles, des estimations privées, ou des propositions encore insuffisamment documentées. Le lecteur doit pouvoir voir cette différence.

## 3 Cinq familles de capacités

Pour lire le cloud autrement qu'à travers une étiquette, le livre regroupe les capacités en cinq familles, elles-mêmes détaillées en dimensions plus fines dans le chapitre 2.

Les capacités **humaines** concernent la formation initiale, le supérieur, les laboratoires et la formation continue : sans vivier capable d'opérer, d'auditer et de migrer, les autres leviers restent fragiles. Les capacités **économiques** concernent les prix, le coût total de possession, les effets de verrouillage et la dynamique de marché. Les capacités **technologiques** concernent les logiciels, les standards, la portabilité et les protocoles de sortie. Les capacités **industrielles** concernent les data centers, les semi-conducteurs, l'énergie, les chaînes d'approvisionnement et la maîtrise opérationnelle. Les capacités **institutionnelles** concernent le droit, la commande publique, la régulation et la coopération entre acteurs publics.

Aucune de ces familles ne suffit seule. Un data center local sans contrôle opérationnel ne produit pas une maîtrise. Un budget public sans offre industrialisée ne crée pas une alternative. Une formation abondante sans débouché opérationnel ne réduit pas automatiquement les dépendances critiques.

## 4 Méthode documentaire

Le livre s'appuie sur un appareil de sources et d'affirmations. Chaque affirmation factuelle importante est présentée avec un niveau de confiance explicite. Les niveaux vont de faits solidement établis à des propositions encore insuffisamment documentées. Les sources examinées sont distinguées des pages seulement consultées. Lorsqu'un document n'a pas pu être archivé ou lu intégralement, le texte le dit.

Cette méthode a un coût de lecture : elle ralentit les conclusions. Elle a un bénéfice : elle empêche de transformer une estimation de parts de marché en mesure de souveraineté, ou un règlement en preuve de migration réussie. Les notes de bas de page renvoient aux sources. Elles ne remplacent pas le raisonnement.

Deux grandeurs, souvent citées ensemble, illustrent la discipline requise. En 2025, 52,7 % des entreprises de l'Union couvertes par l'enquête Eurostat déclaraient utiliser des services cloud payants.[1] Selon des estimations privées de juillet 2025, la part des fournisseurs cloud « européens » sur le marché régional d'infrastructure serait restée autour de 15 %, tandis qu'AWS, Microsoft et Google représenteraient ensemble environ 70 %.[2] L'adoption mesure un usage déclaré. Les parts de marché estiment une concentration de l'offre. Ni l'une ni l'autre ne mesure la souveraineté.

## 5 Organisation du livre

Le livre comporte six parties et dix-huit chapitres.

La **première partie** pose le cloud comme infrastructure, clarifie le vocabulaire de la souveraineté et analyse les mécanismes qui rendent une dépendance critique. La **deuxième** traite du capital humain : école, universités, laboratoires, formation continue. La **troisième** ouvre l'économie des choix : comparaison de prix à périmètre équivalent, coût total de possession, migration et portabilité, logiciels libres et standards. La **quatrième** aborde les technologies et l'industrie : base matérielle, cybersécurité et résilience. La **cinquième** relie recherche, financement, commande publique et dynamique de marché. La **sixième** propose un tableau de bord sans score composite, des scénarios analytiques et une synthèse de l'autonomie progressive.

Chaque chapitre pose une question, développe un raisonnement, présente des objections, marque ses limites, puis ouvre vers la suite. Les chapitres les plus avancés reposent déjà sur un corpus examiné. D'autres restent des armatures analytiques enrichies : leurs lacunes sont visibles, non dissimulées.

[1] Eurostat, « 53% EU enterprises used paid cloud services in 2025 », et dataset associé.

[2] Synergy Research Group, 24 juillet 2025 : estimations privées, non auditables via l'article seul.

## 6 Ce que le lecteur pourra conclure, et ce que le livre ne promet pas

À la fin, le lecteur devrait pouvoir distinguer localisation et contrôle, prix catalogue et TCO, texte juridique et industrialisation, adoption et souveraineté. Il devrait disposer d'une méthode pour lire un contrat, un panier tarifaire, un indicateur ou une annonce politique sans les fusionner.

Le livre ne promet pas un classement des fournisseurs. Il ne promet pas une preuve que telle politique européenne a déjà réussi. Il ne promet pas un protocole de migration d'orchestration exécuté si l'essai n'a pas eu lieu. Il ne fabrique pas de pourcentage européen de propriété ultime des opérateurs lorsqu'aucune série homogène n'a été identifiée. Ces absences font partie du résultat de l'enquête.

La suite commence par le cloud lui-même : avant de parler de souveraineté, il faut comprendre ce que l'informatique en nuage a changé dans l'organisation de la production numérique.

PARTIE I

# Le cloud, la souveraineté et les dépendances



CHAPITRE 1

# Le cloud comme infrastructure économique et stratégique

Pendant longtemps, l'informatique d'entreprise a reposé surtout sur des machines et des logiciels installés dans les locaux de l'organisation. On achetait des serveurs, on les amortissait, on les dimensionnait pour un pic d'activité souvent hypothétique. Le *cloud computing*, l'informatique en nuage, a déplacé ce rapport. Une part croissante du calcul, du stockage, des réseaux et des logiciels est désormais fournie à distance, à la demande, par des opérateurs tiers.

Ce déplacement n'est pas un détail d'architecture. Il change la manière dont les organisations investissent, déploient et font évoluer leurs systèmes. Il change aussi, plus discrètement, ce qu'elles peuvent maîtriser, quitter ou remplacer. Avant de parler de souveraineté, il faut donc comprendre ce que le cloud est devenu : non un simple service informatique parmi d'autres, mais une **infrastructure**, une base technique et économique sur laquelle reposent d'autres activités.

Deux lectures, issues d'une analyse de politique numérique, aident à situer l'enjeu sans le trancher. D'une part, le cloud apparaît comme une technologie critique pour la compétitivité de l'Union européenne dans l'économie numérique. D'autre part, les initiatives de « souveraineté des données » (*data sovereignty*) y sont liées à la volonté de réduire des dépendances stratégiques envers des fournisseurs cloud étrangers dominants sur le marché européen.[1] Ces formulations relèvent d'un cadrage argumenté. Elles ne mesurent pas la souveraineté, et elles ne remplacent pas les données d'adoption ou de parts de marché, qui viennent d'autres sources.

[1] Filippo Gualtiero Blancato, « The cloud sovereignty nexus : How the European Union seeks to reverse strategic dependencies in its digital ecosystem », Policy & Internet, 2024 ; DOI 10.1002/poi3.358. Accès examiné via abstract UCL ; PDF intégral non archivé localement, aucune pagination inventée.

## 1.1 Ce que l'on appelle cloud

Pour ce livre, le cloud désigne un mode de fourniture de ressources informatiques, calcul, stockage, réseau, plateformes, applications, accessibles via un réseau, mises à disposition à la demande, et généralement facturées selon l'usage ou un abonnement.

Cette définition est d'abord pédagogique. Elle converge avec la synthèse que propose l'Organisation de coopération et de développement économiques (OCDE) dans son rapport sur la concurrence dans le cloud, en s'appuyant sur les caractéristiques associées à Mell et Grance (2011) : un accès réseau à la demande à un **pool partagé** de ressources configurables, rapidement provisionnées et libérées.[2] La publication primaire du National Institute of Standards and Technology (NIST) n'est pas traitée ici comme source autonome examinée ; on s'appuie sur ce relais institutionnel, sans inventer de pagination NIST.

Deux propriétés expliquent une grande part de l'attrait économique du modèle. La **mutualisation** (*resource pooling*) permet au fournisseur de regrouper des ressources pour plusieurs clients et de les allouer dynamiquement : le client choisit souvent une région ou un niveau de localisation, mais ne contrôle pas nécessairement la machine physique exacte. L'**élasticité** permet d'augmenter ou de réduire les capacités selon la demande, ce qui réduit le besoin d'acheter « pour le pic » en permanence. Ni l'une ni l'autre n'impliquent, à elles seules, une maîtrise juridique, une réversibilité aisée, ni une quelconque souveraineté.

## 1.2 Trois modèles de service, trois partages de responsabilités

Derrière le mot unique « cloud » se cachent des contrats de responsabilité très différents. On distingue habituellement trois modèles de service.

Dans l'**infrastructure as a service** (IaaS, infrastructure en tant que service), le fournisseur met surtout à disposition serveurs, stockage et réseau de base ; le client conserve les systèmes d'exploitation, les applications, les données et une large part de la configuration. Dans la **platform as a service** (PaaS, plateforme en tant que service), le fournisseur opère la plateforme et les outils d'exécution ; le client se concentre sur ses applications, au prix d'un contrôle moindre sur les couches basses. Dans le **software as a service** (SaaS, logiciel en tant que service), le fournisseur opère l'application complète ; le client gère surtout comptes, réglages limités et données métier.

Plus l'on monte vers le SaaS, plus l'on délègue l'exploitation, et plus des choix implicites (identité, région, interfaces, facturation) peuvent s'imposer. Plus l'on reste en IaaS, plus l'on conserve de leviers techniques, au prix d'une charge opération-

[2] OCDE, « Competition in the provision of cloud computing services », OECD Roundtables on Competition Policy Papers No. 323, 20 mai 2025, DOI 10.1787/595859c5-en.

| Modèle | Ce que porte surtout le fournisseur | Ce que porte surtout le client |
|---|---|---|
| IaaS | Infrastructure de base | Systèmes, applications, données, opérations |
| PaaS | Plateforme et outils d'exécution | Applications et leurs réglages |
| SaaS | Application complète | Comptes, configuration limitée, données métier |

nelle plus lourde. L'adoption d'un « service cloud » ne dit donc pas, à elle seule, qui maîtrise quoi.

À ces modèles s'ajoutent les modes de déploiement. Le **cloud public** s'adresse à une clientèle large, opéré par un tiers. Le **cloud privé** désigne un environnement dédié à une organisation. Le **cloud hybride** combine infrastructures du client et services de fournisseurs tiers. Public, privé, hybride d'un côté ; IaaS, PaaS, SaaS de l'autre : les deux axes se croisent. Les confondre obscurcit ensuite l'analyse des dépendances et des dimensions de souveraineté.

Quatre fonctions traversent presque toutes les architectures utiles à ce livre : l'**identité et l'accès** (qui peut se connecter, avec quels droits) ; le **réseau** (comment les services communiquent) ; l'**orchestration** (l'automatisation du déploiement et du cycle de vie) ; les **données** (où elles sont stockées, comment elles circulent, qui peut les extraire ou les supprimer). Ce n'est pas un inventaire de vulnérabilités : c'est une boussole pour lire les couches.

## 1.3 Une pile, pas un produit plat

On peut se représenter le cloud comme une pile. Tout en bas : les équipements et les sites physiques. Au-dessus : l'infrastructure virtualisée, souvent fournie en IaaS. Puis les plateformes, souvent en PaaS. Puis les applications et services logiciels, souvent en SaaS. Enfin les données et les usages.

Chaque couche repose sur celles du dessous. Cette image, conceptuelle, non chiffrée, justifie de traiter le cloud d'abord comme infrastructure systémique, avant de l'évaluer sous l'angle de la souveraineté ou des verrouillages.[3]

## 1.4 Qui gagne quoi dans la chaîne

Autour de cette pile gravitent des acteurs aux intérêts distincts : fournisseurs d'équipements ; opérateurs de sites et de datacenters ; *cloud service providers* (CSP), qui opèrent et vendent IaaS, PaaS ou SaaS ; éditeurs de logiciels souvent hébergés

[3] Figures conceptuelles du chapitre : architecture multicouche et chaîne de valeur (assets/diagrams). Aucune valeur empirique n'y est encodée.

chez un tiers ; intégrateurs et opérateurs de services ; enfin les clients, qui paient pour une valeur métier.

Les flux de services, les flux économiques et les dépendances possibles ne coïncident pas toujours. Un client peut dépendre d'un éditeur SaaS, qui dépend d'un CSP, qui dépend d'équipements et d'énergie. La criticité de ces liens, substituabilité, délais, impacts, sera le sujet d'un chapitre ultérieur. Ici, il suffit de remarquer que la chaîne de valeur du cloud n'est pas plate : elle empile des intermédiaires.

## 1.5 Ce que disent les parts de marché : et ce qu'elles ne disent pas

Les parts de marché des fournisseurs ne mesurent pas la même chose que l'adoption par les entreprises. Selon un article de Synergy Research Group daté du 24 juillet 2025, la part des fournisseurs cloud « européens » sur le marché régional d'infrastructure cloud serait passée de 29 % en 2017 à 15 % en 2022, puis se serait maintenue autour de 15 % « depuis lors » ; AWS, Microsoft et Google représenteraient ensemble environ 70 % du marché au moment de la publication ; la taille du marché européen est estimée à 61 milliards d'euros pour 2024. Le périmètre produit explicite dans l'article couvre l'IaaS, le PaaS et le *hosted private cloud*.[4]

Ces chiffres sont des **estimations privées rapportées**, non des statistiques Eurostat. L'article n'explicite pas formellement le critère d'« European cloud provider » (siège, capital, marque) au-delà d'exemples. Ils n'établissent ni la souveraineté ni son contraire. Ils indiquent une concentration de l'offre telle que la décrit cette source, rien de plus, et rien de moins.

## 1.6 L'adoption : un fait borné, pas une preuve de maîtrise

En 2025, 52,7 % des entreprises de l'Union européenne couvertes par l'enquête Eurostat déclaraient utiliser des services payants d'informatique en nuage. Cette proportion a progressé de 7,4 points de pourcentage depuis 2023 et de 34,9 points depuis 2014.[5]

Ce que cette statistique établit, c'est une diffusion large et croissante de l'usage déclaré de services cloud **payants** dans la population d'enquête. Ce qu'elle ne mesure pas, par construction : l'intensité d'usage ; la qualité, le coût ou la sécurité des services ; les parts des fournisseurs. Une forte adoption peut coexister avec une offre

[4] Synergy Research Group, « European Cloud Providers' Local Market Share Now Holds Steady at 15% », 24 juillet 2025, https ://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15. Estimations privées (méthode SIA™) ; non auditables via l'article seul.

[5] Eurostat, « 53% EU enterprises used paid cloud services in 2025 », 3 février 2026, https ://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260203-1 ; dataset isoc_cicce_use (indicateur E_CC, entreprises ≥ 10 salariés, EU27_2020), extraction 2026-10-11. Valeurs brutes 2014 = 17,82 ; 2023 = 45,32 ; 2025 = 52,74.

concentrée. Les deux grandeurs ne se contredisent pas ; elles ne se substituent pas non plus.

Trois confusions fréquentes méritent d'être écartées dès maintenant. Premièrement, adoption n'égale pas parts de marché. Deuxièmement, adoption n'égale ni localisation des données ni maîtrise opérationnelle : héberger dans une région européenne ne garantit ni le contrôle juridique effectif ni la capacité de sortir. Troisièmement, adoption n'égale pas souveraineté, ni réduction automatique des dépendances critiques. Ces mécanismes seront analysés plus loin ; ils ne se déduisent pas du taux Eurostat.

L'informatique sur site et l'*edge computing* restent pertinents pour certaines charges. Le reconnaître n'affaiblit pas le constat : pour une part croissante des organisations couvertes par l'enquête, le cloud est devenu une option structurante.

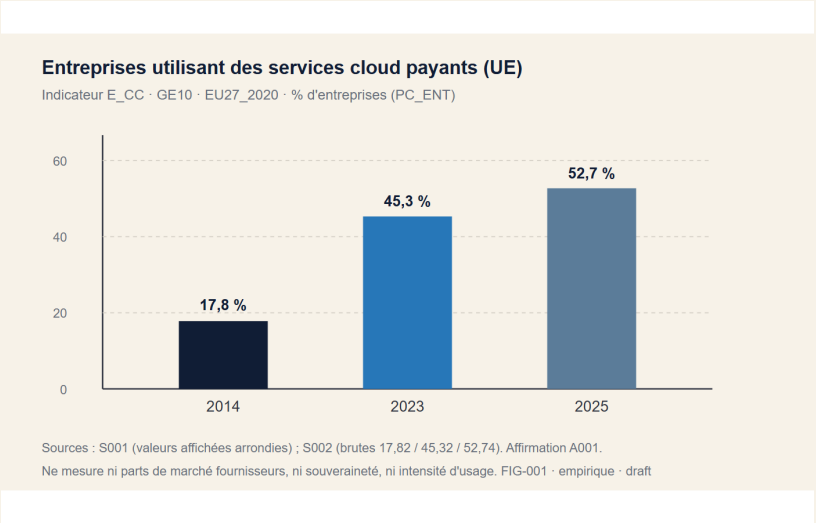



**Fig. 1.1 :** Adoption déclarée des services cloud payants (UE). Ne mesure pas la souveraineté.

## 1.7 Ce que ce chapitre permet de tenir

Le cloud, tel que présenté ici, est une infrastructure : ressources mutualisées et élastiques ; modèles de service à responsabilités variables ; modes de déploiement distincts ; pile en couches ; chaîne d'acteurs et de flux. Les données d'adoption décrivent une diffusion bornée. Les estimations de parts de marché décrivent une concentration de l'offre, avec de fortes réserves. Le cadrage stratégique situe l'enjeu européen sans conclure à une souveraineté atteinte.

Reste alors une question préalable, sans laquelle la suite du livre flotterait : que peut bien vouloir dire « souveraineté cloud » lorsque juridiction, contrôle opérationnel, technologie, données, économie et industrie se mêlent, et que faut-il refuser de

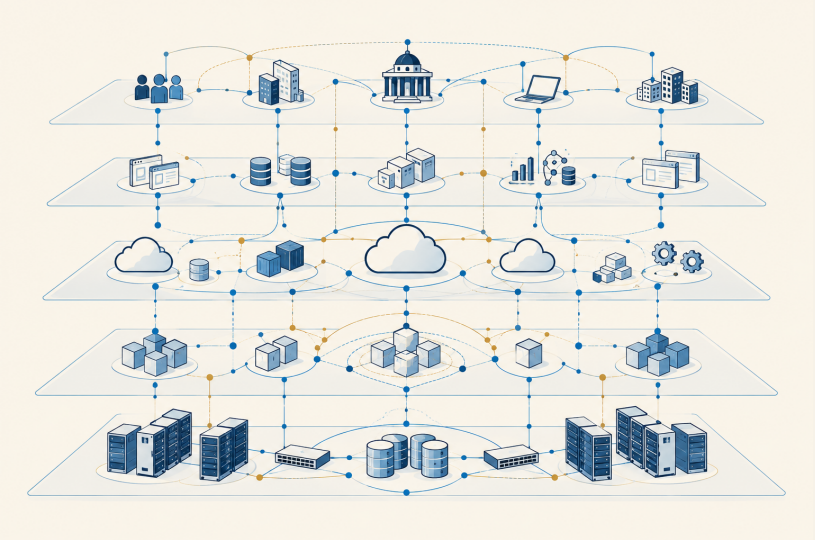


**Fig. 1.2 :** Architecture multicouche — conceptuel non empirique

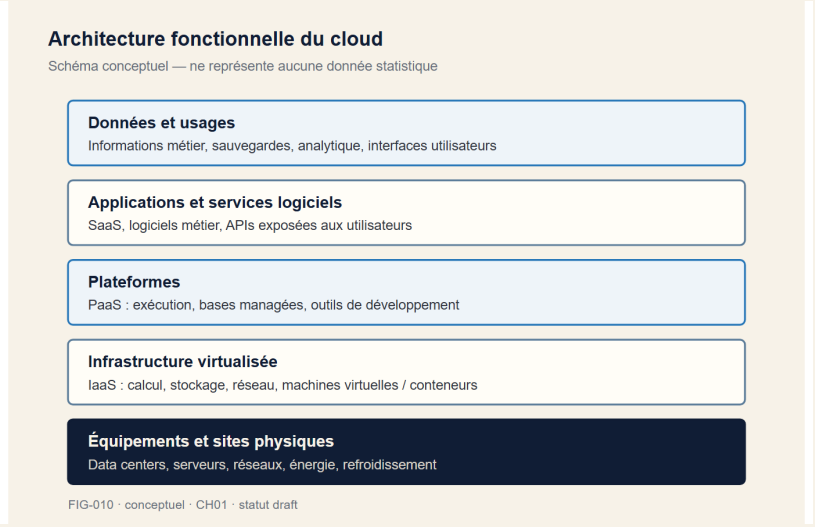



**Fig. 1.3 :** Architecture en cinq couches — schéma pédagogique non empirique

mettre sous ce mot ?

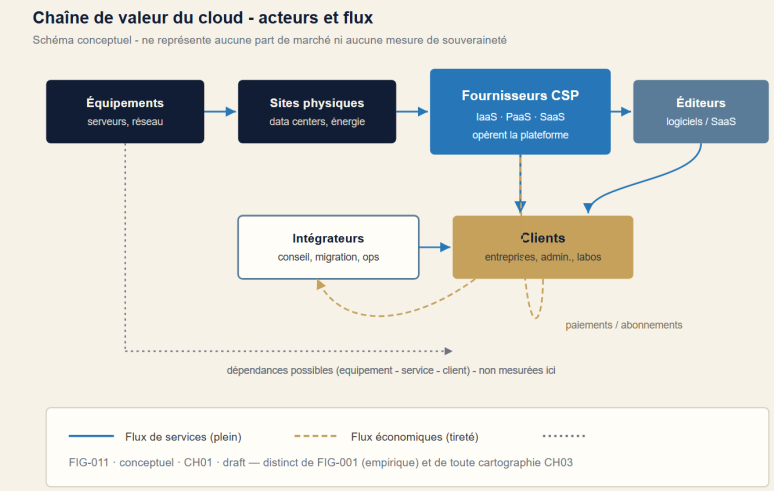



**Fig. 1.4 :** Chaîne de valeur — schéma pédagogique non empirique

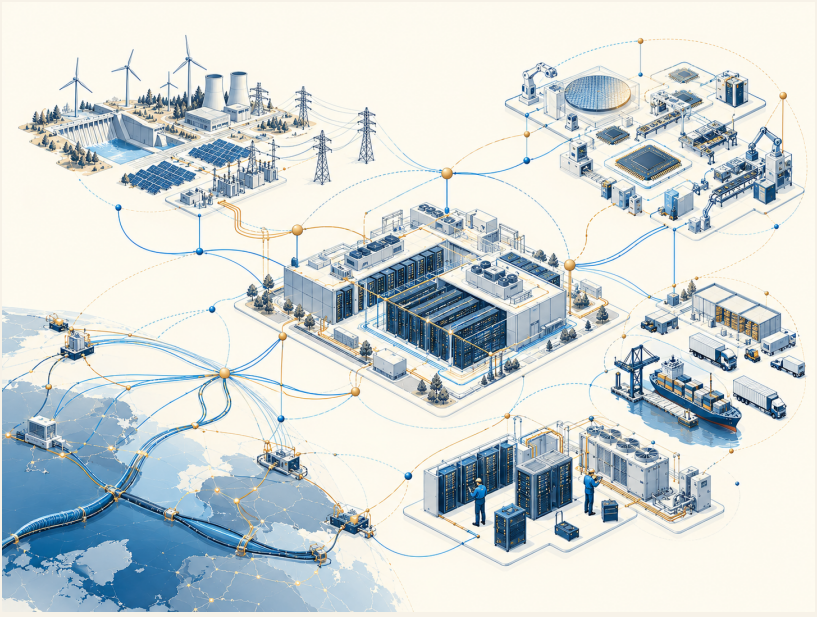


**Fig. 1.5 :** Infrastructure physique et réseau — illustration conceptuelle

CHAPITRE 2

# Que signifie réellement la souveraineté cloud ?

Le mot « souveraineté » circule aujourd'hui dans les discours publics, les stratégies industrielles et les catalogues commerciaux. Appliqué au cloud, il promet tantôt le contrôle des données, tantôt l'autonomie technologique, tantôt la simple localisation des serveurs sur le territoire européen. Ces usages ne sont pas interchangeables. Tant qu'on ne précise pas *de quoi* l'on parle, la thèse de ce livre, des capacités interdépendantes pour réduire des dépendances critiques, reste indécidable.

Le chapitre précédent a montré que le cloud est devenu une infrastructure, et que l'adoption d'un service n'équivaut pas à sa maîtrise. Il reste à fixer un vocabulaire. Ce chapitre propose un **cadre de lecture**. Il ne démontre pas que l'Europe a atteint la souveraineté cloud, ni qu'elle l'a manquée. Il refuse aussi de transformer ce cadre en score composite.

## 2.1 Ce que recouvre déjà le débat politique

Selon le cadrage proposé par Filippo Gualtiero Blancato dans un article de 2024, le cloud computing apparaît comme une technologie critique pour la compétitivité numérique de l'Union européenne, et les initiatives de « souveraineté des données » (*data sovereignty*) y combinent protection des données et instruments de politique industrielle face à des fournisseurs cloud étrangers dominants.[1]

Ce cadrage, tel qu'il ressort de la présentation publique de l'article, sans appui sur une pagination du texte intégral, éclaire un usage politique du vocabulaire : lier protection et réduction de dépendances stratégiques. Il n'établit pas le cadre à huit dimensions proposé plus bas, ni une norme officielle, ni des parts de marché, ni le constat qu'une souveraineté serait déjà atteinte. Les chiffres de concentration de l'offre, lorsqu'ils interviennent, relèvent d'autres sources, et d'un autre chapitre.

Trois glissements rhétoriques méritent d'être nommés dès maintenant. Premier glissement : traiter « data sovereignty » comme synonyme de « cloud sovereignty ». La maîtrise des données n'épuise ni le contrôle opérationnel, ni la base industrielle, ni la réversibilité. Deuxième glissement : traiter la localisation européenne comme preuve de maîtrise. Héberger n'est pas décider. Troisième glissement : traiter un fournisseur « européen » comme automatiquement plus souverain. La nationalité d'une marque n'équivaut pas à la substitutabilité des piles, des composants ou des compé-

[1] Filippo Gualtiero Blancato, « The cloud sovereignty nexus : How the European Union seeks to reverse strategic dependencies in its digital ecosystem », *Policy & Internet*, 2024, DOI 10.1002/poi3.358.

tences.

## 2.2 Un précédent institutionnel : DigComp

Avant d'introduire le cadre propre à ce livre, un contraste est utile. Le cadre européen DigComp, élaboré par la Commission et le Joint Research Centre, décrit des compétences numériques pour la vie quotidienne, l'apprentissage, le travail et la participation sociale. DigComp 3.0 en est la cinquième édition ; le cadre se présente comme *technology-neutral* et adaptable.[2]

DigComp montre qu'un référentiel multidimensionnel institutionnel peut exister sans être un slogan. Il ne définit pourtant pas la souveraineté cloud, et il ne mesure pas les compétences d'exploitation d'infrastructures cloud. Multiplier les dimensions n'est donc pas, en soi, une invention arbitraire, encore faut-il préciser l'objet mesuré.

Ce contraste a une utilité pédagogique. Il autorise le livre à proposer plusieurs dimensions sans imiter DigComp, et sans laisser croire qu'un cadre de compétences citoyennes mesure déjà l'autonomie cloud. DigComp restera mobilisé au chapitre scolaire comme contraste ; ici, il sert surtout à éviter la confusion des objets.

## 2.3 Un degré de capacités, non une étiquette

Dans ce livre, la **souveraineté cloud** désigne un **degré**, et non une étiquette binaire, de capacités permettant de réduire des **dépendances critiques**. Ce cadre analytique est propre à l'ouvrage ; **ce n'est pas une norme officielle européenne**.[3]

Huit dimensions organisent la lecture. Chacune se formule comme une question, non comme un score.

| Dimension | Question opérationnelle |
|---|---|
| Juridique | Quelles règles et juridictions s'appliquent effectivement aux données, aux accès et aux contrats ? |
| Opérationnelle | Qui configure, supervise, répond aux incidents et contrôle les identités ? |
| Technologique | Qui maîtrise les piles, les interfaces, les composants critiques et leur substitutabilité ? |
| Données | Qui peut extraire, porter, supprimer, analyser ou restreindre les flux ? |
| Économique | Les alternatives sont-elles viables aux coûts et délais pertinents ? |

[2] Commission européenne / Joint Research Centre, *Digital Competence Framework* (DigComp) 3.0, page institutionnelle JRC.

[3] Cadre analytique de l'ouvrage *La souveraineté du cloud européen*.

| Dimension | Question opérationnelle |
|---|---|
| Industrielle | Existe-t-il une base de data centers, de composants, d'énergie et d'approvisionnement mobilisable ? |
| Résilience | Le système absorbe-t-il chocs et défaillances sans rupture inacceptable ? |
| Réversibilité | Une sortie a-t-elle été **testée**, et non seulement déclarée ? |

Ces dimensions se chevauchent volontairement. La localisation des données n'est pas le droit applicable ; les outils techniques ne suffisent pas sans opérations ; la réversibilité croise à la fois la technique et l'économie. Les figures associées à ce chapitre sont conceptuelles : elles illustrent ces dimensions, les familles de capacités et l'idée de substitution, sans encoder de mesure ni de score.

Le cadre refuse plusieurs raccourcis fréquents : la localisation seule ; la nationalité du fournisseur ; la conformité seule ; le taux d'adoption ; les parts de marché ; DigComp comme indicateur de souveraineté cloud ; tout score composite unique.

## 2.4 Tensions utiles entre dimensions

Un acheteur peut exiger une localisation européenne et découvrir, en incident, que les accès privilégiés et les outils de supervision restent hors de sa portée. Une organisation peut disposer d'une base juridique robuste et manquer d'alternatives économiques viables. Une administration peut financer des data centers et rester captive d'interfaces PaaS non substituables. Une équipe peut réussir un export de données et échouer à reconstruire le service.

Ces tensions ne sont pas des études de cas inventées. Ce sont des configurations analytiques. Elles justifient de garder les dimensions séparées dans le tableau de bord du livre, plutôt que de les fondre en un indice unique.

## 2.5 Limites sur la dimension juridique

La dimension juridique, pour être consolidée au-delà de ce cadre de lecture, appellerait des textes de droit de l'Union examinés comme sources primaires, ainsi qu'une doctrine et, le cas échéant, la comparaison avec d'autres cadres de capacités. Tant que ces éléments ne sont pas établis dans le même appareil de sources, les affirmations juridiques fortes restent hors de portée d'un fait établi. Le *Data Act*, les marchés publics et les cadres d'acheteur seront traités plus loin comme sources distinctes, sans être absorbés ici dans une définition générale.

## 2.6 Objections

On objecte que huit dimensions rendent le débat trop complexe. La complexité est le prix de la précision : un mot unique a déjà produit assez de confusions. On objecte qu'il faudrait un score pour décider. Un score sans méthode validée décide mal ; ce livre l'interdit par défaut. On objecte enfin que le vocabulaire politique suffit : le vocabulaire politique éclaire des intentions ; il ne mesure pas des capacités.

## 2.7 Repères de vocabulaire

Le débat sur la « data sovereignty » relie protection et dépendance stratégique, sans mesurer à lui seul la souveraineté. DigComp rappelle qu'un cadre multidimensionnel institutionnel peut exister pour un autre objet, les compétences numériques citoyennes. Le vocabulaire de ce livre fixe un degré de capacités face à des dépendances critiques, sans norme officielle et sans score unique.

Reste alors une question distincte, que la définition ne tranche pas : *quelles* dépendances deviennent critiques, et *par quels mécanismes* le verrouillage opère-t-il une fois l'infrastructure adoptée ?

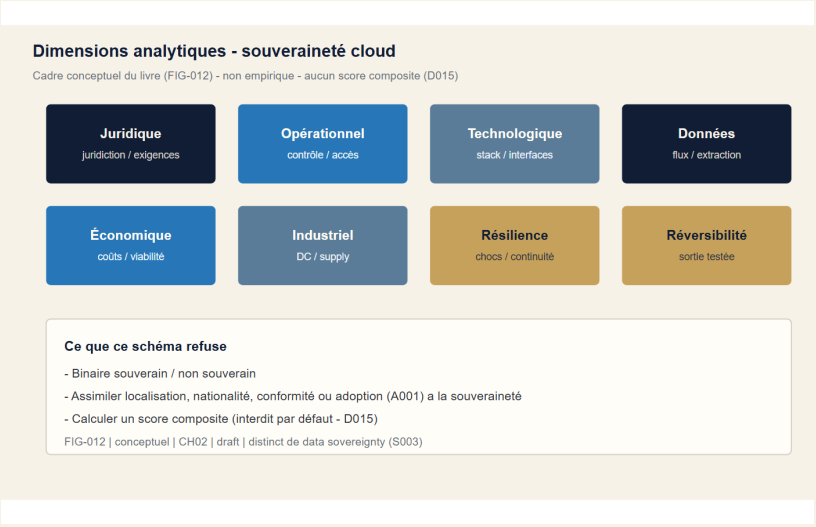



**Fig. 2.1 :** Huit dimensions analytiques — non empirique

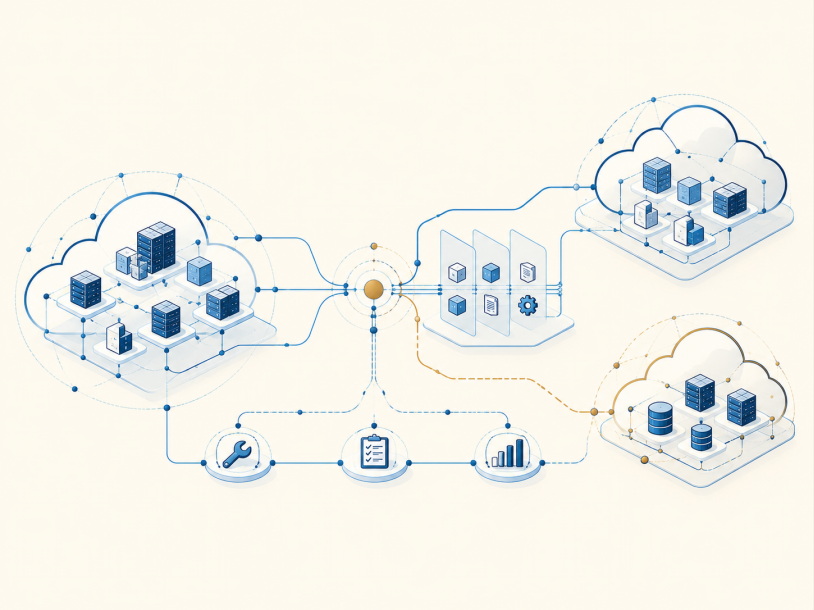


**Fig. 2.2 :** Réversibilité et substitution — illustration conceptuelle



**Fig. 2.3 :** Cinq familles de capacités — illustration conceptuelle

CHAPITRE 3

# Cartographier les dépendances critiques

Toute organisation dépend d'autres acteurs. Le cloud ne crée pas la dépendance : il en redistribue la forme. Une fois le service adopté, la question n'est plus seulement « qui héberge ? », mais « peut-on substituer, en combien de temps, à quel coût, avec quel impact ? ». Lorsque la réponse est défavorable, la dépendance devient **critique**.

Le chapitre précédent a fixé un vocabulaire : la souveraineté cloud, dans ce livre, désigne un degré de capacités face à de telles dépendances. Il reste à comprendre *comment* le verrouillage se produit. Ce chapitre cartographie des mécanismes. Il ne chiffre pas les coûts de sortie, ni ne valide un protocole de migration : ces questions, lorsqu'elles sont traitées, le sont ailleurs dans l'ouvrage.

## 3.1 Familles de dépendances et critères de criticité

On peut distinguer, à titre analytique, plusieurs familles : les données ; le runtime et la plateforme ; le logiciel et le SaaS ; les compétences ; le juridique ; l'approvisionnement et le physique. La figure associée à cette typologie est conceptuelle : elle ordonne la lecture, elle ne mesure aucune criticité.

Quatre critères forment ici une **grille analytique propre au livre**, et non une méthode officielle : une substituabilité limitée ; des délais ou des coûts de sortie élevés ; un impact élevé en cas d'indisponibilité ou de rupture ; une asymétrie d'information entre client et fournisseur. Concentration du marché, difficulté de substitution et criticité stratégique ne se confondent pas. Une mesure systématique, charge par charge, à l'échelle de l'Union européenne, n'est pas encore disponible.

Cette grille a une conséquence immédiate. Une dépendance peut être large sans être critique, si la sortie reste rapide et peu coûteuse. À l'inverse, une dépendance étroite, un seul service managé, une seule région, une seule équipe formée, peut devenir critique si l'impact d'une rupture est élevé. Le volume d'usage ne mesure pas la criticité.

## 3.2 Ce que documente l'OCDE sur le verrouillage

Le rapport de l'OCDE sur la concurrence dans la fourniture de services cloud attire l'attention sur plusieurs mécanismes qui, dans plusieurs juridictions, préoccupent les autorités.[1]

**Concentration.** L'offre se concentre autour de quelques grands fournisseurs. Ce

[1] OCDE, « Competition in the provision of cloud computing services », OECD Roundtables on Competition Policy Papers No. 323, 20 mai 2025, DOI 10.1787/595859c5-en.

constat décrit une structure de marché ; il ne prouve pas, à lui seul, que *chaque* dépendance d'une organisation européenne est critique. Les estimations privées de parts, fournisseurs cloud « européens » autour de 15 % après 2022, trio AWS–Microsoft–Google autour de 70 % au moment d'une publication de juillet 2025, fournissent un **contexte**, pas une cartographie de non-substituabilité.[2]

**Complexité du changement.** Les barrières au changement de fournisseur (*switching*) incluent des processus de migration complexes et des obstacles techniques, contractuels et financiers, ainsi que des limites d'interopérabilité et de standardisation. Une dépendance banale peut devenir critique simplement parce que sortir est long, cher ou risqué. Des délais et coûts de migration européens, reproductibles et comparables, manquent encore.

**Frais de sortie des données.** Les frais pour faire sortir des données d'un cloud (*egress*) peuvent renchérir le changement de fournisseur et contribuer au *lock-in*. Des études nationales rapportent parfois des marges très élevées : ce sont des indices secondaires, non repris ici comme faits établis pour l'Union. Une comparaison datée et homogène serait nécessaire avant toute généralisation chiffrée. Le chapitre sur les prix reviendra sur la nécessité d'un protocole avant tout classement.

**Crédits et remises.** Crédits gratuits et remises de volume peuvent influencer le choix initial et renforcer l'ancrage. Le mécanisme est commercial, distinct de la compétence technique. Son effet causal sur le verrouillage européen n'est pas mesuré ici. Il suffit de noter qu'un bas prix d'entrée n'informe pas sur le coût de sortie.

**Interopérabilité limitée.** Le manque de standardisation entre services complique les stratégies multi-cloud. Il est plausible, mais cela demeure une **hypothèse**, non démontrée dans ce chapitre, que la dépendance à des interfaces et services managés différenciés, surtout en PaaS et en SaaS, dépasse souvent celle d'un IaaS plus homogène. Aucune cartographie d'interfaces critiques à l'échelle de l'UE n'est produite ici. La figure associée illustre l'enjeu d'interopérabilité ; elle n'en mesure pas l'ampleur.

**Coordination du multi-cloud.** Le multi-cloud apparaît souvent comme réponse à la dépendance envers un seul fournisseur. Lorsqu'il est mis en œuvre, il peut, **à titre d'hypothèse**, réduire certains risques tout en **augmentant** les coûts d'intégration et les exigences de compétences. Des cas européens documentés manquent ici ; aucun cas d'entreprise n'est inventé pour combler cette lacune. La figure associée contraste un hub unique et un maillage multi-environnements, sans prétendre décrire un terrain empirique.

[2] Synergy Research Group, « European Cloud Providers' Local Market Share Now Holds Steady at 15% », 24 juillet 2025.

## 3.3 Les compétences comme mécanisme plausible

Même lorsque la portabilité technique est partielle, l'absence de compétences opérationnelles transférables peut bloquer une sortie. Une organisation peut exporter des objets et rester incapable de reconstruire le service faute d'équipes formées à une autre pile. Ce point appartient à la typologie de ce chapitre ; il n'y est pas démontré. La formation, les certifications et la conservation des compétences feront l'objet de la partie suivante du livre.

## 3.4 Ce que ce chapitre refuse de conclure

Il refuse de dire que toute dépendance envers un acteur non européen est critique. Il refuse de dire que la concentration seule prouve l'absence de souveraineté. Il refuse de chiffrer un coût moyen européen de migration sans série comparable. Il refuse d'inventer une cartographie charge par charge. Ces refus ne sont pas des faiblesses stylistiques : ils protègent la thèse contre une démonstration trop large pour les preuves disponibles.

## 3.5 Objections utiles

On objecte parfois que la portabilité est « déclarée » dans les contrats ou les pages marketing ; que le *lock-in* est exagéré dès que l'on reste en IaaS relativement standard ; que le multi-cloud « résout » le problème. Ces objections sont sérieuses. Elles ne se tranchent pas sans preuves de réversibilité **testée**, durée, coût, écarts fonctionnels, plutôt que promise.

On objecte aussi que les frais d'egress baisseront sous la pression réglementaire. Possible pour certains postes. Cela n'élimine ni la dette applicative, ni les compétences manquantes, ni le double run. Le droit peut faciliter ; il ne remplace pas l'essai.

## 3.6 Ce qui est documenté, ce qui reste ouvert

Concentration, barrières au changement, egress, crédits commerciaux et limites d'interopérabilité sont documentés au niveau institutionnel par l'OCDE, avec le contexte de marché fourni par des estimations privées. Leur impact européen quantifié, charge par charge, reste ouvert. Les compétences forment un mécanisme plausible, non encore prouvé dans ces pages.

La suite du livre quitte le seul registre des mécanismes techniques et commerciaux pour examiner une famille de capacités souvent négligée dans les débats de souveraineté : le capital humain, en commençant par l'école, sans prétendre qu'elle produit à elle seule l'autonomie cloud.

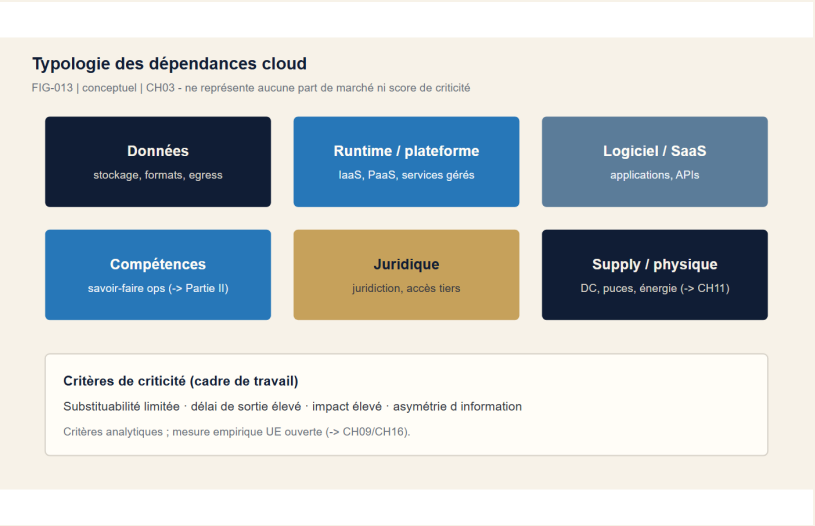



**Fig. 3.1 :** Six familles de dépendances — conceptuel

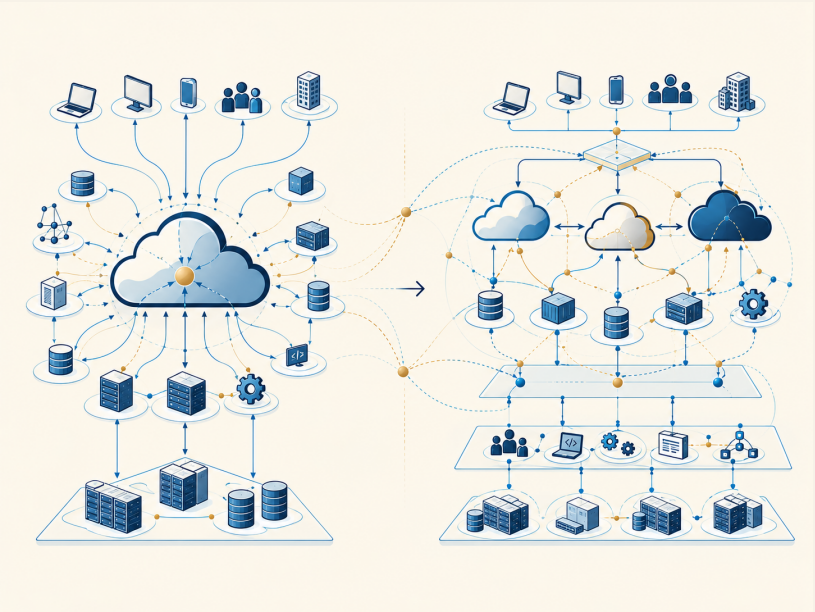


**Fig. 3.2 :** Concentration et multi-cloud — illustration conceptuelle

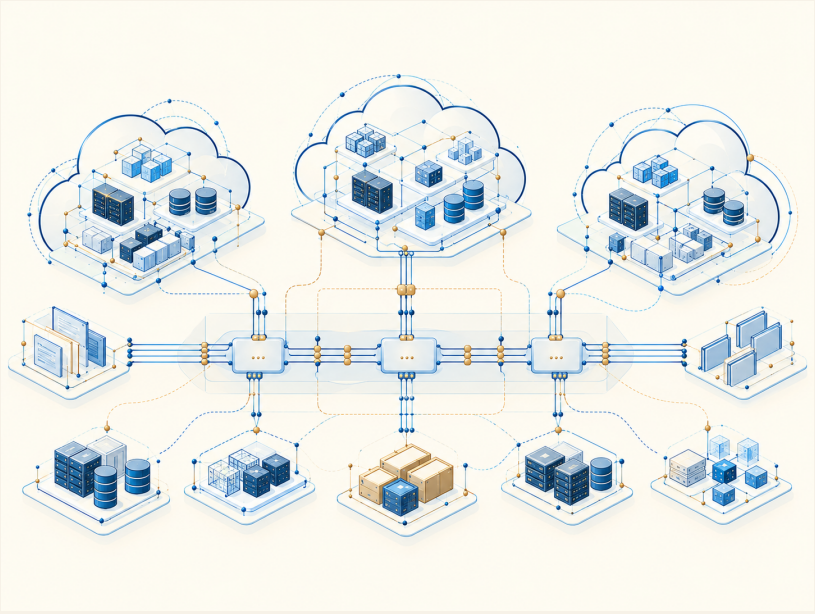
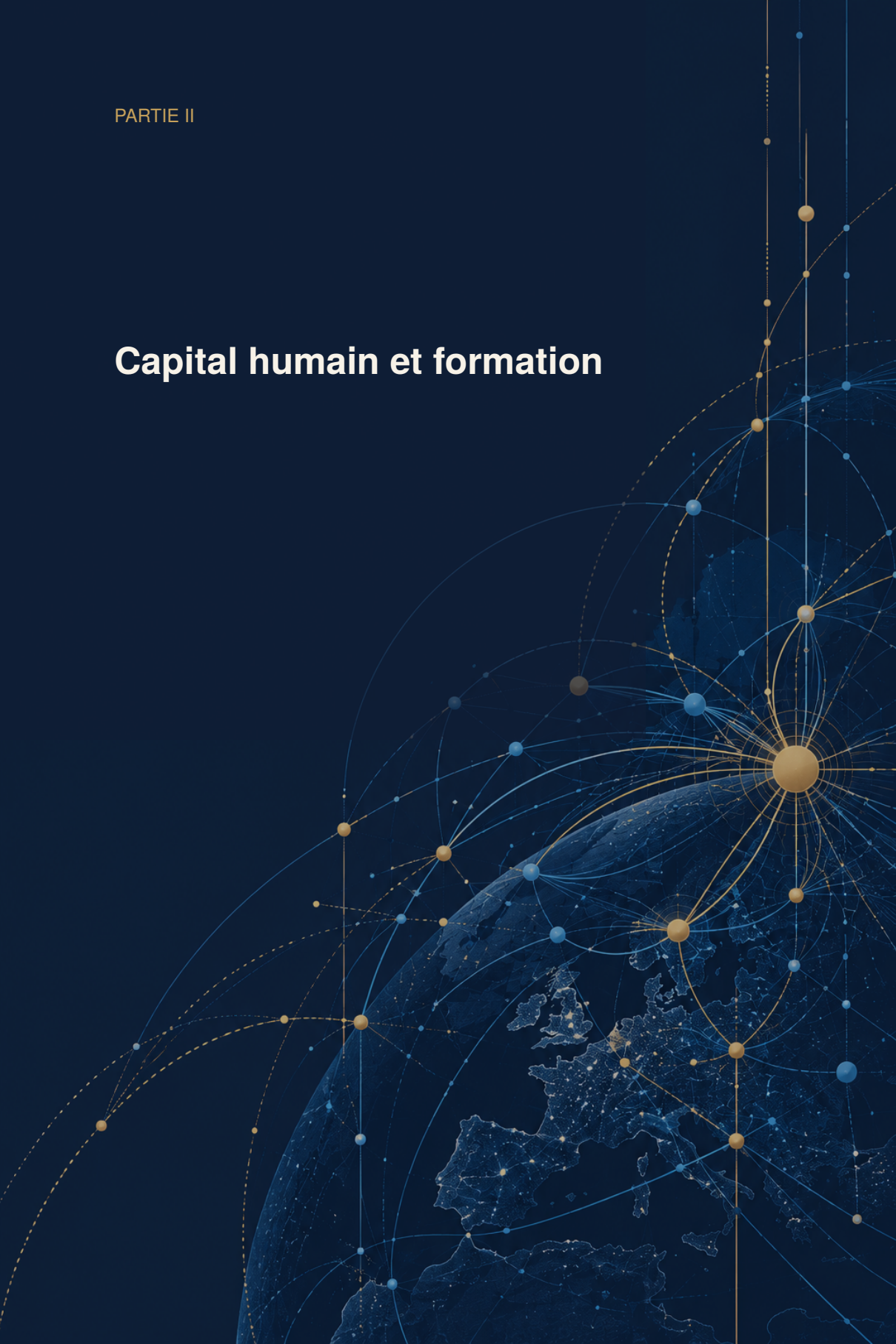


**Fig. 3.3 :** Interopérabilité multi-environnements — illustration conceptuelle



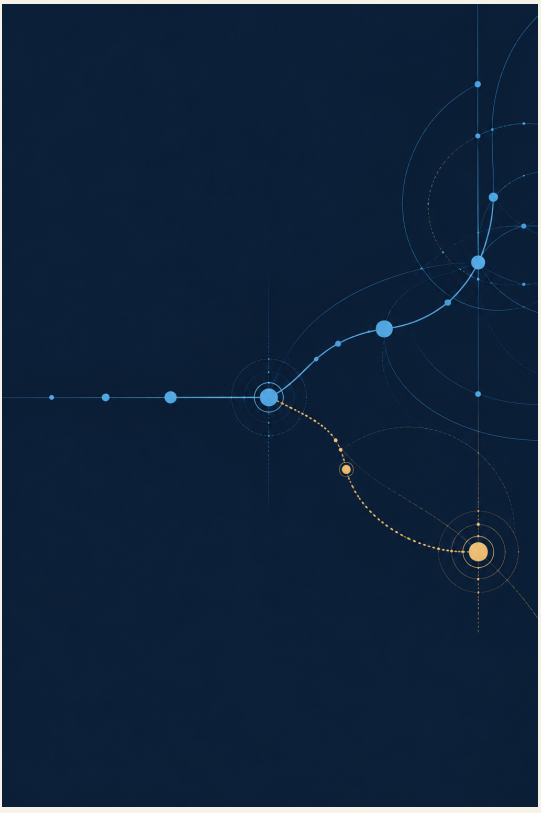
PARTIE II

# Capital humain et formation



CHAPITRE 4

# Former dès l'école : culture numérique et informatique



Transition vers le capital humain (illustration conceptuelle).

Si le cloud est devenu une infrastructure, d'où viennent ceux qui sauront l'architecturer, l'exploiter et, le cas échéant, le quitter ? La réponse la plus tentante est aussi la plus trompeuse : « dès l'école ». Tentante, parce qu'un vivier de compétences ne se crée pas en une année budgétaire. Trompeuse, parce que l'école forme surtout des citoyens et des élèves, non des opérateurs de plateformes.

Les chapitres précédents ont fixé un vocabulaire, degré de capacités face à des dépendances critiques, et des mécanismes de verrouillage. Ce chapitre ouvre la famille du **capital humain** par le socle scolaire. Il examine un rôle *potentiel* de long terme. Il ne prétend pas que l'école garantit la souveraineté cloud.

## 4.1 Trois objets qu'il ne faut pas confondre

Avant toute promesse, trois notions doivent rester distinctes.

| Notion | Sens dans ce chapitre | Ce qu'elle n'est pas |
|---|---|---|
| Compétences numériques | Usages pour vivre, apprendre, travailler, participer (cadre DigComp) | Compétences d'exploitation cloud |
| Enseignement de l'informatique | Curricula, pensée computationnelle, *informatics* | Preuve d'un pipeline vers les métiers cloud |
| Compétences cloud opérationnelles | Architecture, exploitation, sécurité, maîtrise des coûts | Ce que l'école mesure aujourd'hui |

Confondre les trois lignes produit des slogans excessifs : un cours d'initiation au numérique n'est pas une formation d'opérateur ; un module d'informatique n'est pas, à lui seul, une capacité de réversibilité.

## 4.2 Ce que pousse déjà la politique européenne

Selon la recommandation du Conseil du 23 novembre 2023, les États membres sont invités notamment à améliorer l'offre de compétences numériques et à soutenir une éducation de qualité en **informatique** ou en **pensée computationnelle** aux niveaux primaire et secondaire.[1]

Ce texte oriente. Il n'est pas contraignant. Il ne définit pas les compétences d'administration cloud. Il ne mesure pas l'application nationale. Il ne prouve pas un effet sur la souveraineté. Les écarts qu'il évoque, compétences numériques de base, spécialistes des technologies de l'information et de la communication, évaluations internationales, fournissent un **contexte**, non la démonstration d'un pipeline scolaire vers le cloud.

Dans le même sillage, la Commission signale le développement de **lignes directrices** pour l'enseignement de l'informatique, destinées à aider les écoles à renforcer la compétence numérique en classe.[2] L'existence de ces guidelines, telle qu'elle ressort de la présentation institutionnelle, n'équivaut ni à un inventaire des curricula nationaux, ni à une preuve de mise en œuvre homogène. Le détail pédagogique du document n'est pas repris ici comme fait établi ligne à ligne.

[1] Conseil de l'Union européenne, recommandation du 23 novembre 2023 relative à l'amélioration de l'offre de compétences et aptitudes numériques dans l'éducation et la formation, Journal officiel de l'UE.

[2] Commission européenne (DG Éducation et culture / Espace européen de l'éducation), page institutionnelle sur les guidelines d'informatique et le soutien de l'UE.

## 4.3 DigComp : utile, mais pour un autre objet

Le cadre DigComp décrit des compétences numériques citoyennes, *technology-neutral*.[3] Il aide précisément à éviter la confusion entre « digital skills » et compétences d'exploitation d'infrastructures. Comme le rappelait le chapitre définitionnel, DigComp n'est pas un indicateur de souveraineté cloud.

Reprendre DigComp ici n'est pas une répétition gratuite. Au chapitre 2, il servait de contraste définitionnel. Ici, il sert de garde-fou pédagogique : tout progrès mesuré en compétences numériques citoyennes ne peut être compté automatiquement comme progrès en capacités cloud.

## 4.4 Une hypothèse de pipeline, non une démonstration

Dans le cadre analytique de cet ouvrage, l'exposition scolaire précoce à une culture **informatique**, et non seulement numérique, est traitée comme un facteur plausible de pipeline de long terme pour les compétences cloud européennes.[4]

Cette hypothèse reste une hypothèse. Aucune enquête mobilisée ici ne mesure une chaîne « école → compétences d'exploitation cloud → réduction de dépendances critiques ». Une figure conceptuelle peut illustrer un parcours formation–pratique–industrie ; elle n'en établit pas la causalité. Le statut de preuve de cette proposition demeure prudent.

La chaîne se rompt en plusieurs endroits. Que l'Union encourage le numérique et l'informatique à l'école est documenté. Que les États mettent en œuvre de façon homogène reste inconnu sans inventaire national. Que les élèves acquièrent une culture informatique mesurable est partiellement observable ailleurs, mais non traité ici comme preuve autonome. Que cette culture augmente l'entrée dans des formations cloud opérationnelles est plausible, non démontré. Que ces formations réduisent ensuite des dépendances critiques relève de la thèse du livre, non d'un résultat établi dans ce chapitre.

[3] Commission européenne / Joint Research Centre, *Digital Competence Framework* (DigComp) 3.0, page institutionnelle JRC.

[4] Cadre analytique de l'ouvrage *La souveraineté du cloud européen* (facteur d'exposition scolaire).

## 4.5 Inégalités : ce qui pourrait être regardé

Les politiques elles-mêmes signalent des fractures, de genre, de compétences de base, d'accès. Pour le socle scolaire, des indicateurs candidats, *sans les inventer comme résultats*, seraient par exemple : présence d'un enseignement d'informatique distinct ; formation des enseignants ; inégalités territoriales d'équipement ; résultats en littératie informatique. Aucun de ces indicateurs n'est produit ici.

Nommer ces indicateurs candidats a une utilité : empêcher qu'un futur tableau de bord scolaire invente des valeurs pour combler le vide. Une case vide reste préférable à une moyenne européenne fabriquée.

## 4.6 Objections

On objecte parfois que le levier réel serait surtout la formation continue des adultes. L'objection est sérieuse : les délais générationnels de l'école sont longs, alors que les piles techniques évoluent vite. L'école reste, dans ce livre, une **condition amont** possible, non un levier unique.

On objecte aussi que DigComp suffirait. Non pour les métiers d'exploitation cloud. Enfin, l'idée que l'école « souverainiserait » le cloud par elle-même est refusée : une capacité humaine amont n'équivaut pas à la maîtrise d'une infrastructure critique.

## 4.7 Ce que l'école établit, et ce qu'elle ne prouve pas

L'Union pousse les compétences numériques et l'enseignement de l'informatique à l'école ; DigComp cadre le numérique citoyen. Un pipeline scolaire vers les compétences cloud est **plausible**, non démontré. La mise en œuvre nationale homogène et le lien empirique jusqu'à la dépendance critique restent ouverts.

L'école, à elle seule, ne produit pas la souveraineté cloud. Reste une question distincte, plus proche des métiers : le supérieur forme-t-il des architectes et des opérateurs, et dans quelles conditions d'accès réel aux environnements de pratique ?



**Fig. 4.1 :** De l'apprentissage à l'industrie — illustration conceptuelle

CHAPITRE 5

# Universités, laboratoires et infrastructures pédagogiques

Un diplôme peut mentionner le cloud. Un catalogue peut promettre des laboratoires. Reste une question plus rude : l'étudiant a-t-il réellement déployé, observé, cassé et réparé quelque chose, ou a-t-il seulement lu des slides sur des services lointains ?

Le chapitre précédent a situé l'école comme socle possible d'une culture informatique de long terme, sans la confondre avec les compétences d'exploitation. Celui-ci change d'échelle. Il examine l'enseignement supérieur, les universités et l'accès aux moyens de pratique. Il ne prétend pas que le supérieur, à lui seul, garantit la souveraineté cloud.

## 5.1 Ce que l'on risque de compter trop vite

Trois objets se croisent ici, facilement amalgamés.

La **formation** dans le supérieur, systèmes, réseaux, cybersécurité, modules cloud, peut exister sur le papier sans produire une capacité opérationnelle. L'**accès réel** à des laboratoires ou environnements, crédits, bacs à sable, clusters, est une autre chose : un catalogue n'est pas un accès, un accès n'est pas un usage, un usage n'est pas une compétence démontrée. La **recherche** et le transfert, enfin, importent pour l'écosystème, mais compter des publications comme une industrialisation serait une confusion ; ce fil sera repris ailleurs dans l'ouvrage.

La formation continue des adultes, les certifications de fournisseurs et la transférabilité des compétences d'exploitation relèvent du chapitre suivant, non de celui-ci.

## 5.2 Une chaîne qu'il ne faut pas écraser

Entre l'offre affichée et l'insertion professionnelle s'étagent plusieurs niveaux. L'offre de cours, module ou diplôme, n'est pas inventoriée ici à l'échelle européenne. L'accès à un environnement utilisable, le temps de pratique, l'évaluation sur des scénarios réels ne le sont pas davantage. Ce que l'on peut documenter, pour l'instant, c'est surtout un **contexte** de vivier formé aux technologies de l'information et de la communication (TIC), distinct des compétences cloud opérationnelles.

Cette chaîne a une implication pour la thèse. Renforcer seulement l'offre nominale de modules cloud peut produire des diplômes sans opérateurs. Renforcer seulement la recherche peut produire des articles sans offre industrialisée. Le supérieur compte pour la souveraineté cloud surtout lorsqu'il relie formation, accès réel et compétences démontrables, ce que le corpus actuel ne mesure pas encore pan-européenement.

## 5.3 Un vivier TIC tertiarisé, pas un compteur « cloud »

Selon l'aperçu statistique d'Eurostat sur l'éducation TIC, le nombre de personnes dans la force de travail de l'Union possédant une **formation TIC** est passé de plus de 2,5 millions en 2016 à 3,6 millions en 2025 ; parmi elles, 3,3 millions étaient employées ; en 2025, 74,8 % des personnes employées avec une formation TIC avaient un niveau d'éducation **tertiaire**.[1]

Ces chiffres étayent un vivier de formation TIC en croissance, fortement tertiarisé, un contexte pertinent pour raisonner sur le supérieur. Ils n'établissent pas le volume de diplômés « cloud », ni l'accès aux laboratoires, ni la qualité opérationnelle, ni l'adéquation fine aux besoins d'infrastructures à grande échelle ou de stratégies de souveraineté. La formation TIC, au sens de l'enquête, désigne des qualifications au moins du secondaire supérieur dans des champs informatiques spécifiés ; ce n'est ni une certification cloud, ni une compétence d'exploitation multi-cloud.

[1] Eurostat, « ICT education, a statistical overview », Statistics Explained.

## 5.4 L'accès réel comme hypothèse

Dans le cadre analytique de cet ouvrage, l'accès **réel** à des laboratoires et environnements cloud dans l'enseignement supérieur est une condition plausible de formation d'architectes et d'opérateurs compétents, **distincte** de la seule existence nominale de modules.[2]

Cette hypothèse n'est pas mesurée ici. Aucun inventaire pan-européen de laboratoires cloud n'est produit. À titre d'outil de lecture, non de méthode officielle, trois critères aident à ne pas confondre l'affiche et la pratique : un environnement effectivement utilisable ; des scénarios d'exploitation (déploiement, observabilité, incident) ; une évaluation portant sur la pratique.

## 5.5 Compromis pédagogiques, sans inventaire

Les établissements qui veulent faire pratiquer le cloud rencontrent des arbitrages, que l'on peut formuler sans inventer de chiffres.

| Option | Avantage plausible | Risque plausible |
|---|---|---|
| Crédits ou bacs à sable d'un grand fournisseur | Coût d'entrée bas, stacks proches du marché | Ancrage dans des outils et des compétences peu transférables |
| Logiciels ouverts / clouds locaux | Transférabilité, contrôle | Charge d'exploitation, écart possible avec le marché |
| Laboratoires sur site de l'établissement | Maîtrise locale | Investissement, obsolescence, échelle limitée |

Aucun volume de crédits éducatifs ni de laboratoires n'est inventé. Les sources primaires de programmes cloud éducatifs restent à examiner avant toute cartographie. Le compromis n'est pas tranché ici : il est nommé pour empêcher qu'un discours de souveraineté ignore le coût pédagogique de la transférabilité.

## 5.6 Objections

On objecte parfois que l'offre serait déjà abondante. C'est possible localement ; sans inventaire, aucun verdict pan-européen n'est fondé ici. On objecte aussi que le vivier TIC tertiarisé prouverait que le supérieur « suffit ». Non : être employé avec une formation TIC n'équivaut ni à une capacité d'exploitation cloud, ni à un accès documenté aux laboratoires. Enfin, la recherche peut enrichir l'écosystème ; elle ne remplace pas, à elle seule, l'industrialisation des compétences et des infrastructures.

[2] Cadre analytique de l'ouvrage *La souveraineté du cloud européen* (accès aux environnements de pratique).

## 5.7 Ce que le supérieur documente

Un vivier TIC tertiarisé en croissance est documenté. L'accès réel aux environnements de pratique comme condition de formation opérationnelle reste une **hypothèse** plausible, non mesurée. La cartographie des laboratoires, l'usage réel et les compétences cloud démontrées restent ouverts. L'affirmation associée conserve un statut prudentiel.

Universités et laboratoires ne suffisent pas, isolément, à garantir la souveraineté cloud. Reste un maillon souvent décisif une fois les diplômes obtenus : la formation continue, les certifications et la transférabilité des compétences d'exploitation, là où le verrouillage humain peut se renforcer ou se desserrer.



CHAPITRE 6

# Former, certifier et conserver les compétences opérationnelles

Un badge peut ouvrir une porte RH. Il ne dit pas si l'on saura sortir d'une plateforme, reprendre un incident sur une autre pile, ou conserver des compétences lorsque les outils changent. Entre le vivier des spécialistes des technologies de l'information et de la communication (TIC) et la capacité opérationnelle **transférable**, l'écart est souvent ignoré, et politiquement confortable.

Les chapitres précédents ont situé l'école et le supérieur. Celui-ci traite le maillon opérationnel du capital humain : formation continue, certifications, pratique et conservation des compétences. Il ne redéfinit pas la souveraineté cloud. Il ne prétend pas que former suffit à la garantir.

## 6.1 Quatre niveaux qu'il ne faut pas amalgamer

| Niveau | Objet | Ce que cela ne prouve pas |
|---|---|---|
| Compétences numériques générales | Cadres type DigComp | Capacité à opérer un cloud critique |
| Emploi de spécialistes TIC | Agrégats statistiques | Compétences cloud multi-fournisseur |
| Compétences propres à un fournisseur | Certifications, consoles | Transférabilité ni réversibilité |
| Capacité opérationnelle démontrée | Incidents, runbooks, migrations, objectifs de service | Souveraineté automatique |

Un spécialiste TIC n'est pas, par construction, un spécialiste des opérations cloud. Un badge vendeur n'est pas, par construction, une preuve de sortie.

Ces quatre niveaux structurent aussi le tableau de bord du livre. Mélanger DigComp, emploi TIC et badges cloud dans un même indicateur de « capital humain souverain » produirait exactement la fausse précision que le chapitre 16 refuse.

## 6.2 Un vivier TIC large, une mesure ops absente

En 2025, 10,45 millions de personnes étaient employées comme spécialistes TIC dans l'Union européenne, soit 5,0 % de l'emploi total.[1]

Ce vivier d'*emploi* se distingue du vivier de personnes *formées* TIC évoqué au

[1] Eurostat, « Number of ICT specialists in the EU continues to grow », 27 mai 2026.

chapitre précédent : ce sont deux grandeurs, non interchangeables. L'Union dispose d'un réservoir TIC large. Ces agrégats **ne mesurent pas** les compétences cloud opérationnelles, ni leur transférabilité d'un écosystème à l'autre.

## 6.3 La certification comme signal, non comme preuve de transfert

Les pages officielles des programmes fondationnels d'AWS, d'Azure et de Google Cloud décrivent des examens centrés sur les concepts et services de chaque écosystème, Cloud Practitioner, Azure Fundamentals, Cloud Digital Leader.[2][3][4]

Dans le cadre analytique de cet ouvrage, une certification fournisseur est traitée comme un **signal de marché plausible**, non comme une preuve automatique de capacité opérationnelle transférable hors de l'écosystème du vendeur.[5]

Cette hypothèse reste une hypothèse. Aucune enquête empirique de transfert multi-cloud n'est mobilisée ici. L'existence de badges n'autorise pas à conclure à un verrouillage effectif des compétences, seulement à prendre au sérieux des mécanismes *plausibles* : courbe d'apprentissage des consoles et des interfaces de programmation ; procédures liées à un fournisseur ; incentives RH autour du badge dominant.

Le point n'est pas d'accuser les certifications. Elles peuvent être utiles pour un premier recrutement ou une montée en compétences sur une pile donnée. Le point est de refuser qu'elles soient comptées comme preuve de réversibilité ou de souveraineté.

## 6.4 Former en continu, conserver sous peine de dépréciation

La formation continue vise à maintenir l'employabilité opérationnelle face à l'évolution des plateformes. Elle se distingue de l'exposition scolaire, des laboratoires du supérieur et du transfert de recherche.

Sans pratique régulière, incidents, exercices de reprise, migrations contrôlées, le capital compétences **peut** se déprécier. Affirmation plausible, non mesurée dans ces pages. La dépréciation n'est pas une loi physique démontrée ici ; c'est un risque opérationnel que tout tableau de bord sérieux doit laisser visible plutôt que de le remplir par défaut.

[2] Amazon Web Services, page « AWS Certified Cloud Practitioner ».
[3] Microsoft, page « Microsoft Certified : Azure Fundamentals ».
[4] Google Cloud, page « Cloud Digital Leader certification ».
[5] Cadre analytique de l'ouvrage *La souveraineté du cloud européen* (certifications et transférabilité).

## 6.5 Objections

On objecte que le marché « valide » les certifications. Cela vaut pour le marché du travail local, non pour la réversibilité d'une infrastructure. On objecte que les compétences générales suffisent : face à la spécificité des piles managées, l'argument de cadrage est sérieux, mais ce n'est pas une démonstration empirique nouvelle ici. On objecte enfin que former n'est pas le levier principal : même alors, l'absence d'opérateurs aux compétences transférables peut bloquer une sortie techniquement envisageable.

## 6.6 Badge, pratique, transférabilité

Ce chapitre fixe une règle de lecture : distinguer badge, pratique et transférabilité. Le vivier TIC décrit un ordre de grandeur d'emploi, pas une autonomie opérationnelle. L'hypothèse de non-transfert automatique des certifications conserve un statut prudentiel.

Reste une autre famille de capacités, souvent mobilisée dans le débat public avec autant de slogans que de preuves : l'**accessibilité économique**. Avant de parler de « moins cher », il faut une méthode pour comparer stockage, calcul et réseau à périmètre réellement équivalent.



PARTIE III

# Économie des choix cloud



CHAPITRE 7

# Comparer stockage, calcul et réseau à périmètre équivalent

« Moins cher » est une phrase courte. Une comparaison cloud honnête est une phrase longue : quelle date, quelle région, quelle classe de service, quelle redondance, quel volume de transfert, quelle devise, quelles taxes, quelles remises invisibles ? Sans ces précisions, le classement n'est qu'une rhétorique chiffrée.

Le chapitre précédent a traité le capital humain opérationnel. Celui-ci ouvre l'accessibilité économique par la **méthode**. Il présente un scénario de panier catalogue partiel, étude illustrative limitée, datée et reproductible. L'accessibilité économique, au sens de ce livre, commence ici : non par un vainqueur, mais par la capacité à lire un prix.

## 7.1 Que mesure un prix par Go, par vCPU ou par heure ?

Un tarif public n'est jamais un chiffre nu. Un prix « par Go » suppose une unité. En facturation cloud, l'unité usuelle est souvent le *gibioctet* (GiB, 2^30 octets), même lorsque la page marketing écrit « GB ». L'écart avec le gigaoctet décimal (10^9 octets) est d'environ 7 % : négligeable pour une conversation, non négligeable pour un panier de plusieurs tébioctets. Un prix « par vCPU » suppose une génération de processeur, un ratio mémoire, parfois un niveau de performance réseau ou d'entrées-sorties. Un prix « par heure » suppose une machine allumée, un système d'exploitation, parfois un disque système non inclus dans la ligne de calcul.

Comparer deux lignes de catalogue sans aligner ces hypothèses revient à comparer des objets différents. Deux machines « 2 vCPU / 4 GiB » peuvent appartenir à des familles distinctes. Deux stockages « standard » peuvent différer par la redondance, une seule zone contre plusieurs zones, et donc par le risque opérationnel, même si le prix au GiB-mois paraît voisin.

## 7.2 Pourquoi un protocole avant tout chiffre

Sans protocole explicite, date, région, configuration, volume, disponibilité, transfert, taxes et devises, hypothèses, un classement de prix n'est pas soutenable comme résultat empirique.[1]

Les mécanismes de verrouillage évoqués plus tôt, frais de sortie des données, barrières au changement, rendent cette exigence nette : un prix de stockage bas peut masquer un coût de transfert élevé. Un calcul apparemment bon marché peut coûter cher dès que la charge sort massivement des données ou dépend d'un service managé non substituable. Les analyses de concurrence soulignent déjà que les frais d'extraction des données (*egress*) peuvent renchérir le changement de fournisseur.[2]

Quatre natures de montant se distinguent. Le **prix catalogue** est la grille publique. La **remise**, engagement, volume, crédits, est souvent opaque. Le **coût observé** est la facture réelle : il est **absent** de ce chapitre. L'**estimation** multiplie une quantité explicitée par un prix catalogue. Confondre estimation et facture est la première erreur ; confondre estimation partielle et classement général est la seconde.

## 7.3 Dimensions minimales d'une comparaison

| Dimension | Exemples | Risque si omis |
|---|---|---|
| Date de relevé | Jour calendaire du prix | Comparaison obsolète |
| Région tarifaire | Europe centrale, Europe de l'Ouest | Écarts intra-européens |
| Service et classe | Stockage standard vs accès peu fréquent ; famille de machine | Non-équivalence |
| Performance | Processeurs virtuels, mémoire, opérations d'entrée-sortie | « Moins cher » mais plus lent |
| Capacité / durée / volume | GiB-mois, heures, GiB sortants | Scalaires incomparables |
| Disponibilité / redondance | Multi-zones vs stockage localement redondant | Risque non pricé |
| Transfert | Sortie Internet, inter-région | Sous-estimation du verrouillage |
| Taxes / devises | Hors taxes / toutes taxes ; dollar / euro | Illusion d'écart |
| Conditions commerciales | Catalogue vs remise | Catalogue ≠ facture |

[1] Cadre méthodologique de l'ouvrage *La souveraineté du cloud européen* (comparaison à périmètre équivalent).

[2] OCDE, « Competition in the provision of cloud computing services », OECD Roundtables on Competition Policy Papers No. 323, 20 mai 2025, DOI 10.1787/595859c5-en.

Ces dimensions ne garantissent pas l'équivalence parfaite. Elles rendent l'inéquivalence **visible**. Une organisation qui publie ces bornes peut être contredite sur les faits ; une organisation qui publie un podium sans bornes ne peut même pas être auditée.

## 7.4 Région, redondance, stockage, calcul, transfert

Cinq leviers techniques pèsent souvent plus que le slogan commercial.

La **région** fixe un catalogue, parfois une latence, et parfois une contrainte juridique de localisation. Deux régions « européennes » ne sont pas un seul marché tarifaire. Le panier utilise `eu-central-1` pour Amazon Web Services et `europe-west1` pour Google Cloud : ce choix est documenté ; il n'est pas une affirmation d'équivalence géographique stricte.

La **redondance** transforme le sens d'un prix de stockage. Baisser le prix en baissant la redondance n'est pas une économie : c'est un transfert de risque. Le **stockage** se décline en classes et en coûts d'opérations ; le panier simplifie en retenant une classe « standard ». Le **calcul** combine famille de machine, système d'exploitation et durée d'allumage. Le **transfert**, surtout la sortie Internet, relie la facture du mois à la difficulté de sortir plus tard. Le chapitre suivant l'intégrera dans un coût total ; le chapitre sur la réversibilité le traitera comme composante de migration. Ici, il suffit de l'inclure pour qu'il cesse d'être invisible.

## 7.5 Gratuité, remises, crédits : pourquoi le catalogue n'est pas la facture

Les mécanismes de gratuité compliquent les comparaisons. Un fournisseur peut offrir une franchise mondiale de transfert sortant ; un autre une franchise très limitée ; un troisième un trafic externe annoncé comme gratuit sur une page commerciale. Tant que ces franchises ne sont pas alignées, et tant que l'on ignore le trafic réel du compte, comparer des lignes « egress » au taux marginal n'est qu'une approximation.

Les remises d'engagement et les crédits d'entrée abaissent souvent le prix unitaire apparent. Elles peuvent aussi renforcer l'ancrage commercial : le bas prix d'entrée n'informe pas sur le coût de sortie. Les analyses de concurrence signalent déjà le rôle plausible des crédits et remises dans le choix initial ; leur effet causal exact sur le verrouillage européen n'est pas mesuré ici.[3] Ce chapitre refuse d'inventer une « remise moyenne européenne ». Il compare des prix catalogue hors engagement, puis avertit que la facture réelle peut différer.

[3] OCDE, « Competition in the provision of cloud computing services », *op. cit.*

## 7.6 Mécanisme : comment un « moins cher » devient un « plus cher »

Imaginez, **scénario illustratif hypothétique**, non un cas observé, une organisation qui choisit un stockage catalogue moins cher, mais en redondance locale, alors que sa charge exige une résilience multi-zones. Le différentiel de prix initial disparaît dès qu'il faut ajouter de la redondance, des sauvegardes, ou absorber un incident. Ajoutez un volume de transfert sortant sous-estimé : le poste d'egress peut dépasser l'économie réalisée sur le stockage. Ajoutez enfin une équipe formée uniquement à la console du fournisseur dominant : le coût de sortie n'apparaît pas sur la facture du mois 1, mais sur le projet de migration du mois 18.

Le mécanisme causal se lit en quatre étapes. Premièrement, le tarif visible oriente le choix d'achat. Deuxièmement, les postes omis, redondance, egress, performance, corrigent le coût d'exploitation. Troisièmement, les compétences et les services propriétaires fixent le coût de sortie futur. Quatrièmement, la somme de ces postes peut inverser l'avantage apparent du mois 1.

## 7.7 Étude illustrative : le panier SCE-BASKET-01

Le scénario retient, pour un mois conventionnel de 730 heures, hors taxes et **sans** remises d'engagement : 1 024 GiB-mois de stockage, une machine Linux d'environ 2 vCPU et 4 GiB de mémoire, et 100 GiB de transfert sortant. Ce panier est une **étude illustrative limitée**. Il n'est ni un devis, ni une architecture de production.

Formules de travail : prix horaire × 730 pour le calcul ; prix au GiB-mois × 1 024 pour le stockage (ou équivalent horaire × 730 × 1 024) ; quantité facturable × taux marginal pour le transfert, après franchise documentée. Ces multiplications sont reproductibles à partir des relevés cités. Elles ne fabriquent pas les valeurs manquantes pour inventer un total multi-fournisseurs.

| Poste | AWS (eu-central-1 | Google Cloud (europe-west1 | Azure | OVHcloud |
|---|---|---|---|---|

### 7.7.1 Couverture du panier : par postes, sans total consolidé

| Poste | AWS (eu-central-1 | Google Cloud (europe-west1 | Azure | OVHcloud |
|---|---|---|---|---|
| Stockage objet / blob « standard » | Complet (catalogue) | Complet (catalogue) | Partiel (Hot LRS ≠ multi-zones) | Partiel (multi-zones ; €) |
| Calcul petite machine Linux | Complet (*t3.medium*) | Complet (*e2-medium*, non identique) | Absent | Absent |
| Transfert sortant 100 GiB | Complet (taux marginal) | Complet (Premium EU) | Absent | Annoncé gratuit sur la page consultée, non superposable |
| Devise / taxes | USD, HT | USD, HT | USD, HT (fragment) | EUR, HT (fragment) |
| Date de relevé | 2026-10-11 | 2026-10-13 | 2026-10-11 | 2026-10-11 |

Lire cette matrice comme une carte de *disponibilité documentaire*, non comme un classement. Les machines AWS et Google Cloud sont proches en étiquette, non en garantie de performance identique. Les redondances et franchises diffèrent. Les devises et équivalences s'opposent encore à tout total unique.

### 7.7.2 Lectures catalogue séparées (estimations, pas un podium)

**Amazon Web Services**, relevé Price List API du **11 octobre 2026**, région `eu-central-1` : stockage objet standard (0,0245 USD/GiB-mois × 1 024) **25,088** dollars ; calcul *t3.medium* Linux (0,048 USD/heure × 730) **35,04** dollars ; transfert au taux marginal (0,09 USD/GiB × 100) **9,00** dollars. Sous-total d'infrastructure catalogue pour *ces trois postes seulement* : **69,128** dollars.[4] Un transfert de 100 Go *peut* tomber dans une franchise mondiale selon le compte ; le panier publie le taux marginal pour rendre le poste visible.

**Google Cloud**, relevé du **13 octobre 2026**, région `europe-west1` : *Cloud Storage* Standard régional ; machine `e2-medium` ; 100 GiB *Premium Tier* vers l'Europe. Estimation : stockage **20,480** dollars ; calcul **24,459** dollars ; transfert **11,880** dollars. Sous-total pour *ces trois postes seulement* : environ **56,819** dollars.[5] Ce sous-total

[4] Amazon Web Services, Price List API, stockage objet, calcul et transfert, région Europe (Francfort), extraction 2026-10-11.

[5] Google Cloud, pages publiques Compute Engine, Cloud Storage pricing et VPC network pricing, consul-

n'est pas un classement face à AWS. Les non-équivalences de la matrice ci-dessus l'interdisent.

**Azure**, fragment : stockage *Hot* en redondance locale (Europe de l'Ouest), extension d'environ **20,07** dollars pour 1 024 unités, LRS ≠ multi-zones.[6] **OVHcloud**, fragment : stockage multi-zones standard, ordre de grandeur d'environ **12,80** euros hors taxes ; trafic externe annoncé comme gratuit sur la page consultée, unités et périmètre non superposables au relevé AWS.[7]

Un régulateur britannique a documenté, dans son périmètre national, des écarts élevés de frais de sortie entre certains acteurs.[8] Cet indice contextualise l'importance de l'egress ; il ne calibre pas le panier européen.

## 7.8 Quelles données réunir avant de conclure à un avantage ?

Avant de conclure qu'un service est économiquement avantageux, une organisation doit au minimum réunir : la date et l'URL du relevé ; la région ; la classe de service et la redondance ; la configuration exacte de calcul ; les volumes de stockage et de transfert estimés sur la trajectoire réelle ; le régime fiscal et la devise ; l'existence ou non d'engagements ; et, si possible, un extrait de facture ou un devis. Sans ces éléments, elle dispose d'une estimation catalogue, utile, mais insuffisante pour une décision d'architecture.

## 7.9 Objections fréquentes

On objecte que les organisations obtiennent toujours des remises et que le catalogue est donc trompeur. L'objection est juste : c'est pourquoi le chapitre distingue catalogue et facture. Elle ne justifie pas d'inventer des remises moyennes. On objecte qu'un fournisseur « européen » serait forcément moins cher. **Ce n'est pas démontré** dans ces pages. On objecte enfin que la méthode est trop lourde pour un acheteur pressé. Sans elle, l'acheteur presse surtout une conclusion prématurée.

Les données manquantes restent ouvertes : équivalence stricte multi-fournisseurs, taxes, remises, coûts observés, machines Azure et OVHcloud alignées poste à poste. Elles ne seront pas comblées par des valeurs inventées.

---

tation 2026-10-13.

[6] Microsoft Azure, Retail Prices API, Blob Hot LRS, West Europe, extraction 2026-10-11.

[7] OVHcloud, page des prix Public Cloud, consultation 2026-10-11.

[8] Ofcom, *Cloud services market study final report* (extrait), 2023 : Royaume-Uni, non une statistique de l'Union européenne.

## 7.10 Ce que cela change pour la souveraineté

L'accessibilité économique est une capacité : elle conditionne l'adoption d'alternatives. Mais une alternative seulement « moins chère » sur un poste catalogue, sans équivalence ni sortie, ne réduit pas automatiquement une dépendance critique. La méthode de comparaison est un instrument de souveraineté au sens du livre, une capacité à lire les prix, non un classement industrialiste.

Reste à agréger ces postes, et d'autres, souvent invisibles sur une grille publique, dans un coût total de possession transparent, sans double comptage et sans inventer les paramètres manquants. C'est l'objet du chapitre suivant.



CHAPITRE 8

# Comprendre le coût total de possession

On peut « économiser » sur le prix catalogue d'une machine virtuelle et perdre sur la sortie des données, le personnel d'astreinte ou une migration mal amortie. Le coût total de possession, *total cost of ownership*, TCO, n'est pas le tarif d'une ligne de facture. C'est la somme, rendue explicite, de ce qu'une organisation engage pour faire vivre, sécuriser et, le cas échéant, quitter un système.

Le chapitre précédent a montré qu'une comparaison de prix exige un protocole. Celui-ci agrège des catégories. Tant que des paramètres déterminants restent non calibrés, le modèle publie des sous-totaux partiels et des lacunes, pas un total maquillé.

## 8.1 Dépense d'infrastructure, coût d'exploitation, coût total

Trois notions s'empilent.

La **dépense d'infrastructure** regroupe ce que la grille publique facture souvent en premier : calcul, stockage, transfert d'exploitation. C'est le territoire du panier du chapitre précédent. Elle est nécessaire ; elle n'est pas suffisante.

Le **coût d'exploitation** ajoute ce qui fait tenir le service au quotidien : supervision, sauvegardes, correctifs, support, astreintes, gestion des incidents. Une partie peut apparaître sur la facture cloud ; une autre dans les salaires, les outils tiers ou le temps interne.

Le **coût total de possession** élargit encore : formation, sécurité, connectivité dédiée, projet de migration initial, double exploitation pendant une transition, et coûts de sortie. Il regarde une trajectoire, pas seulement un mois.

Réduire le TCO à trois lignes de catalogue, c'est confondre le ticket de caisse du mois avec le coût de la trajectoire. L'accessibilité économique, au sens de ce livre, concerne la trajectoire.

## 8.2 Les catégories en langage courant

Avant toute formule, voici ce que chaque famille de coût désigne concrètement.

**Infrastructure** : machines, stockage, transfert d'exploitation en régime permanent, ce que le catalogue affiche le plus clairement.

**Exploitation** : faire tourner le service sans interruption majeure, surveillance, sauvegardes, correctifs.

**Personnel** : salaires et astreintes des personnes qui opèrent, diagnostiquent et répondent aux incidents.

**Sécurité** : identités, détection, audits, réponse aux incidents de sécurité.

**Connectivité** : liens dédiés, diffusion de contenu, peering, réseaux hors catalogue de base.

**Formation** : certifications, laboratoires, montée en compétence hors console unique.

**Migration initiale** : projet de bascule amorti sur la durée d'analyse.

**Double fonctionnement** : période où l'ancien et le nouvel environnement coexistent.

**Réversibilité** : export, réécriture, tests de sortie et indisponibilité éventuelle lorsqu'on quitte plus tard.

Un modèle transparent doit garder ces catégories **disjointes**, séparer ce qui est observé, catalogue, estimé, hypothétique ou scénarisé, et refuser de combler les trous par des moyennes inventées.[1]

Il précise aussi quatre bornes : la **durée** d'analyse (douze mois n'égalent pas trente-six) ; le **périmètre** (IaaS n'égalent pas SaaS) ; la **charge** (stable ou saisonnière) ; les **hypothèses** étiquetées comme telles.

## 8.3 Une seule formule

Une fois les catégories nommées en français, le modèle de travail SCE-TCO-01 s'écrit :

C_TCO = C_infra + C_ops + C_personnel + C_securite + C_connectivite + C_formation + C_migration + C_double_run + C_reversibilite

Cette formule est un **cadre de calcul**, pas une estimation empirique complète. Dès qu'un terme critique reste hypothétique ou inconnu, **aucun total TCO** n'est annoncé : le modèle refuse de publier un TCO complet maquillé.

[1] Cadre analytique de l'ouvrage *La souveraineté du cloud européen* (modèle de coût total de possession).

| Catégorie | Exemples | Statut dans le modèle de travail |
|---|---|---|
| Infrastructure | Calcul, stockage, transfert d'exploitation | Estimation partielle (catalogue AWS du panier) |
| Exploitation | Supervision, sauvegardes, correctifs | Inconnu / à séparer si mesuré |
| Personnel | Salaires opérationnels, astreintes | Hypothétique, non calibré |
| Sécurité | Identités, détection, audits | Hypothétique, non calibré |
| Connectivité | Liens, diffusion de contenu, peering | Hypothétique, non calibré |
| Formation | Certifications, laboratoires | Hypothétique, non calibré |
| Migration / démarrage | Projet initial amorti | Hypothétique, non calibré |
| Double exploitation | Coexistence pendant la bascule | Hypothétique, non calibré |
| Réversibilité | Transfert de sortie, tests de sortie | Hypothétique, non calibré |

Règle anti-double-comptage : le transfert d'exploitation en régime permanent reste dans l'infrastructure ; le transfert **ponctuel** de sortie relève de la réversibilité **ou** de la migration amortie, jamais des deux à la fois.

## 8.4 Sous-total partiel d'infrastructure

Pour ancrer le raisonnement, le sous-total d'infrastructure catalogue AWS du panier précédent (transfert au taux marginal) vaut :

25,088 + 35,04 + 9,00 = **69,128 dollars**.[2]

Ce montant est une **estimation partielle d'infrastructure catalogue**. Ce n'est ni une facture client, ni un classement de fournisseurs. Azure, OVHcloud et Google Cloud ne sont pas agrégés ici en un total unique.

## 8.5 Pourquoi les choix d'architecture déplacent les coûts

Le personnel n'est pas un accessoire : il décide souvent si un catalogue bas reste avantageux. La supervision et le support transforment une architecture en service tenu. La sécurité et la disponibilité déplacent des montants entre infrastructure, exploitation et, indirectement, réversibilité. Un sous-investissement peut diminuer la facture visible et augmenter le coût d'un arrêt, coût rarement visible avant l'arrêt.

Une architecture très managée peut réduire le besoin de personnel d'exploitation tout en augmentant la dépendance à des services propriétaires, et donc le coût de réécriture en sortie. Une architecture plus proche de l'infrastructure peut exiger davan-

[2] Amazon Web Services, Price List API, lignes du panier catalogue Europe (Francfort) reprises du chapitre précédent.

tage d'astreinte tout en facilitant la substitution. Ces arbitrages sont des mécanismes plausibles ; ils ne sont pas chiffrés ici comme constantes européennes.

L'automatisation suit la même logique. Des scripts d'infrastructure-as-code peuvent baisser le coût marginal d'exploitation et faciliter une migration ultérieure, *si* ils ne sont pas liés à des extensions propriétaires. Sinon, ils accélèrent surtout le déploiement *dans* un écosystème.

## 8.6 Migration, double fonctionnement et réversibilité

La **migration initiale** amortit un projet : conception, tests, bascule. La **double exploitation** désigne la période où les deux environnements coexistent : elle protège la continuité, au prix d'un doublement temporaire de certains postes. La **réversibilité** désigne ce qu'il faudra pour sortir plus tard. Elle sera le cœur du chapitre suivant ; elle figure déjà dans la formule parce qu'un TCO sans sortie est un TCO de captivité assumée, ou oubliée.

## 8.7 Sensibilité qualitative : sans simulation inventée

Certains paramètres, **une fois sourcés**, peuvent renverser un avantage apparent de catalogue.

| Paramètre | Direction plausible | Statut |
|---|---|---|
| Volume de transfert récurrent | Hausse favorise les faibles frais de sortie | À calibrer |
| Intensité de plateformes propriétaires | Hausse augmente le coût de réécriture | Hypothèse |
| Ratio personnel / infrastructure | Hausse réduit l'avantage d'un catalogue bas | Hypothèse |
| Engagement pluriannuel | Baisse du prix unitaire, hausse du coût de sortie | Qualitatif |
| Durée d'analyse | Allongement amortit ou révèle les coûts de sortie | Méthode |

Cette table n'est pas une simulation quantitative. Aucune valeur numérique n'est inventée pour les paramètres non calibrés. Lorsque les données sont incomplètes : lister les trous ; estimer seulement ce qui est mesurable ; identifier les postes qui invertiraient l'arbitrage ; décider si l'incertitude restante est acceptable.

## 8.8 Fiche pédagogique à compléter : hypothèse illustratrice

Supposons, **hypothèse non observée**, qu'une organisation dispose du sous-total d'infrastructure catalogue de 69,128 dollars pour un mois. Elle ne connaît pas encore son astreinte, sa supervision ni le coût d'un test de sortie. Plutôt que d'inventer un « TCO moyen », elle peut remplir la fiche suivante.

| Case | Contenu à renseigner | Statut actuel (exemple) |
|---|---|---|
| Données observées | Factures, tickets, temps d'incident | À compléter |
| Données catalogue | Lignes de grille datées | Partiel (infra 69,128 USD) |
| Données manquantes | Astreinte, supervision, devis de sortie… | Liste ouverte |
| Hypothèses explicites | Durée d'analyse, périmètre, charge | À écrire |
| Responsable de validation | Nom / rôle interne | À désigner |

Cette fiche n'est pas un cas réel. Elle montre comment refuser une fausse précision.

## 8.9 Objections et pièges

Le *FinOps*, le pilotage des dépenses cloud, est utile pour la facture courante ; il reste incomplet pour la réversibilité et les compétences. Des benchmarks industriels n'entrent ici que s'ils sont sourcés, datés et périmétrés. Un TCO trop large peut devenir inutilisable : mieux vaut un sous-total honnête.

Un piège plus subtil : en chargeant la sortie, on pourrait rendre toute alternative « européenne » artificiellement chère, alors que rester chez un hyperscaler éviterait ce coût immédiat. L'objection est sérieuse. Elle ne justifie pas d'exclure la sortie : elle justifie de la séparer, de la dater, et de la comparer à d'autres risques, indisponibilité, changement de conditions commerciales, obligation réglementaire.

## 8.10 Pont vers la sortie

Une capacité économique de souveraineté n'est pas le prix le plus bas du mois. C'est la capacité à voir les postes qui fixent la dépendance : compétences, double fonctionnement, sortie. Le TCO n'établit pas, à lui seul, la souveraineté. Il rend visibles des conditions économiques sans lesquelles le discours de souveraineté reste indécidable.

Reste la question distincte de la **sortie** : ce que le droit européen impose, ce que les analyses de concurrence décrivent, et ce qu'il faut *tester* pour parler de réversibilité réelle, plutôt que de portabilité promise.



CHAPITRE 9

# Expérimenter, migrer et réduire les coûts de sortie

Un contrat peut promettre la portabilité. Une page marketing peut affirmer que les données « sortent ». Une obligation légale peut même interdire certains frais de changement de fournisseur. Reste la seule question qui tranche : a-t-on **testé** une sortie, durée, coût, écarts fonctionnels, ou s'est-on contenté de la déclarer ?

Ce chapitre ne rapporte **aucune** expérimentation de migration déjà menée pour cet ouvrage. Il propose une grille de preuve, un rappel du droit européen, et une checklist pour *préparer* un test crédible. Un protocole conteneurisé a été formalisé sur le papier ; **il n'a pas été exécuté**.

Les chapitres précédents ont cartographié des mécanismes de verrouillage, une méthode de comparaison et une grille de coût total. Celui-ci demande : *peut-on sortir, en combien de temps, à quel coût réellement éprouvé ?*

## 9.1 Quatre niveaux de réversibilité

| Niveau | Sens | Exemple de preuve |
|---|---|---|
| Déclarée | Promesse marketing ou clause générique | Le mot « portable » sur une page |
| Documentée | Procédure, formats, interfaces d'export décrits | Cahier des charges, spécification |
| Interopérabilité vérifiée | Même charge testée sur au moins deux environnements | Journal de test, critères satisfaits |
| Migration réussie | Bascule ou double exécution mesurée | Durée, coût, écarts fonctionnels |

Une obligation juridique peut renforcer la documentation et réduire certains frais de changement. Elle ne constitue **pas**, à elle seule, une migration testée. Pour parler de capacité, ce livre exige au moins le troisième niveau, et, pour une charge critique, le quatrième.

## 9.2 Pourquoi pouvoir partir n'est pas pouvoir migrer

La possibilité contractuelle de résilier ouvre une porte juridique. Elle ne reconstruit pas une application.

Les interfaces de programmation (*API*) propriétaires fixent souvent des appels sans équivalent exact ailleurs. Les services managés, files d'attente, bases avec extensions spécifiques, fonctions liées à un écosystème, accélèrent le développement initial et alourdissent la réécriture. Les formats d'export incomplets permettent parfois de récupérer des fichiers sans récupérer le schéma, les métadonnées ou les droits. Les compétences peuvent être étroitement liées à une console : même avec un droit de sortie, l'équipe peut manquer du savoir-faire pour reconstruire ailleurs.

Le coût d'export des données, l'*egress*, n'est qu'une composante. S'y ajoutent la réécriture, les tests, la coexistence des deux environnements, l'indisponibilité éventuelle, et le temps des équipes. L'egress d'exploitation récurrent du chapitre précédent n'est pas le même objet que le transfert ponctuel de sortie.

## 9.3 Ce que documentent les analyses de concurrence

Selon le rapport de l'OCDE déjà mobilisé pour les mécanismes de dépendance, le secteur attire l'attention notamment pour des barrières au changement, migration, interopérabilité, et des pratiques telles que des frais élevés de transfert des données hors cloud.[1]

Ces barrières ne prouvent pas que *chaque* charge européenne est captive. Elles montrent pourquoi la réversibilité mérite d'être traitée comme capacité. Un indice britannique relie également des frais de sortie élevés à des freins au multi-cloud ; son périmètre est le Royaume-Uni, non une statistique de l'Union.[2] Aucun chiffre moyen européen de coût de migration n'a été trouvé pour ce chapitre ; aucun n'est inventé.

## 9.4 Ce que le Data Act change : et ce qu'il ne garantit pas

Le règlement (UE) 2023/2854, le *Data Act*, prévoit, au chapitre VI, des obligations visant à faciliter le changement de fournisseur de services de traitement de données.[3]

Ces dispositions modifient le paysage contractuel et tarifaire du changement. Sous-estimer le droit serait aussi trompeur que de le surestimer.

Limite critique : l'interdiction des frais de *switching* **n'élimine pas** automatique-

[1] OCDE, « Competition in the provision of cloud computing services », OECD Roundtables on Competition Policy Papers No. 323, 20 mai 2025, DOI 10.1787/595859c5-en.

[2] Ofcom, *Cloud services market study final report* (extrait), 2023.

[3] Règlement (UE) 2023/2854 du Parlement européen et du Conseil (Data Act), Journal officiel de l'Union européenne, CELEX 32023R2854.

| Disposition | Contenu retenu |
|---|---|
| Article 25 | Contrat écrit ; préavis d'initiation au plus de deux mois ; transition en principe au plus de trente jours calendaires (sinon délai alternatif motivé, au plus de sept mois après notification) ; période de récupération des données d'au moins trente jours après la transition |
| Article 29 | Frais de *switching* (y compris frais d'extraction au sens du règlement) réduits du 11 janvier 2024 au 12 janvier 2027 (plafond = coûts directs), puis **interdits** à compter du 12 janvier 2027 |
| Article 31 | Exceptions : services fortement personnalisés hors catalogue commercial ; versions non productives de test ou d'évaluation à durée limitée |
| Article 50 | Application générale à partir du 12 septembre 2025 |

ment tous les coûts de migration, réécriture, double exécution, personnel, tests, dette liée aux plateformes managées, indisponibilité. Conformité documentaire n'est pas réversibilité technique testée.

## 9.5 Mécanisme : une sortie qui échoue « en droit »

Reprenons un enchaînement plausible, **scénario illustratif**, non un cas observé. Une organisation dispose d'une clause de résiliation et d'un régime de frais de *switching* plus favorable. Elle exporte les données. Les fichiers arrivent. Mais l'application dépend d'une file d'attente propriétaire, d'une identité cloud-spécifique et d'extensions non standard. La réécriture prend des mois. Les deux environnements coexistent. Les tests révèlent des écarts. La bascule est reportée. Le coût dépasse largement les frais d'extraction.

Le droit ouvre la porte ; l'architecture, les formats et les compétences décident si l'on peut franchir le seuil.

| Indicateur | Comment le mesurer | Limite d'interprétation |
|---|---|---|

## 9.6 Grille d'évaluation mesurable

| Indicateur | Comment le mesurer | Limite d'interprétation |
|---|---|---|
| Délai de migration | Temps entre décision de sortie et bascule validée | Dépend du périmètre et de la charge |
| Coût direct | Budget projet, transfert, outils, prestataires | Exclut souvent le coût d'opportunité |
| Temps d'indisponibilité | Fenêtre d'interruption mesurée | Peut être masqué par un double run |
| Effort de réécriture | Jours-personnes sur services non portables | Subjectif sans journal de travail |
| Dépendances non substituables | Inventaire des services sans équivalent testé | Inventaire souvent incomplet |
| Capacité d'export des données | Formats, exhaustivité, délais d'extraction | Export ≠ reconstruction du service |
| Couverture des tests | Scénarios critiques rejoués après migration | Couverture ≠ absence de défauts |
| Compétences requises | Profils réellement mobilisés | Rarement documenté |
| Fonctionnement après migration | Objectifs de service atteints sur N jours | Horizon trop court trompeur |

Aucun score composite n'est produit. Mieux vaut neuf mesures partielles et datées qu'un classement cosmétique.

## 9.7 Checklist : préparer un test de sortie crédible

Avant de parler de réversibilité testée, une organisation peut enchaîner, concrètement :

1. **Inventorier** les services, données et compétences réellement utilisés (pas seulement ceux du contrat).

2. **Choisir** une charge représentative mais bornée, assez critique pour être instructive, assez petite pour être testable.

3. **Documenter** les formats d'export, les dépendances non substituables et les critères de réussite *avant* le test.

4. **Préparer** un environnement cible minimal et les droits d'accès nécessaires.

5. **Exécuter** l'export, le redéploiement et les scénarios de test en journalisant durée, écarts et incidents.

6. **Mesurer** l'indisponibilité éventuelle et le coût direct du test (sans double-compter l'egress d'exploitation).

7. **Décider** explicitement si le niveau atteint est « interopérabilité vérifiée », « migration réussie », ou seulement « documenté ».

Cette checklist n'est pas un résultat d'essai. Elle transforme une intention en procédure.

## 9.8 Protocole conteneurisé : proposé, non exécuté

La documentation de Kubernetes décrit une plateforme portable pour des charges conteneurisées.[4] Un protocole de test a été formalisé dans le cadre de cet ouvrage (charge minimale, manifests standards, critères de réussite, journal horodaté).

**Il n'a pas été exécuté.** Aucun cluster n'a été déployé pour ce livre. Aucun journal d'essai n'existe. L'interopérabilité vérifiée et la migration réussie ne sont donc **pas atteintes** ici. Kubernetes peut faciliter certains déplacements ; il ne rend pas toutes les architectures portables. Le chapitre suivant situe cette ouverture logicielle dans une chaîne plus large, sans rejouer le protocole.

## 9.9 Ce que le lecteur peut retenir

La réversibilité est une **capacité testable**, non un slogan. Le Data Act peut faciliter certains aspects du changement de fournisseur ; il ne remplace pas l'essai et ne supprime pas tous les coûts de migration. Tester a un coût : c'est une assurance mesurable. Une organisation peut choisir de ne pas la payer ; elle ne peut pas alors prétendre disposer d'une capacité démontrée.

Sans réversibilité testée, on peut accumuler des capacités juridiques et tarifaires sans réduire la criticité des dépendances. Pouvoir sortir n'oblige pas à sortir. Rester sans savoir sortir, en revanche, est une dépendance critique potentielle.

Dans quelles conditions les logiciels libres, les standards ouverts et les interfaces compatibles réduisent-ils réellement ces frictions, et où cette contribution s'arrête-t-elle ? C'est l'objet du chapitre suivant.



[4] Kubernetes / CNCF, documentation, Concepts Overview, kubernetes.io.

PARTIE IV

# Technologies, industrie et résilience



CHAPITRE 10

# Logiciels libres, standards et interopérabilité

Ouvrir le code, publier un standard, adopter un orchestrateur « portable » : trois gestes souvent présentés comme des preuves de souveraineté. Ils peuvent réduire certaines dépendances. Ils peuvent aussi déplacer le problème, vers un intégrateur, un nuage sous-jacent, un mainteneur unique, ou une spécification jamais mise à l'épreuve.

Le chapitre précédent a distingué portabilité déclarée et migration testée, et a formalisé un protocole conteneurisé **non exécuté**. Celui-ci n'y revient que pour situer l'ouverture logicielle dans la même discipline de preuve. Il examine ce que les logiciels libres, les standards ouverts et les interfaces compatibles **peuvent** apporter, et ce qu'ils ne prouvent pas. Il refuse de traiter « open source », « ouvert », « européen » et « souverain » comme des synonymes.

## 10.1 Définir l'open source sans l'idéaliser

Selon la Open Source Definition de l'Open Source Initiative, l'open source ne se réduit pas à l'accès au code : la distribution doit respecter un ensemble de critères, redistribution, code source, œuvres dérivées, non-discrimination, licence technologiquement neutre, entre autres.[1]

Cette définition empêche de compter comme « open source » n'importe quel code consultable sous conditions restrictives. Distinguer **code source accessible** et **licence réellement libre** (au sens de la définition) est le premier geste analytique. Elle n'implique pas, à elle seule, qu'une organisation sache maintenir, sécuriser et opérer le logiciel au rythme des incidents.

## 10.2 Six distinctions qui évitent le slogan

| Notion | Sens | Piège fréquent |
|---|---|---|
| Licence conforme à la définition | Droits de distribution et d'usage selon les critères OSI | Confondre avec la gratuité |
| Disponibilité du code | Code lisible et récupérable | Sans capacité de maintenance |
| Standard ouvert | Spécification documentée, accessible | Implémentation divergente |

[1] Open Source Initiative, *The Open Source Definition*.

| Notion | Sens | Piège fréquent |
|---|---|---|
| Compatibilité théorique | Interfaces décrites comme compatibles | Non testée |
| Portabilité d'un composant | Un module se déplace | Le système complet reste captif |
| Ouverture technique | Outils et formats accessibles | Sans maîtrise opérationnelle |

Licence ouverte, disponibilité du code ou adoption d'un standard **ne suffisent pas**, isolément, à établir l'absence de dépendance critique ni un degré de souveraineté.[2]

Réduire une dépendance n'est pas la faire disparaître. Compatibilité théorique n'est pas compatibilité testée.

## 10.3 Bénéfices conditionnels

Les standards ouverts, les formats documentés, les interfaces stables, les outils d'automatisation et les logiciels libres peuvent faciliter l'inspection et l'audit, élargir le vivier de compétences hors d'une console propriétaire, réduire certains coûts de réécriture lorsque l'implémentation est réellement compatible, et permettre des tests d'interopérabilité reproductibles, *si* l'organisation résiste aux extensions propriétaires.

Chacun de ces bénéfices dépend de l'architecture, de la gouvernance, des compétences et des tests réellement exécutés. Un format documenté que personne ne sait reconstruire ailleurs n'allège pas la sortie.

## 10.4 Limites et coûts souvent oubliés

L'ouverture a un prix. Intégration, maintenance, réponse aux vulnérabilités, formation des opérateurs et divergences d'implémentation peuvent dépasser le coût d'une licence propriétaire sur un horizon donné. Ce constat n'est pas un argument contre l'open source ; c'est un argument pour le traiter dans le TCO, plutôt que comme une économie automatique.

L'interopérabilité à grande échelle est difficile à tester : ce qui fonctionne pour un service de démonstration peut échouer pour un système métier avec état, conformité et objectifs de service stricts. Deux implémentations d'un même standard peuvent diverger sur des détails qui bloquent une migration réelle. Sans journal d'essai, le standard reste une ressource potentielle.

[2] Cadre analytique de l'ouvrage *La souveraineté du cloud européen* (limites de l'open source et des standards).

## 10.5 Exemple hypothétique : socle ouvert, dépendance propriétaire

Imaginez, **scénario explicitement hypothétique**, non un cas observé, une application déployée sur un orchestrateur dont le cœur est open source et documenté. Les manifests de base sont standards. Mais, au fil des sprints, l'équipe ajoute : un équilibreur de charge lié au fournisseur cloud ; une identité de charge de travail propre à ce cloud ; une classe de stockage sans équivalent testé ailleurs ; et un registre d'images privé authentifié uniquement dans cet écosystème.

Le socle reste « ouvert ». Le *système* devient difficile à déplacer. L'ouverture du composant central n'a pas disparu ; elle a été contournée par des extensions. Réduire la dépendance au runtime n'a pas fait disparaître les dépendances d'identité, de réseau et de stockage. Ce mécanisme explique pourquoi l'audit de licence et l'audit de sortie ne se confondent pas.

## 10.6 Rhétorique institutionnelle, preuves bornées

Une page institutionnelle de la stratégie open source de l'Union présente l'open source comme un outil de « souveraineté technologique ».[3] Des chiffres promotionnels y figurent **sans méthodologie affichée** : ils ne sont pas repris ici comme faits établis. Le document de stratégie 2020–2023 n'a pas pu être téléchargé lors de l'examen des sources ; aucune pagination inventée n'en est tirée.

Intention politique et résultat industriel restent séparés. Ce livre évalue des capacités, non des communiqués.

## 10.7 Lien avec les barrières au changement

Les analyses de concurrence relient déjà les limites d'interopérabilité et de standardisation aux barrières au changement de fournisseur.[4] Il est plausible, mais **non mesuré** ici, qu'améliorer standards et interfaces réduise certains coûts de sortie. L'effet net dépend de l'implémentation, des compétences et des tests de réversibilité décrits au chapitre précédent.

[3] Commission européenne, page factuelle « EU Open Source Strategy », Shaping Europe's digital future.

[4] OCDE, « Competition in the provision of cloud computing services », OECD Roundtables on Competition Policy Papers No. 323, 20 mai 2025, DOI 10.1787/595859c5-en.

## 10.8 De l'ouverture à la capacité : en quatre étapes

Premièrement, un standard ou une licence libre crée une *possibilité* technique. Deuxièmement, une implémentation concrète crée une *disponibilité*. Troisièmement, un test d'interopérabilité crée une *preuve partielle*. Quatrièmement, une migration réussie, avec compétences et exploitation, crée une *capacité*.

Sauter de la première étape à la dernière est le raccourci le plus fréquent du débat sur la souveraineté logicielle. Pour un cas conteneurisé, le chapitre 9 a déjà établi que la propriété annoncée n'équivaut pas à une migration démontrée : le protocole associé reste non exécuté. Ici, l'enjeu est plus large : l'ouverture est un levier, pas une garantie.

La documentation de Kubernetes illustre la même discipline sans la redétailler : portabilité annoncée d'une plateforme d'orchestration de conteneurs, distincte d'une plateforme applicative monolithique ; pas d'interopérabilité ni de migration mesurées dans cet ouvrage.[5]

## 10.9 Objections

« Tout open source » réduirait la dépendance : la dépendance peut se déplacer vers des intégrateurs, le cloud sous-jacent ou les mainteneurs. Le standard suffirait : sans test, le texte ne porte pas la charge. L'open source serait à faible coût : intégration et maintenance relèvent du TCO. Sur certains horizons, un service propriétaire peut rester moins coûteux en TCO, ce qui n'en fait pas une solution « souveraine ».

## 10.10 Vers la matière industrielle

Les logiciels libres et les standards sont des **leviers de capacités technologiques**. Ils peuvent soutenir la réduction de dépendances critiques lorsqu'ils sont combinés à des compétences, des tests et une base industrielle. Les présenter comme garanties de souveraineté transforme une capacité facilitatrice en slogan. Les ignorer parce qu'ils ne suffisent pas serait l'erreur symétrique.

La matière industrielle, data centers, composants, énergie, conditionne ensuite ce que ces leviers logiciels peuvent réellement soutenir. Sans capacités physiques et industrielles, l'ouverture logicielle reste une condition nécessaire partielle, non une stratégie complète. C'est l'objet du chapitre suivant.



[5] Kubernetes / CNCF, documentation, Concepts Overview, kubernetes.io.

CHAPITRE 11

# Data centers, semi-conducteurs, énergie et chaînes d'approvisionnement

Un bâtiment climatisé, des baies de serveurs, une ligne électrique haute capacité : l'image du data center rassure. Elle donne l'impression que la souveraineté cloud se voit depuis la rue. Or des mégawatts peuvent héberger des services dont la pile logicielle, les composants, la maintenance et les décisions d'incident restent hors de portée. À l'inverse, prétendre qu'aucune politique cloud n'a de sens sans autonomie totale sur les semi-conducteurs transforme un goulet réel en prétexte d'immobilisme.

Entre ces deux excès, ce chapitre pose une question industrielle : **quelles capacités matérielles et énergétiques conditionnent**, sans la garantir, une réduction des dépendances critiques ? Les logiciels libres et les standards, traités au chapitre précédent, ne remplacent pas une base physique. Ici, quatre sous-ensembles liés, calcul hébergé, composants, énergie et réseaux, chaînes d'approvisionnement, puis une grille qui sépare ce que l'on localise, ce que l'on possède, ce que l'on contrôle et ce que l'on maîtrise réellement.

Aucune statistique industrielle européenne homogène de propriété ultime n'est inventée. L'affirmation industrielle centrale du chapitre demeure une hypothèse de travail.

## 11.1 Capacité installée, capacité disponible

La capacité physique de calcul et d'hébergement constitue une base matérielle des services cloud. Sans sites, sans puissance électrique disponible, sans connectivité, il n'y a pas d'offre cloud à échelle. Une étude commandée pour la préparation du *Cloud and AI Development Act* estime, pour 2025, une capacité de centres de données de l'ordre de 12,4 GW dans l'UE-27, avec une forte concentration dans quelques États membres. Allemagne, France, Pays-Bas et Irlande représenteraient, selon cette modélisation, environ 63 % du total.[1]

Ces chiffres méritent d'être lus avec sobriété. Ils décrivent une **capacité**, souvent modélisée, parfois croisée avec des enquêtes. Ils ne disent pas qui détient les sites, qui opère les hyperviseurs, qui contrôle les accès privilégiés, ni si les services hébergés pourraient être reconstruits ailleurs. Un gigawatt localisé en Europe peut servir une pile non européenne. Une capacité plus modeste, mieux maîtrisée opéra-

[1] Cloud & AI Study, Office des publications de l'UE, 2026, DOI 10.2759/9828163, capacité modélisée / enquête CATI ; ≠ propriété ultime des opérateurs.

tionnellement, peut réduire certaines dépendances critiques sans égaler la taille des hyperscalers.

Il faut aussi distinguer capacité **installée** et capacité **effectivement disponible**. Une baie pleine, une ligne électrique saturée, un permis non obtenu ou une contrainte de refroidissement peuvent rendre inutilisable une part de ce qui figure sur une carte de puissance. La concentration géographique ajoute une autre nuance : si une part importante de la capacité se situe dans un petit nombre d'États membres, les politiques nationales d'énergie, d'urbanisme et de fiscalité pèsent sur l'offre européenne autant que les discours industriels pan-européens.

## 11.2 Localisation, propriété, contrôle ultime, exploitation

Une étude externe du BEREC distingue cinq grandes catégories de modèles d'ownership et d'affaires : colocation indépendante (*carrier-neutral*) ; sites appartenant à des hyperscalers ; initiatives publiques ou partenariats public-privé ; centres détenus par des opérateurs de télécommunications ; modèles hybrides ou émergents.[2]

Cette typologie empêche de traiter « data center européen » comme une catégorie unique. Un site de colocation peut héberger des clients aux nationalités et aux piles très diverses. Un site d'hyperscaler peut être situé en Europe tout en relevant d'une chaîne de décision mondialisée. Un partenariat public-privé peut combiner financement public et exploitation privée. Un opérateur télécoms peut posséder le bâtiment et sous-traiter une partie de la couche cloud.

Quatre questions se séparent alors :

1. **Où** sont les machines et les données ? (localisation)
2. **Qui possède** les actifs et les contrats ? (propriété)
3. **Qui est le bénéficiaire ultime** des droits de contrôle économique ? (propriété ultime)
4. **Qui configure, supervise et décide** en incident ? (maîtrise d'exploitation)

Localisation et propriété ne coïncident pas. Propriété et bénéficiaire ultime non plus : un siège social européen peut masquer une chaîne de contrôle hors Union, et l'inverse. Contrôle juridique et maîtrise opérationnelle divergent encore : un contrat peut attribuer des droits sans que les équipes sachent les exercer sous contrainte. Aucune série européenne homogène de propriété ultime des opérateurs n'a été identifiée dans le corpus actuel. Aucun pourcentage européen de « propriété » ou de « maîtrise » n'est donc fabriqué ici. Cette absence n'est pas un détail de note : c'est une lacune structurante pour quiconque voudrait transformer la carte des mégawatts en carte de souveraineté. Une statistique industrielle homogène de propriété ultime

[2] BEREC, External Study on Data Centres, BoR (26) 01, 2026 : typologie ; pas de série UE de bénéficiaires effectifs.

reste à constituer ; elle n'a pas été inventée.

## 11.3 Semi-conducteurs : goulet amont du cloud

L'accès aux puces et composants critiques contraint ce que l'on peut produire, faire évoluer ou sécuriser. Sans composants, pas de serveurs. Sans capacité de fabrication ou d'approvisionnement crédible, les annonces d'autonomie cloud rencontrent vite la réalité des délais, des nœuds technologiques et des chaînes mondiales.

Le *Chips Act* fixe un cadre politique pour renforcer l'écosystème européen des semi-conducteurs.[3] Des rapports du JRC et de la Cour des comptes européenne documentent des parts de fabrication ou de capacité mondiale de l'ordre de quelques pourcents, avec des définitions qui **ne se superposent pas**. Production, capacité installée, objectifs de la Digital Decade : ces grandeurs ne se fusionnent pas. Les ordres de grandeur souvent cités, autour de 7 %, 9 % ou 11,7 % selon les définitions, doivent rester attachés à leurs sources et à leurs méthodes.[4]

Ces chiffres contextualisent une dépendance industrielle. Ils ne mesurent pas la souveraineté cloud. Une Europe plus capable en semi-conducteurs pourrait réduire certains risques d'approvisionnement pour les infrastructures numériques. Elle ne transformerait pas automatiquement chaque contrat cloud en maîtrise opérationnelle, ni chaque localisation en réversibilité. Symétriquement, l'impossibilité d'une autarcie totale sur les nœuds les plus avancés n'interdit pas de cartographier les goulets et de diversifier les approvisionnements.

Le lien avec le cloud est mécanique : la disponibilité des serveurs, des accélérateurs et des équipements de réseau dépend de chaînes qui dépassent le fournisseur cloud. Une politique cloud qui ignore ce goulet traite le bâtiment comme s'il se suffisait à lui-même.

## 11.4 Énergie, raccordement et réseaux

Sans énergie et sans connectivité, pas de capacité cloud durable. Les data centers sont des consommateurs électriques majeurs et croissants. Eurostat publie des séries nationales de consommation électrique des centres de données ; leur agrégation UE n'est pas homogène.[5] Une estimation JRC situe la consommation des centres de données de l'UE-27 entre 45 et 65 TWh en 2022.[6] Le rapport COM(2026) 500 cite, pour 2024, une valeur de 68 TWh en renvoyant à l'AIE. Ce n'est pas une somme

[3] Règlement (UE) 2023/1781 (Chips Act).

[4] JRC, Semiconductors in the EU (JRC133850), 2023 ; Cour des comptes européenne, Special report 12/2025. Ne pas fusionner 7 %, 9 % et 11,7 % sans préciser les définitions.

[5] Eurostat, isoc_env_ict_nrg.

[6] Kamiya & Bertoldi (JRC), 2024.

vérifiée des cellules Eurostat, et elle n'est **pas fusionnable** mécaniquement avec la fourchette JRC.[7]

L'énergie est une condition, non l'ensemble du problème de souveraineté. Une région électrique contrainte, file d'attente de raccordement, pic de demande, acceptabilité locale, peut limiter l'expansion de capacité même si la demande cloud croît. Une capacité abondante alimentée sans maîtrise des piles logicielles ne produit pas davantage de souveraineté. Les réseaux complètent le tableau : un data center isolé, mal interconnecté, ne soutient pas les mêmes services qu'un nœud situé près des points d'échange et des routes internationales.

## 11.5 Chaînes d'approvisionnement : résilience sans autarcie

Chocs géopolitiques, ruptures logistiques, délais de livraison, dépendance à des équipements de réseau ou à des pièces de rechange : la résilience d'une *supply chain* limite les points de défaillance uniques. Résilience n'est pas autarcie. Une Europe qui diversifie fournisseurs et stocks stratégiques ne devient pas indépendante de toute chaîne mondiale. Elle réduit certains risques de rupture.

Une carte quantitative unifiée de la chaîne cloud européenne, du wafer au rack, du firmware à la maintenance, reste à documenter. Elle ne sera pas remplacée par des valeurs illustratives non étiquetées. Tant que cette carte manque, le chapitre peut formuler des mécanismes et des distinctions ; il ne peut pas prétendre mesurer le degré de résilience industrielle de l'offre cloud européenne.

## 11.6 Grille : localiser n'est pas contrôler

| Dimension | Question | Confusion fréquente |
|---|---|---|
| Localisation | Où sont les machines et les données ? | Local = souverain |
| Propriété | Qui possède les actifs et les contrats ? | Propriété locale = indépendance technique |
| Contrôle ultime | Qui détient le pouvoir économique effectif ? | Siège social = bénéficiaire ultime |
| Exploitation | Qui configure, supervise, décide en incident ? | Conformité = maîtrise opérationnelle |
| Indépendance fournisseurs | Peut-on substituer composants et services critiques ? | Un second fournisseur suffit toujours |

Ces questions ne se répondent pas par un seul indicateur. Un site localisé peut être propriété d'un acteur non européen. Une propriété locale peut coexister avec

[7] Commission européenne, COM(2026) 500 final, citation IEA en note ; ne pas fusionner avec JRC.

une dépendance logicielle non substituable. Un contrôle documentaire peut masquer une incapacité opérationnelle. Une double source d'approvisionnement peut rester insuffisante si les deux sources partagent le même goulet amont.

Dans le cadre analytique de cet ouvrage, la base industrielle européenne, data centers, composants, énergie, *supply*, **contraint** le degré de réduction des dépendances cloud, sans la confondre avec la localisation seule ni avec une autarcie technologique.[8] Cette proposition reste une **hypothèse de travail**. Les sources contextuelles ne remplacent pas un inventaire de capacités et de propriété ultime.

## 11.7 Objections

On objecte que des data centers locaux « suffisent ». Seulement s'ils s'accompagnent de contrôle opérationnel, de substitutabilité logicielle et de compétences, ce que la localisation n'apporte pas automatiquement. On objecte que l'autonomie sur les puces est impossible à moyen terme : l'objection peut être juste pour une autarcie totale ; elle n'interdit pas de cartographier les goulets. On objecte que les contraintes énergétiques rendent l'expansion indésirable : cela renforce l'idée que la capacité cloud n'est pas un bien gratuit.

Une objection plus subtile affirme que la propriété ultime n'importe pas si les contrats et les certifications sont robustes. Le chapitre suivant montre pourquoi contrats et certifications ne mesurent pas, à eux seuls, la capacité d'agir sous incident. Ici, l'absence d'inventaire européen de bénéficiaires effectifs empêche de trancher empiriquement cette objection à l'échelle de l'Union.

## 11.8 Pont vers l'exploitation

Sans base industrielle lisible, l'autonomie cloud reste contrainte. Localisation, propriété, contrôle ultime et maîtrise d'exploitation ne coïncident pas. Le corpus fournit des contextes énergétiques, semi-conducteurs et typologiques ; l'inventaire de propriété ultime et de contrôle mesuré reste ouvert.

La matière ne suffit pas : sans maîtrise opérationnelle et sans résilience face aux incidents, le cadre juridique et les mégawatts restent creux. C'est l'objet du chapitre suivant.



[8] Cadre analytique de l'ouvrage (capacités industrielles), proposition de travail, preuves industrielles encore partielles.

CHAPITRE 12

# Cybersécurité, résilience et maîtrise opérationnelle

Une clause de localisation peut rassurer un acheteur. Elle ne dit pas qui détient les clés d'administration, qui répond à trois heures du matin, ni si un accès extraterritorial peut être exigé. Sans contrôle opérationnel et sans résilience, le cadre juridique risque de rester une enveloppe vide, élégante sur le papier, inerte sous contrainte.

Le chapitre précédent a rappelé que la matière, data centers, puces, énergie, conditionne sans garantir. Celui-ci porte sur la **capacité d'agir**. Des sources institutionnelles contextualisent le débat. Elles ne mesurent pas une maîtrise opérationnelle européenne agrégée. Aucun cas d'incident sensible n'est inventé. Aucun classement de sécurité des fournisseurs n'est établi.

## 12.1 Huit questions concrètes

Avant les labels, les questions :

1. Qui peut **administrer** les systèmes, et avec quels droits ?
2. Qui détient les **accès privilégiés**, et comment sont-ils journalisés ?
3. Qui peut **intervenir** en cas d'incident, dans quel délai, depuis où ?
4. Qui contrôle les **journaux** et les outils de supervision ?
5. Qui peut **restaurer** données et services, et a-t-on testé cette restauration ?
6. Qui maîtrise les **procédures de crise**, isolations, bascules, communications ?
7. Quelles **dépendances** subsistent envers fournisseurs et sous-traitants ?
8. Comment **démontrer** ces capacités, tests, journaux, exercices, au lieu de les déclarer ?

Ces questions distinguent quatre couches souvent confondues : la **conformité réglementaire**, les **engagements contractuels**, les **dispositifs documentés** et les **capacités effectivement testées**. Une organisation peut exceller sur les deux premières et échouer sur la quatrième.

## 12.2 Ce que désigne le contrôle opérationnel

Configurer, superviser, gérer les identités, répondre aux incidents, décider d'une isolation ou d'une bascule : voilà le cœur du contrôle opérationnel. Il se distingue de la conformité documentaire et de la seule présence de serveurs sur un territoire. Un audit réussi peut coexister avec une équipe incapable de reconstruire un service critique. Une certification peut attester d'un processus sans garantir sa mobilisation sous stress.[1]

Le modèle de **responsabilité partagée** entre client et fournisseur redistribue ces tâches selon le service, infrastructure, plateforme ou logiciel, sans abolir la question : *qui peut réellement faire quoi ?* En IaaS, le client conserve une large part des systèmes et des applications. En PaaS, la plateforme échappe davantage à sa main. En SaaS, l'essentiel de l'exploitation est délégué. Monter dans la pile n'élimine pas le besoin de contrôle ; il en change la nature.

La figure associée illustre ces frontières. Elle est un **modèle pédagogique**, non un contrat universel, ni une statistique d'incidents.

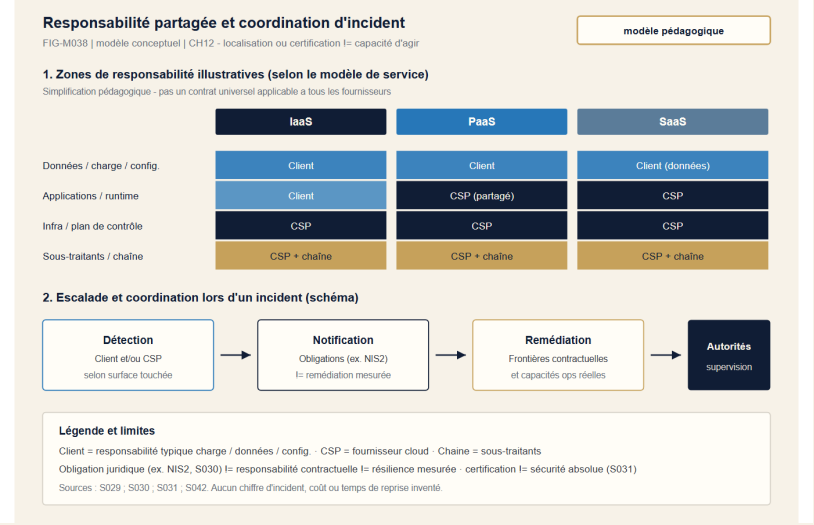



**Fig. 12.1 :** Responsabilité partagée et coordination d'incident (modèle pédagogique, non empirique).

Le schéma ne prouve pas une indépendance opérationnelle. Il montre pourquoi confondre responsabilité contractuelle et capacité d'agir est une erreur.

[1] ENISA / CSA, limites de la certification.

## 12.3 Localisation n'est pas contrôle

Localiser des données ou des machines peut être nécessaire pour certaines exigences légitimes : proximité, juridiction, latence, politiques sectorielles. Cela ne garantit ni la maîtrise des accès privilégiés, ni l'indépendance des outils de supervision, ni l'absence de dépendances logicielles non substituables. L'argument « local donc sûr » est une confusion, non une démonstration.

Un cadre d'acheteur institutionnel peut exiger des niveaux de « souveraineté » déclarés. Cela ne prouve pas, à soi seul, une capacité d'agir mesurée.[2] Le cadre de cet ouvrage et les outils d'acheteur ne doivent pas être fusionnés. L'un propose une grille analytique. L'autre structure une procédure d'achat.

## 12.4 Résilience : absorber sans prétendre à l'autarcie

La résilience désigne ici la capacité à absorber chocs et défaillances sans rupture inacceptable, panne majeure, rupture d'approvisionnement, incident de sécurité, indisponibilité prolongée. Elle n'exige pas l'absence totale de dépendance. Elle exige de savoir ce qui casse, combien de temps on tient, et quelles alternatives existent réellement.

Les rapports de menaces et les obligations de notification structurent le paysage réglementaire. Pour certaines entités cloud et centres de données, la directive NIS2 introduit des obligations de cybersécurité et de signalement.[3] Une obligation de notifier n'est pas une mesure de résilience observée. Des indicateurs de continuité comparables entre acteurs, temps de rétablissement, couverture d'astreinte, substitutabilité des outils de supervision, manquent encore dans le corpus. Ils ne seront pas inventés. Aucun classement homogène de « maîtrise opérationnelle » des fournisseurs n'est donc publié ici.

La résilience croise aussi la *supply chain* du chapitre précédent. Un incident n'est pas seulement un logiciel malveillant. Ce peut être l'indisponibilité d'un composant, d'un firmware, d'un prestataire de maintenance ou d'une région cloud entière.

[2] Cloud Sovereignty Framework, outil d'acheteur Commission ; distinct du cadre de mesure de cet ouvrage.

[3] ENISA Threat Landscape ; directive NIS2, obligations ≠ résilience mesurée.

## 12.5 Extraterritorialité des accès : question ouverte

Les régimes d'accès par des autorités étrangères aux données ou aux infrastructures situées en Europe constituent un enjeu souvent cité. Des lignes directrices anciennes pour les institutions de l'Union rappellent des responsabilités d'acheteur ; leur périmètre est étroit et daté.[4]

La question relève du droit, des modèles opérationnels et des architectures d'accès privilégié. Elle ne se tranche pas par une anecdote. Elle ne disparaît pas non plus parce qu'un site est situé dans l'Union.

## 12.6 Hypothèse de travail

Dans le cadre analytique de cet ouvrage, **sans maîtrise opérationnelle et sans résilience**, un cadre juridique ou une localisation ne produit pas, à lui seul, une capacité d'agir face aux dépendances cloud critiques.[5]

Cette proposition est une **hypothèse de travail**. Les sources contextuelles ne remplacent pas une comparaison d'incidents ni une mesure de maîtrise opérationnelle.

## 12.7 Objections

On objecte que les grands fournisseurs mondiaux sont « plus sûrs » que des alternatives locales. C'est possible pour certains périmètres, redondance mondiale, budgets de sécurité, maturité des processus. Ce n'est pas une preuve que la dépendance associée est acceptable, ni que la sortie reste possible. Sécurité relative et criticité de dépendance sont deux questions distinctes.

On objecte que la sécurité relève surtout de normes et d'audits. Utile, cette objectivation ne remplace pas la pratique d'incident. On objecte que les incidents sensibles sont peu documentés publiquement : précisément pourquoi ce chapitre refuse les exemples inventés.

Une objection inverse affirme que la maîtrise opérationnelle locale suffit toujours. Or une équipe locale peut dépendre d'outils propriétaires, de support extraterritorial ou de compétences rares. Maîtrise déclarée et maîtrise exercée sous contrainte ne se confondent pas.

[4] EDPS, guidelines cloud pour institutions UE, 2018 : ne pas généraliser à toutes les administrations.

[5] Cadre analytique de l'ouvrage, proposition de travail sur maîtrise opérationnelle et résilience ; preuves agrégées encore absentes.

## 12.8 De l'agir à l'offre

Cybersécurité et résilience modifient le degré de souveraineté cloud en tant que **capacités d'action**, non comme labels. Localisation ≠ contrôle. Certification ≠ capacité d'agir. Obligation de notification ≠ résilience mesurée. Le corpus institutionnel contextualise ; la maîtrise opérationnelle mesurée reste ouverte.

Reste le passage de la capacité technique à l'**offre viable** : recherche, financement, startups et industrialisation, sans quoi les alternatives restent des laboratoires. C'est l'objet du chapitre suivant.

---



PARTIE V

# Recherche, marchés et concurrence



CHAPITRE 13

# Recherche, financement, startups et industrialisation

Une publication ne fait pas un produit. Un prototype ne fait pas une alternative cloud viable. Entre le laboratoire et un fournisseur capable de durer s'étendent des goulets, capital, industrialisation, demande, compétences d'exploitation, souvent confondus dans les discours de « souveraineté ». Compter des articles, des démonstrateurs ou des enveloppes budgétaires comme s'ils mesuraient déjà une offre cloud industrialisée est l'une des confusions les plus coûteuses du débat.

Les chapitres sur l'école et le supérieur ont amorcé la recherche et le transfert. Celui-ci change d'échelle : il regarde l'**offre**, comment une capacité technique devient, ou non, une alternative économique crédible. Aucune success-story inventée. Aucun taux de conversion startup→échelle fabriqué.

## 13.1 Sept étapes, six ruptures possibles

Pour qu'une capacité scientifique ou technique devienne une capacité industrielle durable, un enchaînement minimal se dessine :

1. **Financement de la recherche**, ressources pour explorer et expérimenter.
2. **Production de connaissances**, publications, brevets, savoir-faire tacite.
3. **Prototypes et démonstrateurs**, preuve de concept bornée.
4. **Transfert technologique**, passage vers une organisation capable de vendre et d'opérer.
5. **Création et croissance d'entreprises**, structure, capital, équipes.
6. **Adoption par les clients**, usage réel, paiement, rétention.
7. **Industrialisation et exploitation à grande échelle**, engagements de disponibilité, support, sécurité, coûts unitaires soutenables.

Entre ces étapes, les ruptures sont fréquentes. Un financement discontinu coupe la recherche avant le prototype. Un prototype brillant meurt faute de product owners ou d'équipes d'exploitation. Une startup obtient du capital sans atteindre les coûts de conformité et de support comparables à ceux des grands fournisseurs. Une adoption initiale s'effondre si le service ne tient pas la charge. Une industrialisation bute sur des composants, des compétences ou des services tiers non substituables, ceux du chapitre 11 et du chapitre 12.

Ces ruptures ne sont pas des anecdotes. Elles expliquent pourquoi un programme public peut être réussi sur ses indicateurs de dépense et échouer sur l'offre cloud

réellement disponible.

## 13.2 Ce que l'on risque de compter trop tôt

| Niveau | Sens | Piège |
|---|---|---|
| Production scientifique | Publications, brevets | Compter comme industrialisation |
| Prototype / démonstrateur | Preuve de concept | Confondre avec un service opéré |
| Startup | Organisation naissante | Ignorer la viabilité |
| Scale-up | Capacité à grandir | Sous-estimer le capital et l'exploitation |
| Fournisseur viable | Alternative durable | Utiliser la part de marché comme souveraineté |

Ces niveaux ne forment pas une échelle automatique. Une économie peut exceller en publications et manquer d'offre managée. Elle peut financer des startups sans qu'elles atteignent l'échelle opérationnelle nécessaire pour concurrencer des piles complètes.

## 13.3 Intention, acte, résultat

Le programme *Digital Europe* fixe des objectifs généraux, dont une autonomie stratégique, et des enveloppes budgétaires par domaines (calcul haute performance, IA, cybersécurité, compétences, déploiement).[1] Lire ce règlement comme une preuve d'industrialisation cloud serait une erreur de catégorie. Un cadre budgétaire autorise des actions. Il ne démontre pas qu'une offre cloud européenne durable existe.

Le *Chips Act* vise l'écosystème des semi-conducteurs. Il est distinct d'une offre cloud managée, même s'il conditionne une partie de la base industrielle évoquée au chapitre 11.[2] Des pages de politique de la Commission annoncent des instruments et des alliances. Une annonce n'est pas un acte adopté, ni un résultat de marché.[3]

Trois cases restent séparées : **intention** (discours, feuille de route), **acte** (règlement, décision, budget engagé), **résultat** (capacité industrialisée, service opéré, adoption soutenue). Passer de la première à la troisième sans preuves intermédiaires produit des récits de souveraineté déjà acquise.

[1] Règlement (UE) 2021/694 (Digital Europe Programme), texte JO examiné. Financement ≠ capacité cloud industrialisée.

[2] Règlement (UE) 2023/1781.

[3] Pages politiques Commission / communications, distinguer intention et résultat.

## 13.4 Capital, compétences et demande

L'accès au financement peut permettre d'industrialiser une offre cloud européenne. Il ne crée pas, à lui seul, un *product-market fit*. Industrialiser, ici, signifie passer d'un démonstrateur à un service capable de tenir des engagements de disponibilité, de support, de sécurité et d'échelle. Cela exige du capital, mais aussi des compétences d'exploitation, celles du chapitre 12, une chaîne de vente, une intégration avec des écosystèmes existants, et une demande solvable.

À l'inverse, une demande publique ou privée sans offre scalable laisse les acheteurs face aux mêmes dépendances. Les deux goulets, capital et demande, doivent rester distincts jusqu'à preuve du contraire. Le chapitre suivant traitera la commande publique. Celui-ci refuse de résoudre le problème de l'offre en le renvoyant uniquement à l'achat.

Le capital n'est pas homogène. Financer un prototype n'est pas financer une plateforme opérée vingt-quatre heures sur vingt-quatre. Financer une startup n'est pas assurer sa capacité à affronter des coûts de conformité comparables à ceux des grands fournisseurs.

## 13.5 Indicateurs observables : sans valeurs inventées

Tant que les taux de transfert, de survie et de passage à l'échelle manquent dans le corpus, on peut au moins **nommer** ce qu'il faudrait observer, sans inventer les chiffres :

| Indicateur candidat | Ce qu'il rendrait visible | Statut dans ce livre |
|---|---|---|
| Part des projets passant du démonstrateur au service opéré | Rupture transfert | Non mesuré ici |
| Délai et coût pour atteindre un engagement de disponibilité contractuel | Industrialisation ops | Non mesuré ici |
| Taux de rétention clients après 12 / 24 mois | Adoption réelle | Non mesuré ici |
| Dépendance à des composants ou services tiers non substituables | Fragilité industrielle | Qualitatif seulement |
| Capacité d'astreinte et de restauration testée | Lien avec CH12 | Non mesuré ici |

Ces indicateurs sont une agenda de mesure, pas un tableau de résultats.

## 13.6 Hypothèse de travail

Dans le cadre analytique de cet ouvrage, l'industrialisation et le financement conditionnent l'existence d'**alternatives cloud viables**, distinctes de la seule production scientifique ou de la seule existence de modules universitaires.[4]

Cette proposition reste une **hypothèse**. Les cadres de financement examinés contextualisent. Ils ne mesurent pas l'industrialisation aboutie d'une offre cloud européenne.

## 13.7 Objections

On objecte que le goulet est la demande, pas le capital. Possible : c'est pourquoi le chapitre suivant traite la commande publique. On objecte que le marché « sélectionne » déjà les meilleures offres : la concentration documentée ailleurs dans le livre rappelle que la sélection n'implique pas la substituabilité. On objecte que l'Europe « innove assez » : innover n'est pas industrialiser à l'échelle des piles managées critiques.

Une objection plus radicale affirme que l'Europe n'a pas vocation à produire des hyperscalers, mais seulement à réguler. Cette position politique existe. Elle n'annule pas la question du livre : si des dépendances sont jugées critiques, quelles capacités permettent de les réduire ? Réguler sans capacités peut encadrer ; cela ne substitue pas.

## 13.8 Vers la demande publique

Sans industrialisation et sans viabilité des fournisseurs, les capacités humaines et logicielles restent en amont. Les programmes européens documentés ne prouvent pas, à eux seuls, une offre cloud durable. Intention ≠ acte ≠ résultat. Publication ≠ produit. Budget ≠ industrialisation.

La demande publique peut-elle créer un débouché crédible sans fermer le marché ni promettre une industrialisation automatique ? C'est la question suivante.



[4] Cadre analytique de l'ouvrage, proposition de travail sur industrialisation et financement ; outcomes non mesurés.

CHAPITRE 14

# Commande publique et politique industrielle

L'État et les collectivités sont souvent les premiers à parler de souveraineté cloud, et parmi les premiers à acheter des services. La commande publique peut structurer une demande, imposer des clauses, créer un débouché. Elle peut aussi engendrer contentieux, fragmentation ou préférence locale sans capacités réelles. Ce chapitre lit ces arbitrages. Il n'est pas un conseil juridique. Il n'est pas non plus une évaluation d'impact industriel pan-européenne : les volumes nationaux et les études d'effet manquent encore.

Le chapitre précédent a situé l'offre et l'industrialisation. Celui-ci regarde un levier de **demande**. Le droit des marchés publics, le *Data Act*, un cadre d'acheteur institutionnel et un marché documenté fournissent un corpus partiel. Ils ne démontrent pas, à eux seuls, qu'une progression de souveraineté a été causée par l'achat public.

## 14.1 Ce que la demande publique peut faire : et ne pas faire

| Levier | Effet plausible | Limite |
|---|---|---|
| Volume d'achat | Débouché pour alternatives | Sans offre viable, volume = dépendance |
| Clauses de réversibilité | Exigence de sortie | Clause ≠ test de migration |
| Critères de localisation | Conformité territoriale | Localisation ≠ contrôle ops |
| Critères de sécurité | Exigences minimales | Audit ≠ capacité d'agir |
| Transparence des dépendances | Visibilité des sous-traitants et piles | Inventaire ≠ substitutabilité |
| Coût total de possession | Lecture trajectoire (voir chapitre 8) | TCO incomplet si paramètres absents |
| Préférence « locale » | Soutien industriel | Risque d'inefficacité / contentieux ; ≠ capacités |

Ces leviers ne sont pas interchangeables. Exiger une réversibilité testable n'est pas la même chose qu'exiger une nationalité de façade. Imposer un volume d'achat à une offre inexistante ne crée pas magiquement un fournisseur viable. Soutenir industriellement par l'achat peut être tentant ; cela peut aussi verrouiller des solutions médiocres ou exposer l'acheteur à des recours.

## 14.2 Objectifs, règles, critères, clauses, exécution, résultats

Six couches se distinguent :

1. **Objectifs politiques**, discours de souveraineté, feuilles de route.
2. **Règles juridiques**, textes en vigueur (directives, règlements).
3. **Critères d'achat**, ce que le cahier des charges exige concrètement.
4. **Clauses contractuelles**, ce que le contrat formalise.
5. **Exécution**, ce qui est réellement livré, testé, contrôlé.
6. **Résultats observés**, effets sur capacités, concurrence, dépendances.

Confondre la couche 1 avec la couche 6 produit des récits de succès non démontrés. Un objectif politique n'est pas un résultat industriel.

## 14.3 Droit en vigueur, projets et rhétorique

Il faut distinguer un texte **en vigueur**, un projet, et une intention politique. La directive 2014/24 fixe des principes de non-discrimination et d'attribution, dont le critère du mieux-disant économiquement (*MEAT*).[1] Elle n'interdit pas toute considération de qualité, de sécurité ou de performance liée à l'objet du marché. Elle n'autorise pas non plus, à elle seule, une préférence nationale généralisée présentée comme souveraineté.

Le règlement sur les données (*Data Act*) impose, dans son champ, des obligations de *switching*. Il ne crée pas à lui seul une offre industrielle.[2] Une obligation juridique de faciliter le changement de fournisseur n'équivaut pas à une migration réussie, ni à une capacité opérationnelle de sortie chez l'acheteur.

Un *Cloud Rulebook* et une guidance générale d'achat sont annoncés sur les pages de politique. Ils n'étaient pas publiés comme actes au moment de l'examen.[3] Annonce ≠ droit applicable.

Un *Cloud Sovereignty Framework* et sa guidance d'implémentation permettent à un acheteur institutionnel de structurer des critères pour une procédure donnée.[4] Ce cadre est une pratique d'acheteur. Il n'est pas le cadre de mesure de cet ouvrage. Un marché documenté des institutions européennes, ordre de grandeur évoqué : environ 180 millions d'euros, illustre une pratique. Il ne se généralise pas à toutes les administrations de l'Union, et un montant contractuel n'est pas un effet industriel mesuré.[5]

La figure distingue ce que le droit **impose**, ce qu'il **autorise**, ce qui est **observé**

[1] Directive 2014/24/UE.

[2] Règlement (UE) 2023/2854 (Data Act), CELEX 32023R2854, détail aussi au chapitre réversibilité.

[3] Page politique Commission « Cloud computing ».

[4] Cloud Sovereignty Framework ; Implementation guidance, faculté / pratique acheteur, pas obligation UE générale.

[5] Documentation marché institutions / Cloud III.

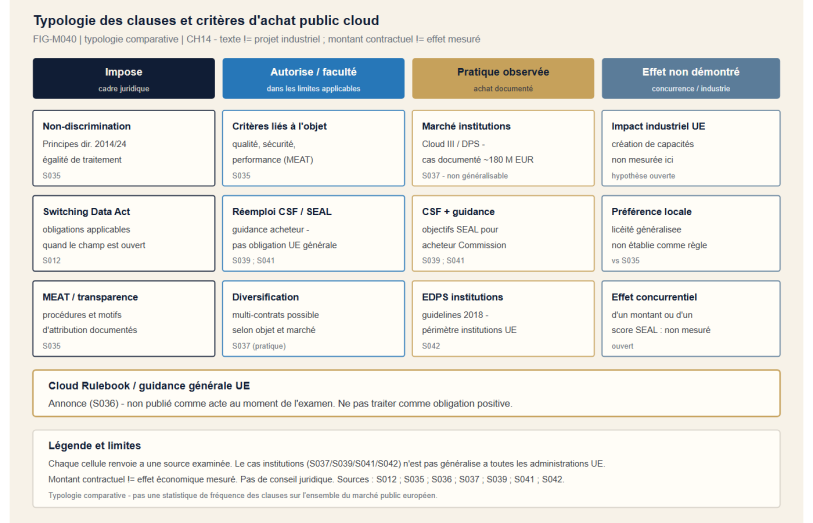



**Fig. 14.1 :** Typologie des clauses et critères d'achat public cloud (cadre analytique ; pratique institutions partiellement documentée).

dans une pratique documentée, et ce dont l'**effet** industriel n'est **pas démontré**. Elle n'est pas un manuel d'achat. Elle est une boussole contre les confusions.

## 14.4 Critères qui peuvent influencer les capacités : à condition d'être vérifiés

Parmi les critères utiles au sens de ce livre, lorsqu'ils sont réellement contrôlés après attribution, figurent :

- l'**interopérabilité** et la **réversibilité** (formats, délais, assistance de sortie, tests exigés) ;
- la **sécurité** et la **continuité** (objectifs de service, exercices de restauration) ;
- la **transparence des dépendances** (sous-traitants, composants critiques, régions) ;
- le **coût total de possession** sur une trajectoire explicite, et non le seul prix catalogue ;
- la **capacité réelle** du fournisseur à répondre, équipes, références opérationnelles, pas seulement des slides.

Sans vérification après attribution, ces critères restent des intentions contractuelles. La commande publique peut exiger ; elle ne fabrique pas, par la seule force du cahier des charges, des compétences d'exploitation absentes chez l'acheteur, ni une offre alternative inexistante sur le marché.

De même, un critère de localisation peut être pertinent pour certaines charges. Il ne mesure pas le contrôle opérationnel. Un acheteur qui localise sans maîtriser les accès privilégiés achète une conformité territoriale, non une capacité d'agir.

## 14.5 Effets sur la concurrence et les petites entreprises

Des exigences élevées de sécurité, de continuité ou de réversibilité peuvent écarter des acteurs incapables d'y répondre, y compris des petites entreprises européennes. Des exigences trop faibles peuvent favoriser des piles déjà dominantes. L'effet net sur la concurrence n'est pas démontré ici comme une constante européenne. Il dépend du marché, du lotissement des marchés, de la possibilité de consortiums et de la proportionnalité des critères à l'objet.

La figure et le tableau de ce chapitre rappellent donc une limite : ce qui est **autorisé** juridiquement n'est pas automatiquement **souhaitable** industriellement, et ce qui est **souhaitable** n'est pas automatiquement **mesuré**.

## 14.6 Hypothèse de travail

Dans le cadre analytique de cet ouvrage, la commande publique **peut** structurer la demande cloud et les exigences de réversibilité, mais elle ne crée pas automatiquement des capacités industrielles ou opérationnelles ; la préférence locale n'équivaut pas au succès industriel.[6]

Cette proposition est une **hypothèse de travail**. Les volumes d'achat cloud publics par État membre et les études d'impact dédiées manquent encore. Aucune affirmation selon laquelle la commande publique aurait causé une progression mesurée de la souveraineté du cloud européen n'est établie dans ces pages.

## 14.7 Objections

On objecte que la préférence locale est inefficace ou juridiquement risquée. L'objection est sérieuse : elle justifie de préférer des critères de capacité, de réversibilité testable et de sécurité à une nationalité de façade. On objecte que le marché unique interdit toute politique industrielle par l'achat : la réalité juridique est nuancée et hors de portée d'un conseil dans ces pages. On objecte que la coopération européenne suffit : la coopération sera traitée avec la dynamique de marché, sans la confondre avec l'acte d'achat.

Une objection inverse affirme que sans préférence locale, aucune offre européenne n'émergera. Possible comme mécanisme de marché. Non démontré ici comme loi générale, et non démontré que la préférence produit des capacités plutôt

[6] Cadre analytique de l'ouvrage, proposition de travail sur commande publique et effet industriel ; impact non démontré.

que des rentes.

## 14.8 Ouverture vers le marché

La demande publique est un levier conditionnel. Elle peut exiger ; elle ne fabrique pas à elle seule. Texte en vigueur ≠ projet ≠ rhétorique. Montant contractuel ≠ effet industriel. Clause de sortie ≠ migration testée. Le corpus juridique et institutionnel est partiel ; l'effet industriel reste non démontré.

Adoption déclarée, parts de marché et coopération européenne interagissent ensuite, sans qu'aucune de ces grandeurs n'égale, à elle seule, la souveraineté cloud. C'est le terrain du chapitre suivant.



CHAPITRE 15

# Adoption, concurrence, coopération et effets de réseau

Trois chiffres circulent souvent dans le même paragraphe : combien d'entreprises utilisent le cloud, quelle part de marché détiennent les grands fournisseurs, quel degré de « souveraineté » l'Europe aurait atteint. Ce sont trois objets distincts. Les fusionner produit la confusion la plus tenace du débat, et l'une des plus utiles aux discours qui veulent conclure trop vite.

Les chapitres sur l'industrie, l'exploitation, le financement et la commande publique ont situé l'offre et un levier de demande. Celui-ci regarde la **dynamique de marché** : ce qui attire les clients, ce qui les retient, ce qui renforce ou fragilise une concurrence crédible, et ce que la coopération européenne peut, ou ne peut pas, y changer. Il rappelle des grandeurs déjà documentées. Il n'en invente pas. Il refuse de les transformer en verdict de souveraineté.

## 15.1 Trois grandeurs à ne pas fusionner

| Grandeur | Ce qu'elle mesure | Ce qu'elle ne mesure pas |
|---|---|---|
| Adoption | Usage déclaré de services cloud payants | Parts de fournisseurs ; souveraineté |
| Parts de marché | Concentration de l'offre (estimations) | Maîtrise opérationnelle ; réversibilité |
| Souveraineté cloud (cadre du livre) | Degré de capacités face aux dépendances critiques | Un taux d'adoption ou une part |

En 2025, 52,7 % des entreprises de l'Union couvertes par l'enquête Eurostat déclaraient utiliser des services payants d'informatique en nuage.[1] Cette proportion a progressé depuis 2023 et depuis 2014. Elle décrit une adoption. Elle ne dit pas qui capture la valeur, ni si l'on peut sortir, ni quelles couches, infrastructure, plateforme ou logiciel, dominent chez les répondants.

Selon des estimations privées de juillet 2025, la part des fournisseurs cloud « européens » sur le marché régional d'infrastructure serait restée autour de 15 % après 2022, tandis qu'AWS, Microsoft et Google représenteraient ensemble environ 70 % au moment de la publication.[2] Ce sont des estimations de marché, non une statis-

[1] Eurostat, « 53% EU enterprises used paid cloud services in 2025 », et dataset associé (indicateur d'usage cloud payant).

[2] Synergy Research Group, « European Cloud Providers' Local Market Share Now Holds Steady at 15% »,

tique officielle, et non une mesure de souveraineté. Les lire comme un baromètre de maîtrise serait une erreur de catégorie.

La souveraineté cloud, dans le cadre de cet ouvrage, n'est ni le taux Eurostat ni la part Synergy. C'est un degré de capacités face à des dépendances critiques. Une adoption élevée peut coexister avec une concentration forte. Une part européenne plus élevée pourrait coexister avec une faible réversibilité. Les trois grandeurs peuvent évoluer dans des directions différentes.[3]

## 15.2 Effets de réseau, coûts de changement, économies d'échelle

Un marché cloud n'est pas seulement une confrontation de catalogues. Plus un écosystème est adopté, plus il attire outils, compétences, formations et intégrateurs. Ces **effets de réseau** rendent l'écosystème plus utile pour le prochain client, et plus coûteux à quitter pour le client déjà engagé. Le mécanisme est plausible et largement discuté. Il n'implique pas que la concentration soit « optimale » au sens de la réversibilité. Il n'implique pas non plus qu'une fragmentation forcée produirait automatiquement des capacités européennes.

Les **coûts de changement** prolongent ce raisonnement. Ils ne se réduisent pas au prix d'une migration technique. Ils incluent la réécriture d'applications, la reconversion des équipes, la perte temporaire de fonctionnalités, la coordination entre métiers, et parfois des frais de sortie des données. Les chapitres sur les prix et le coût total ont déjà montré pourquoi le catalogue seul trompe. Ici, l'enjeu est dynamique : plus ces coûts sont élevés et peu mesurés, plus une adoption initiale peut se transformer en dépendance structurelle, même si des concurrents existent sur le papier.

Les **économies d'échelle** jouent dans l'autre sens du débat. Les grands opérateurs répartissent des coûts fixes, régions, sécurité, recherche, support, sur une base mondiale. Cela peut expliquer une partie de leur attractivité tarifaire et fonctionnelle. Cela n'efface pas la question de la criticité des dépendances, ni celle de la possibilité de sortir. Dire « c'est moins cher parce que plus grand » décrit un mécanisme économique. Ce n'est pas une preuve que la dépendance associée est acceptable pour chaque charge critique.

---

24 juillet 2025 : estimations privées ; définition « European provider » partielle.

[3] Cadre analytique de l'ouvrage, distinction adoption / parts / souveraineté.

## 15.3 Confiance, adoption et multi-cloud

L'adoption déclarée mesure une confiance opérationnelle minimale : assez pour payer un service. Elle ne mesure pas la confiance dans la capacité de sortir, ni dans la maîtrise des accès privilégiés, ni dans la continuité sous contrainte. Une organisation peut adopter massivement tout en reportant indéfiniment les tests de réversibilité. Le chapitre sur la réversibilité a déjà séparé obligation juridique, clause contractuelle et migration réellement testée. Le marché amplifie cette confusion lorsqu'il vend l'adoption comme maturité.

Le **multi-cloud**, souvent présenté comme remède, n'est pas une preuve de substituabilité. Opérer deux fournisseurs peut augmenter la complexité et les coûts de coordination sans réduire la criticité si les charges critiques restent captives d'un seul. Là encore, mécanisme plausible ≠ résultat observé pour chaque organisation. Sans tests, le multi-cloud peut n'être qu'une diversification de factures.

## 15.4 Concurrence, interopérabilité et résilience

Les analyses de concurrence soulignent concentration, barrières au changement et limites d'interopérabilité dans plusieurs juridictions.[4] La concurrence ne se juge pas seulement au nombre d'acteurs sur une slide. Elle se juge aussi à la possibilité réelle de basculer, formats, délais, compétences, coûts totaux.

Trois exigences se croisent sans se confondre. La **concurrence** vise des alternatives crédibles. L'**interopérabilité** vise la portabilité des charges et des données. La **résilience** vise la capacité d'absorber un choc sans rupture inacceptable. Renforcer l'une peut affaiblir une autre si l'on n'y prend garde : une standardisation trop lente peut freiner l'offre ; une course à l'adoption peut sacrifier la sortie ; une exigence de résilience très haute peut écarter des acteurs plus petits, y compris européens, incapables d'y répondre immédiatement. Ces arbitrages ne se résolvent pas par un slogan. Ils se lisent charge par charge, marché par marché.

## 15.5 Coopération européenne : échelle sans magie

La coordination entre États membres et institutions peut réduire la fragmentation des exigences et augmenter l'échelle des projets. Elle peut aussi produire une harmonisation de façade sans capacités partagées. Sans évaluation de programmes enregistrée ici comme preuve d'effet industriel, on s'en tient à cette tension : coopération ≠ uniformisation forcée, fragmentation ≠ expérimentation réussie.

La coopération peut porter sur des standards, des marchés communs, des infrastructures de recherche, des exigences de sécurité ou des projets industriels. Chacun de ces objets a ses conditions de succès. Les confondre sous le seul mot « coopéra-

[4] OCDE, « Competition in the provision of cloud computing services », 2025.

tion européenne » produit un optimisme indifférencié. Le livre préfère relier chaque forme de coopération aux capacités qu'elle est censée renforcer, humaines, économiques, technologiques, industrielles, institutionnelles, et aux preuves disponibles. La commande publique, traitée au chapitre précédent, est un levier de demande. Elle ne remplace pas une offre industrialisée ni des compétences d'exploitation.

## 15.6 Ce que le marché ne prouve pas seul

Les mécanismes économiques rappelés ici, effets de réseau, coûts de changement, économies d'échelle, confiance, coopération, éclairent pourquoi certaines dépendances deviennent critiques. Ils ne démontrent pas, à eux seuls, le degré de souveraineté du cloud européen. Ils ne remplacent pas l'inventaire industriel manquant, ni la maîtrise opérationnelle mesurée, ni les tests de sortie encore absents du corpus.

Dans le cadre analytique de cet ouvrage, adoption, concurrence et coopération **conditionnent** la trajectoire des dépendances cloud, sans qu'aucune de ces grandeurs n'égale à elle seule la souveraineté.[5]

Cette proposition articule des faits bornés (adoption Eurostat), des estimations privées (parts de marché) et des mécanismes de concurrence documentés. Elle n'attribue pas de probabilités aux scénarios futurs. Elle n'élève pas les lacunes des chapitres industriels et opérationnels.

## 15.7 Objections

On objecte que la concentration reflète surtout l'efficacité. Possible pour certains services. Cela n'élimine pas la question des coûts de sortie et de la criticité. On objecte que l'adoption prouve l'acceptation sociale du cloud : elle prouve un usage déclaré, non une maîtrise. On objecte que la coopération européenne est trop lente : la lenteur n'autorise pas à inventer des résultats.

Une objection inverse affirme que seules des parts de marché européennes élevées prouveraient la souveraineté. Le livre refuse cette réduction. Des parts plus élevées pourraient accompagner une faible maîtrise opérationnelle ou une faible réversibilité. Elles resteraient néanmoins une grandeur utile, parmi d'autres, pour lire la dynamique d'offre.

## 15.8 Vers la mesure

Adoption, parts de marché et souveraineté cloud ne se fusionnent pas. Les effets de réseau et les coûts de changement éclairent la criticité des dépendances. La coopération européenne peut accroître l'échelle ; elle ne crée pas magiquement des capacités. Les grandeurs rappelées ici restent bornées à leurs sources.

[5] Cadre analytique de l'ouvrage, proposition de travail sur adoption, concurrence et coopération.

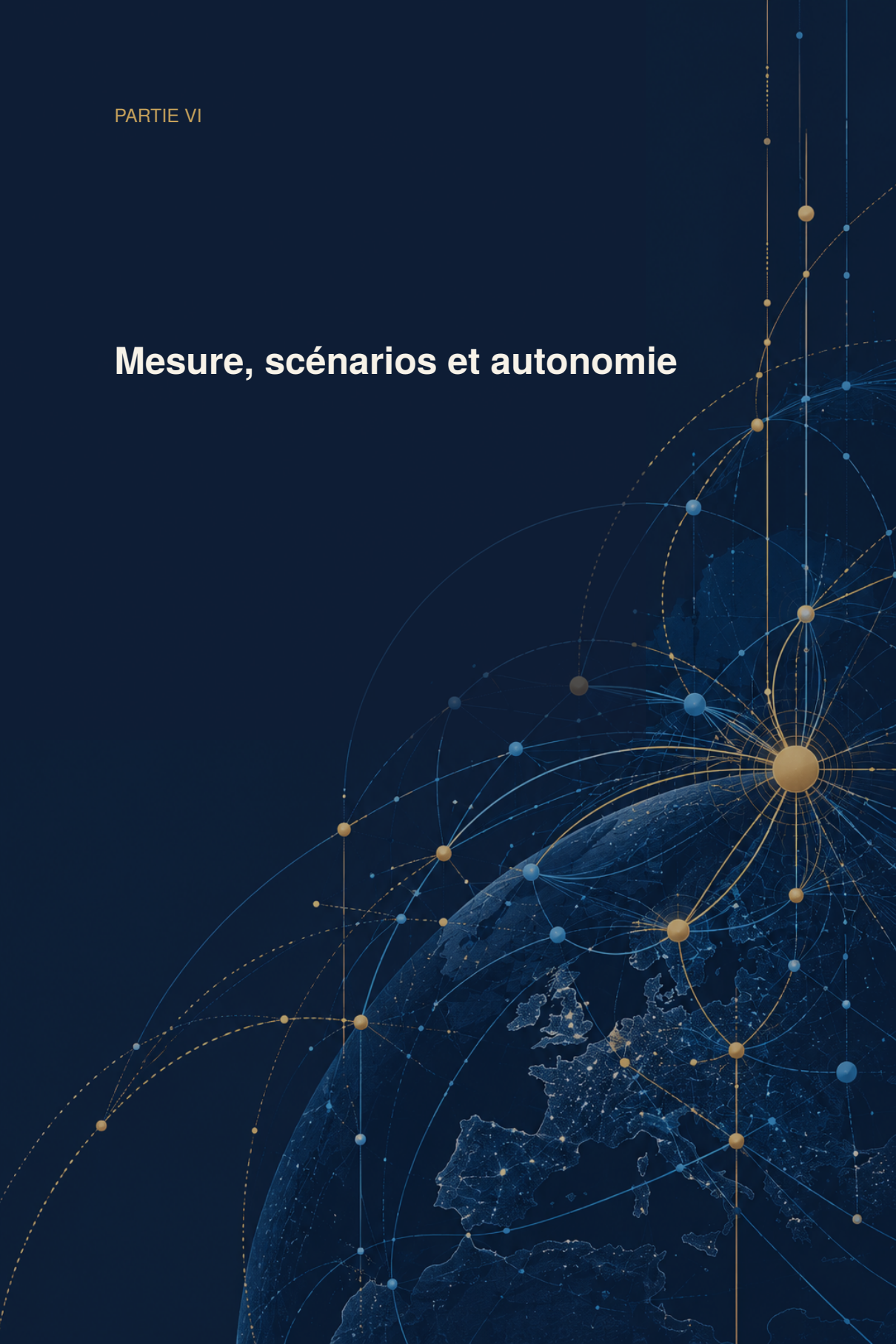
Pour rendre visibles capacités et dépendances sans fabriquer un score unique, il faut un tableau de bord discipliné. C’est l’objet du chapitre suivant.

---



PARTIE VI

# Mesure, scénarios et autonomie



CHAPITRE 16

# Construire un tableau de bord des capacités et dépendances

Un seul chiffre de « souveraineté cloud » rassurerait les tableaux de bord politiques. Il tromperait aussi. Pondérations arbitraires, valeurs manquantes masquées, fusion d'objets incomparables : le score composite promet une fausse précision. Ce chapitre propose autre chose, un **cadre de suivi** d'indicateurs distincts, avec des trous admis et des familles séparées.

Le chapitre précédent a séparé adoption, parts de marché et souveraineté, et a rappelé les mécanismes de marché. Celui-ci opérationnalise le cadre de mesure du livre. Il n'attribue **aucun score composite**. Il n'invente aucune série manquante. Il refuse d'élever automatiquement des affirmations encore insuffisamment documentées.[1]

## 16.1 Quatre familles d'indicateurs

Avant les dimensions, quatre rôles analytiques :

| Famille | Question | Exemple de sens |
|---|---|---|
| Entrée | Qu'injecte-t-on ? | Budgets de formation, enveloppes de recherche, volumes d'achat |
| Capacité | Que peut-on faire ? | Labos accessibles, équipes d'astreinte, offre industrialisée |
| Résultat | Qu'observe-t-on ? | Délais de migration testés, coûts totaux calibrés, alternatives utilisées |
| Résilience | Que tient-on sous contrainte ? | Restauration testée, substitutabilité, points de défaillance uniques |

Confondre une *entrée* (dépenser) avec un *résultat* (sortir réellement) est l'une des erreurs les plus fréquentes des politiques cloud. Confondre une *capacité* déclarée avec une *résilience* testée en est une autre. Le tableau de bord doit rendre ces confusions visibles, non les lisser.

Ces familles prolongent le cadre multidimensionnel déjà fixé : la souveraineté cloud y désigne un **degré** de capacités permettant de réduire des dépendances cri-

[1] Cadre de mesure de l'ouvrage, indicateurs distincts et profils ; interdiction par défaut du score composite.

tiques, non une étiquette binaire.[2]

## 16.2 Dimensions et fiches d'indicateurs

Pour chaque dimension, les deux tableaux ci-dessous proposent un indicateur *candidat*, pas une valeur peuplée. Le premier fixe l'objet et l'unité ; le second fixe la source, la disponibilité dans ce livre et les risques de manipulation. Lorsque la donnée est absente ou partielle dans le corpus, la cellule le dit. Aucune interpolation n'est proposée.

| Dimension | Ce qui est mesuré | Indicateur opérationnel candidat | Unité / population |
|---|---|---|---|
| Capital humain | Pipeline et accès réel aux environnements | Part d'établissements avec labos cloud accessibles ; part d'ops formés hors écosystème unique | % établissements / % professionnels (UE ou État) |
| Économie | Prix et coût total | Écart de coût total sur trajectoire explicite (catalogue + sortie + verrouillage) | Monnaie / charge type ; panier borné |
| Technologie / réversibilité | Capacité de sortie et d'interopérabilité | Nombre et succès de migrations testées sur charges prioritaires | Comptage / délai / coût par charge |
| Industrie | Capacité matérielle et contrôle | Capacité DC disponible ; inventaire UBO / contrôle des opérateurs | GW / MW ; part documentée d'opérateurs |
| Exploitation / cyber | Maîtrise opérationnelle | Exercices de restauration réussis ; couverture d'astreinte documentée | Taux de succès / délais ; périmètre de service |
| Gouvernance / achat | Exigences et vérification | Part de marchés avec clauses de sortie *et* vérification après attribution | % marchés / volume |

[2] Cadre analytique de l'ouvrage, définition multidimensionnelle.

| Dimension | Ce qui est mesuré | Indicateur opérationnel candidat | Unité / population |
|---|---|---|---|
| Marché | Adoption et concentration | Adoption déclarée ; parts estimées, **en colonnes séparées** | % entreprises ; % marché (définition explicite) |

| Dimension | Source nécessaire | Fréquence souhaitable | Disponibilité dans ce livre | Limites / risques de manipulation |
|---|---|---|---|---|
| Capital humain | Enquêtes établissements ; enquêtes compétences | Annuelle | **Absente** (hypothèses amont seulement) | Compter des modules nominaux comme accès réel |
| Économie | Catalogues + paramètres de sortie calibrés | Semestrielle | **Partielle** (méthode + panier ; total non calibré) | Afficher le seul prix catalogue |
| Technologie / réversibilité | Protocoles exécutés et journalisés | Annuelle + après incident | **Absente** (protocole non exécuté ici) | Transformer une clause juridique en test réussi |
| Industrie | Études capacité + registres société | Annuelle | **Partielle** (capacité/énergie/typologie ; UBO absent) | Confondre localisation et propriété ultime |
| Exploitation / cyber | Journaux d'exercices ; audits ops | Annuelle + post-crise | **Absente** (pas de comparaison homogène) | Confondre certification et capacité d'agir |
| Gouvernance / achat | Données acheteurs publics | Annuelle | **Partielle** (droit + pratique institutions bornée) | Compter des intentions politiques comme résultats |
| Marché | Statistique officielle + étude de marché étiquetée | Annuelle | **Partielle** (Eurostat + estimations privées distinctes) | Fusionner adoption, parts et souveraineté |

Ces tableaux forment un **cadre analytique**. Ils ne constituent pas un peuplement empirique européen. Ils n'autorisent aucun classement général des États ou des fournisseurs.

## 16.3 Règles de valeurs manquantes

Quatre règles minimales évitent de transformer le tableau de bord en fiction.

Premièrement, une valeur manquante reste manquante : pas de zéro implicite, pas de moyenne européenne inventée. Deuxièmement, une estimation privée porte son étiquette et ne se fond pas dans une statistique officielle. Troisièmement, un protocole non exécuté n'apparaît pas comme un résultat de migration. Quatrièmement, une affirmation encore hypothétique ne change pas de statut parce qu'elle figure dans un beau tableau.

Un outil d'acheteur institutionnel peut calculer un score pour une procédure donnée. Ce n'est pas le cadre de mesure de cet ouvrage. Les deux ne doivent pas être fusionnés.[3]

## 16.4 Profils plutôt que podium

Un profil multidimensionnel, avec des trous explicites, permet de comparer des situations sans prétendre à une note unique. Une administration peut être forte en localisation contractuelle et faible en réversibilité testée. Un fournisseur peut être « européen » au sens d'une estimation de marché et peu documenté sur le contrôle opérationnel. Un État membre peut disposer de capacité électrique sans inventaire clair de propriété ultime.

Le profil rend ces tensions lisibles. Le podium les efface. Par défaut, **aucun score composite** global n'est calculé. Les pondérations éventuelles du cadre de mesure restent provisoires ; elles ne justifient pas un classement tant qu'elles n'ont pas été testées en sensibilité avec des données adaptées.

## 16.5 État des lieux des données : sans interpolation

| Famille du livre | Intention | État documentaire actuel |
|---|---|---|
| Capital humain | Pipeline scolaire, supérieur, ops | Hypothèses et contextes partiels ; certification ≠ capacité ops |
| Économie | Prix équivalents, coût total, sortie | Méthodes + panier partiel ; total non calibré |
| Technologie / réversibilité | Interop, tests de sortie, logiciels libres | Protocoles ; essai d'orchestration **non exécuté** |
| Industrie | Data centers, puces, énergie, supply | Capacité, énergie, typologies documentées ; propriété ultime absente |

[3] Distinction entre cadre de mesure du livre et outils d'acheteur institutionnels.

| Famille du livre | Intention | État documentaire actuel |
|---|---|---|
| Exploitation | Contrôle ops, résilience | Contextualisé ; maîtrise mesurée absente |
| Gouvernance | Droit, achat public, coopération | Textes et pratiques partielles ; effet industriel non démontré |
| Marché | Adoption, concentration | Grandeurs distinctes, partiellement peuplées |

Lorsqu'une cellule dit « absente » ou « non exécuté », le tableau de bord doit afficher un trou, non une interpolation discrète.

## 16.6 Proposition de travail

Le tableau de bord utile à la thèse est un ensemble d'**indicateurs documentés et séparables**, assorti de règles de valeurs manquantes, non un indice unique de souveraineté.[4]

## 16.7 Objections

On objecte qu'il faut un score pour décider. Un score non justifié décide mal. On objecte qu'il y a trop d'indicateurs : mieux vaut peu d'indicateurs peuplés qu'une mosaïque opaque. On objecte enfin que sans séries complètes le chapitre est vide : au contraire, l'aveu structuré des trous est une condition de sérieux.

Une objection politique affirme qu'un tableau de bord sans score ne convainc pas. Peut-être. Le livre préfère ne pas convaincre par une fausse précision.

## 16.8 Vers les trajectoires

Mesurer, ici, c'est rendre visible, y compris ce qui manque. Pas de classement. Pas de score composite par défaut. Les peuplements partiels restent séparés.

Sur cette base méthodologique, on peut formuler des **scénarios** analytiques, non des prédictions, pour exposer arbitrages et conditions d'échec. C'est l'objet du chapitre suivant.



[4] Cadre analytique de l'ouvrage, tableau de bord des capacités et dépendances.

CHAPITRE 17

# Scénarios européens, arbitrages et politiques possibles

Les scénarios ne sont pas des prévisions. Ils exposent des trajectoires plausibles, des arbitrages et des signes observables, sans attribuer de probabilités inventées. Ce chapitre en propose trois, analytiques. Il **ne clôt pas la thèse** du livre. Il ne transforme pas non plus les lacunes documentaires des chapitres industriels et opérationnels en certitudes scénarisées.[1]

Le tableau de bord du chapitre précédent fournit le vocabulaire : entrées, capacités, résultats, résilience, trous visibles. Ici, on combine ces éléments, ou l'on montre comment ils échouent à se combiner. Chaque scénario doit pouvoir être confronté à des observables. Sinon ce n'est qu'une fable stratégique.

Aucune simulation calibrée n'est produite. Aucune probabilité n'est affichée. Les trajectoires ne sont ni un « succès total » ni un « échec total » : chacune admet des progrès sectoriels et des dépendances persistantes.

## 17.1 Scénario A : Dépendance persistante

**Hypothèses.** L'adoption continue de croître. Les coûts de changement restent élevés et peu mesurés. Les tests de sortie restent rares. La base industrielle et les compétences d'exploitation transférables restent insuffisamment articulées. Les politiques multiplient labels et localisations sans vérifier la capacité d'agir.

**Mécanismes.** Les effets de réseau et les économies d'échelle renforcent les écosystèmes déjà dominants. La commande publique achète de la conformité territoriale plus que de la réversibilité testée. La formation reste centrée sur des piles uniques. L'industrialisation locale produit des démonstrateurs sans offrir opérée à l'échelle.

**Décisions ou conditions qui y conduisent.** Reporter indéfiniment les exercices de migration ; traiter le multi-cloud comme une preuve ; fusionner adoption et souveraineté dans les tableaux de bord politiques ; financer la recherche sans suivre le passage à l'offre.

**Dépendances critiques.** Couches plateforme peu substituables ; outils de supervision propriétaires ; compétences non transférables ; composants et régions difficiles à remplacer rapidement.

**Signaux observables.** Parts estimées des grands fournisseurs stables ou crois-

[1] Cadre analytique de l'ouvrage, scénarios analytiques, non prédictifs.

santes ; frais et délais de migration non publiés ; protocoles de réversibilité non exécutés ; exercices de restauration absents ou purement documentaires.

**Risques et compromis.** Continuité de service élevée chez des acteurs mondiaux peut coexister avec une criticité accrue. Le scénario n'est pas une accusation morale : c'est une trajectoire cohérente avec une adoption forte et une sortie faible.

**Ce qui l'affaiblirait.** Des migrations, testées et répétées, sur des charges prioritaires ; des coûts de sortie réellement mesurés et décroissants ; une offre alternative industrialisée utilisée hors niches.

## 17.2 Scénario B : Autonomie ciblée

**Hypothèses.** L'Europe ne vise pas l'autarcie. Elle choisit des périmètres, données sensibles, certains traitements publics, piles où l'interopérabilité est testable, et y réduit des dépendances critiques. Ailleurs, des dépendances globales persistent et sont cartographiées.

**Mécanismes.** La commande publique exige des preuves de sortie et les vérifie après attribution. La formation continue vise la transférabilité, pas seulement des badges. L'industrie et l'énergie restent des contraintes, mais l'inventaire des goulets s'améliore. Les tests de réversibilité deviennent une pratique, non une clause décorative.

**Décisions ou conditions nécessaires.** Prioriser des charges ; financer l'exploitation autant que le prototype ; accepter des coûts totaux parfois plus élevés contre une sortie crédible ; refuser les scores uniques qui masquent les trous.

**Dépendances critiques restantes.** Semi-conducteurs avancés ; certains écosystèmes logiciels mondiaux ; talents rares ; interconnexions internationales.

**Signaux observables.** Migrations testées sur un portefeuille explicite de charges ; clauses de réversibilité vérifiées ; indicateurs industriels partiels mais renseignés ; adoption et parts toujours publiées séparément de la maîtrise.

**Risques et compromis.** Le ciblage peut laisser hors périmètre des dépendances qui se révèlent critiques trop tard. Il peut aussi fragmenter les exigences si chaque État membre invente son propre périmètre sans coordination.

**Ce qui l'affaiblirait.** Des labels sans tests ; une préférence locale sans capacité réelle ; l'abandon des exercices dès la première difficulté budgétaire.

Le scénario B n'est pas un compromis tiède. Il exige plus de discipline empirique que les discours d'autonomie totale. Il décrit aussi une trajectoire **intermédiaire** : progrès sectoriels possibles, dépendances persistantes assumées.

## 17.3 Scénario C : Écosystème intégré

**Hypothèses.** Capacités humaines, économiques, technologiques, industrielles et institutionnelles se renforcent mutuellement à une échelle significative. La coopération européenne réduit la fragmentation des exigences sans abolir toute expérimentation. Des alternatives viables existent pour une part croissante des charges critiques, sans prétendre éliminer toute dépendance globale.

**Mécanismes.** Le vivier d'exploitation devient documenté et mobile entre piles. Les coûts totaux et les sorties sont calibrés sur des paniers publics. L'offre industrialisée dialogue avec une demande qui vérifie. La base matérielle, capacité, énergie, chaînes, est lue avec des inventaires de contrôle, non seulement des cartes de bâtiments.

**Décisions ou conditions nécessaires.** Continuité de financement au-delà du démonstrateur ; coopération sur des standards réellement mis en œuvre ; refus de confondre parts de marché et maîtrise ; investissement dans la résilience testée autant que dans la communication.

**Dépendances critiques plausibles même ici.** Composants amont ; certains firmware et équipements ; interdépendances mondiales de réseau et de talent. Les nier rendrait le scénario caricatural.

**Signaux observables.** Vivier ops transférable documenté ; migrations et restaurations répétées ; base industrielle et offre en dialogue mesurable avec la demande ; tableau de bord peuplé sans score composite trompeur.

**Risques et compromis.** Le coût et le temps d'une telle articulation sont élevés. Une harmonisation mal conçue peut étouffer des expérimentations utiles. Une réussite partielle sur un segment peut être présentée, à tort, comme une souveraineté globale.

**Ce qui l'affaiblirait.** Des success-stories non reproductibles ; un peuplement fictif d'indicateurs ; l'oubli des dépendances persistantes.

Le scénario C n'est pas une promesse. Il décrit une articulation exigeante de capacités, encore non démontrée à l'échelle européenne dans le corpus actuel.

| Arbitrage | Tension |
|---|---|

## 17.4 Arbitrages qui traversent les trois trajectoires

| Arbitrage | Tension |
|---|---|
| Vitesse d'adoption vs réversibilité | Adopter vite peut accroître le verrouillage |
| Coût catalogue vs coût de sortie | Économie apparente / dette cachée |
| Préférence locale vs capacité réelle | Soutien industriel / façade |
| Harmonisation vs expérimentation | Échelle / diversité |
| Open source vs industrialisation | Licence ouverte / offre opérée |
| Résilience exigée vs accès des petites entreprises | Exigence haute / barrière d'entrée |

Ces arbitrages ne désignent pas un vainqueur. Ils rappellent que chaque trajectoire paie un prix, parfois en dépendance, parfois en coût, parfois en lenteur.

## 17.5 Leviers et conditions d'échec

Les leviers évoqués dans le livre, école, supérieur, exploitation, prix, coût total, tests de sortie, logiciels libres, industrie, cybersécurité, financement, achat public, coopération, n'agissent pas isolément. Un levier unique peut échouer si les autres manquent : formation sans labos ; labos sans industrialisation ; droit sans contrôle opérationnel ; open source sans maintenance ; achat sans offre.

Les scénarios servent précisément à rendre ces échecs **lisibles** avant qu'ils ne deviennent des récits de surprise.

## 17.6 Objections

On objecte que la politique industrielle est inefficace. Possible : les scénarios doivent alors montrer des conditions d'échec observables, non des slogans. On objecte que le laisser-faire suffit : la concentration et les barrières au changement documentées ailleurs rendent cette objection discutable, non tranchée ici. On objecte enfin qu'il faudrait des probabilités : sans modèle calibré, les afficher serait une imposture.

## 17.7 Vers la conclusion

Trois scénarios, des arbitrages, des observables, pas de verdict. La clôture intellectuelle du livre appartient au chapitre suivant.



CHAPITRE 18

# Vers une autonomie cloud progressive, mesurable et réaliste

La thèse de ce livre n'était pas une conclusion déguisée. Elle proposait d'examiner une idée : la souveraineté du cloud européen résulte du développement progressif de capacités humaines, économiques, technologiques, industrielles et institutionnelles interdépendantes, dont la combinaison permet de réduire les dépendances critiques envers les acteurs non européens.

Après le parcours, infrastructure, définitions, dépendances, capital humain, coûts, réversibilité, logiciels libres, industrie, cybersécurité, offre, demande publique, marché, mesure, scénarios, que peut-on **tenir analytiquement**, et que doit-on laisser ouvert ? Ce chapitre est la **synthèse du cadre** : ce qui est établi, plausible ou non démontré, les interdépendances, les conditions de réfutation. Il ne déclare pas le livre scientifiquement validé. L'adresse finale au lecteur appartient à la conclusion générale.

## 18.1 Ce que le parcours a établi

Certaines distinctions tiennent solidement. Le cloud est une infrastructure ; l'adopter n'est pas la maîtriser. La souveraineté cloud, dans ce livre, est un **degré** de capacités, non une étiquette. Les dépendances deviennent critiques par des mécanismes, concentration, coûts de changement, sortie des données, interopérabilité limitée, non par slogan. Adoption déclarée, parts de marché estimées et degré de souveraineté restent des grandeurs distinctes. Le tableau de bord refuse le score unique. Les scénarios exposent des trajectoires sans prédire.

Des faits bornés ancrent le raisonnement : une adoption déclarée mesurée par l'enquête européenne ; des estimations privées de concentration à manier avec sobriété ; des textes juridiques en vigueur sur les marchés et sur le changement de fournisseur ; des protocoles de comparaison tarifaire et de coût total qui refusent les trous inventés. Ces éléments ne « prouvent » pas la thèse. Ils empêchent de la discuter dans le vide.

## 18.2 Ce que le parcours a rendu plausible

D'autres propositions restent plausibles sans être démontrées à l'échelle européenne. L'école et le supérieur forment des conditions amont du vivier. Les certifications ne prouvent pas la transférabilité. L'open source et les standards sont des leviers conditionnels. La base industrielle et la maîtrise opérationnelle **conditionnent** la réduction des dépendances. L'industrialisation et le financement conditionnent l'existence d'alternatives viables. La commande publique peut structurer la demande sans créer automatiquement des capacités. Adoption, concurrence et coopération orientent les trajectoires sans les dicter seules.

Ces articulations forment le cœur de la thèse. Elles expliquent pourquoi la souveraineté ne se réduit ni à la **localisation** des machines, ni à une **préférence** de fournisseur. Localiser sans contrôler les accès, sans pouvoir restaurer, sans pouvoir sortir, ce n'est pas maîtriser. Préférer un acteur « local » sans offre industrialisée ni compétences d'exploitation, ce n'est pas réduire une dépendance critique, c'est parfois la déplacer.

## 18.3 Ce que le parcours n'a pas démontré

La thèse n'a pas prouvé que l'Europe a atteint une souveraineté cloud. Elle n'a pas prouvé qu'une autonomie complète est possible ni souhaitable. Elle n'a pas produit d'inventaire pan-européen de propriété ultime des opérateurs, de maîtrise opérationnelle mesurée de façon homogène, ni de migrations d'orchestration exécutées dans ce dépôt. Le panier tarifaire et le modèle de coût total restent partiels. Les effets industriels de la commande publique ne sont pas établis comme une constante européenne. Aucune simulation calibrée des scénarios n'a été produite.

Ces absences ne sont pas des détails de note. Elles définissent la frontière entre ce que le livre peut affirmer et ce qu'il doit laisser ouvert.

## 18.4 Interdépendances : pourquoi un levier seul échoue

Compétences sans labos, labos sans industrialisation, industrialisation sans demande solvable, demande sans réversibilité testée, droit sans contrôle opérationnel, localisation sans inventaire de contrôle : chaque maillon isolé peut donner l'illusion du progrès. La thèse insiste sur la **combinaison**. Réduire une dépendance critique exige souvent, en même temps, un savoir-faire humain, un calcul économique honnête, une possibilité technique de sortie, une base matérielle lisible, une capacité d'agir sous incident, et des institutions qui vérifient ce qu'elles exigent.

C'est pourquoi les scénarios du chapitre précédent ne sont pas des menus politiques. Ce sont des manières de voir comment ces maillons s'assemblent, ou se défont.

## 18.5 Autonomie progressive

Dans le cadre analytique de cet ouvrage, une **autonomie cloud progressive** désigne une réduction mesurable, partielle et révisable de dépendances critiques, distincte de l'autarcie et d'un score unique.[1]

Mesurable : des indicateurs séparés, des tests, des trous avoués. Partielle : certaines dépendances globales peuvent rester. Révisable : ce qui était critique hier peut ne plus l'être demain, et l'inverse. Cette définition n'est pas une loi empirique. Elle est une boussole contre deux excès : promettre l'indépendance totale, ou renoncer à toute réduction parce que l'autarcie est impossible.

## 18.6 Conditions de réfutation

La thèse de travail serait affaiblie ou à réviser si, notamment :

- des capacités interdépendantes se développaient sans aucune réduction observable des dépendances critiques sur des périmètres testés ;
- une réduction des dépendances s'obtenait sans ces capacités, par exemple par un simple déplacement de fournisseur sans maîtrise ;
- la mesure ne pouvait jamais séparer adoption, parts et capacités ;
- l'autarcie s'avérait l'unique lecture cohérente, ce que le livre refuse comme cadrage, mais qui devrait alors être argumenté autrement.

## 18.7 Besoins de recherche

Le corpus appelle des travaux que ce livre ne remplace pas : inventaires de propriété ultime et de contrôle des infrastructures ; comparaisons homogènes de maîtrise opérationnelle et de restauration ; exécution publique de protocoles de réversibilité ; calibration de coûts totaux sur des paniers représentatifs ; suivi des passages recherche → offre opérée ; évaluations d'impact de la commande publique sur les capacités, et non seulement sur les montants contractuels. Tant que ces preuves manquent, la prudence n'est pas une faiblesse. C'est une méthode.

## 18.8 Objections finales

On objecte que l'autonomie est impossible : alors il faut dire lesquelles des dépendances sont inéliminables et pourquoi. On objecte qu'elle est déjà atteinte : les mécanismes de verrouillage et les lacunes de réversibilité testée rendent cette affirmation prématurée. On objecte qu'elle est indésirable : c'est un débat normatif distinct de la mesure des capacités.

[1] Cadre analytique de l'ouvrage, autonomie progressive et limites.

## 18.9 Proposition à examiner

La thèse demeure une **proposition à examiner**, enrichie par un vocabulaire, des distinctions et des protocoles, non une loi empirique établie. Une autonomie cloud progressive, mesurable et réaliste désigne ici une direction de travail : combiner des capacités, tester ce qui peut l'être, refuser les scores trompeurs, et admettre ce qui manque encore.

Ce chapitre arrête la **synthèse analytique**. La conclusion générale reprend la question centrale pour le lecteur et ouvre sur les priorités qu'autorise, sans les imposer, le corpus disponible.



# Conclusion

La question de départ était simple à formuler et difficile à trancher : dans quelles conditions la souveraineté du cloud européen peut-elle être comprise comme le résultat de capacités interdépendantes, plutôt que comme une étiquette déjà acquise ou un simple lieu d'hébergement ?

Le livre répond d'abord par une **méthode**. Il refuse de fusionner adoption, parts de marché, localisation, propriété, contrôle opérationnel, prix catalogue, coût total, obligation juridique et industrialisation. Il traite la souveraineté cloud comme un **degré de capacités** face à des dépendances critiques. Cette réponse n'est pas un verdict de souveraineté atteinte. C'est un cadre pour lire ce qui est établi, ce qui est estimé, ce qui est plausible et ce qui reste ouvert.

Le chapitre précédent a dressé l'inventaire analytique : ce que le parcours a établi, rendu plausible ou laissé non démontré, ainsi que les conditions de réfutation. Ici, il s'agit d'assumer ce cadre face aux décisions et aux recherches à venir.

## 1 Ce que le lecteur peut emporter

Plusieurs distinctions tiennent. Adoption n'est pas souveraineté. Localisation n'est pas contrôle. Un prix catalogue n'est pas un coût total. Un texte juridique n'est pas une industrialisation. Une certification n'est pas une compétence transférable. Un financement n'est pas une offre opérée. Ces règles de lecture ne remplacent pas les preuves manquantes. Elles empêchent de conclure trop vite.

La thèse insiste sur la **combinaison** des capacités humaines, économiques, technologiques, industrielles et institutionnelles. Un levier isolé peut donner l'illusion du progrès. Des dépendances mondiales peuvent rester même dans une trajectoire favorable. Le livre ne promet ni autarcie ni score unique.

## 2 Limites assumées

L'inventaire européen homogène de propriété ultime des opérateurs manque. La maîtrise opérationnelle agrégée n'est pas mesurée de façon comparable. L'effet industriel de la commande publique n'est pas démontré. Le panier tarifaire et le modèle de coût total restent partiels. Un protocole de réversibilité peut être formulé sans avoir été exécuté. Plusieurs affirmations industrielles et institutionnelles demeurent des hypothèses de travail.

Ces lacunes font partie du résultat de l'enquête. Elles indiquent ce qu'il faudrait observer pour renforcer, nuancer ou réfuter la thèse, sans les combler par invention.

## 3 Priorités proportionnées aux preuves

Sans proclamer une feuille de route politique, le livre autorise des priorités analytiques prudentes. Clarifier les grandeurs avant de les fusionner. Exiger des protocoles de prix et de coût total avant les classements. Tester la réversibilité plutôt que de s'en remettre aux seules clauses. Distinguer intention, acte et résultat dans les programmes publics. Traiter localisation, propriété et contrôle comme des questions séparées. Refuser les scores composites de souveraineté sans méthode validée.

Ces priorités ne remplacent pas le débat démocratique. Elles le disciplinent.

## 4 Ouverture

Le cloud restera, pour longtemps encore, un espace de dépendances partielles, d'arbitrages économiques et de capacités inégalement distribuées. La question n'est pas de savoir si l'Europe peut tout produire seule. Elle est de savoir quelles dépendances elle juge critiques, quelles capacités elle construit réellement, et comment elle évite de prendre des labels pour des preuves.

La souveraineté du cloud européen, si le terme doit garder un sens, n'est pas un drapeau planté sur un data center. C'est une trajectoire de capacités, exigeante, mesurable par morceaux, toujours incomplète, dont ce livre a cherché à rendre les engrenages visibles.

# Épilogue

Une infrastructure numérique ne devient maîtrisable que lorsque l'on peut en comprendre les composants, en former les opérateurs, en mesurer les coûts réels, en tester les sorties et en distinguer ce que l'on possède de ce que l'on contrôle. Sans ces capacités, le nuage reste une promesse d'efficacité et un risque de dépendance.

L'Europe n'a pas à choisir entre naïveté technologique et fantasme d'autarcie. Elle a à construire, pièce par pièce, des capacités vérifiables. Certaines preuves manquent encore : inventaires de contrôle, migrations réellement exécutées, coûts totaux calibrés, effets industriels mesurés. Les admettre, ce n'est pas renoncer. C'est refuser de prendre un label pour une maîtrise.

La souveraineté cloud, si le mot doit garder un sens, ne se décrète pas sur une couverture. Elle se construit dans les laboratoires, les contrats, les usines, les budgets et les compétences, là où l'on accepte enfin de **mesurer** ce que l'on prétend maîtriser.

CONTINUITÉ VISUELLE

## Illustration d’accompagnement

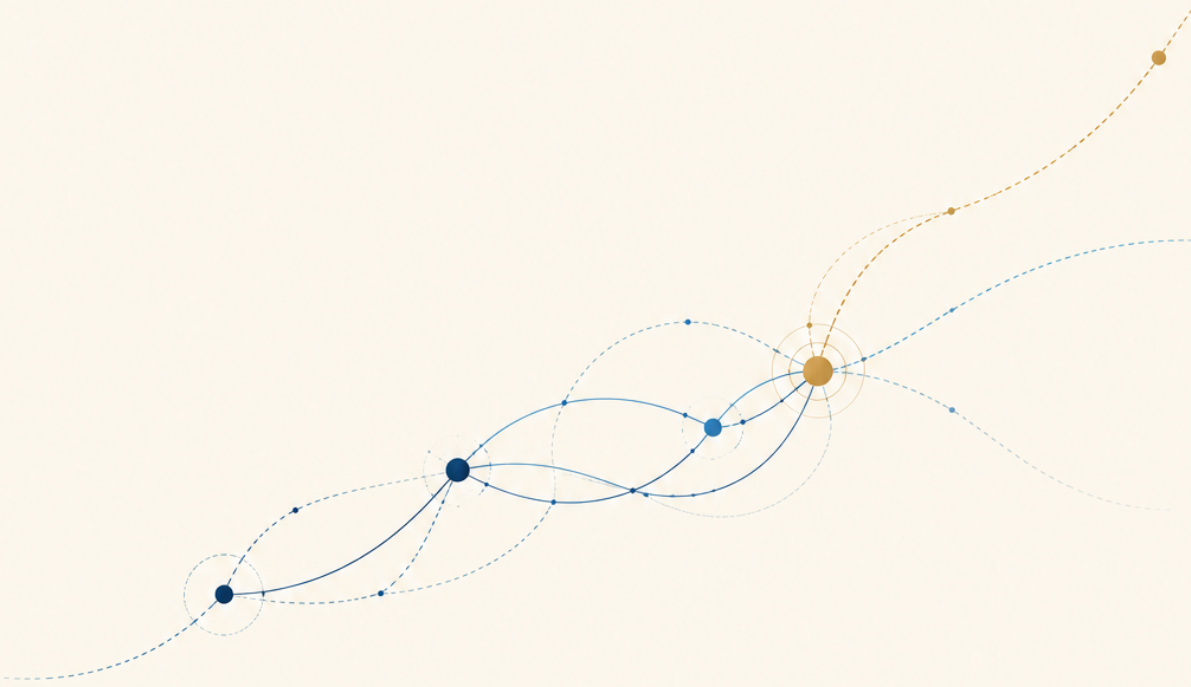
Cette page n’est **pas** une conclusion supplémentaire. La conclusion rédigée et l’épilogue précèdent cette illustration. L’image prolonge le parcours du livre par une continuité visuelle.



Continuité visuelle (illustration conceptuelle).

## Fin du volume

Les pages intérieures s’achèvent ici. Les limites empiriques exposées dans le livre restent ouvertes : elles appartiennent au raisonnement.



**Quatrième de couverture**

Pourquoi parler de souveraineté cloud si l'hébergement en Europe ne garantit ni la maîtrise, ni la sortie, ni l'industrialisation ? Ce livre propose un cadre : des capacités humaines, économiques, technologiques, industrielles et institutionnelles interdépendantes, dont la combinaison peut réduire des dépendances critiques, sans proclamer une souveraineté déjà acquise.

Adoption, parts de marché, localisation et contrôle : des grandeurs distinctes.



FRANCK MEVENGUE