numeum

# Les essentiels de l'informatique en nuage

Dans un contexte où l'informatique en nuage *(cloud computing)* est la technologie au cœur de la transformation et la numérisation de l'économie constituant ainsi le support du développement des nouvelles technologies comme l'intelligence artificielle et le quantique, ce document a vocation d'illustrer l'intérêt et la manière pour les entreprises d'embrasser cette technologie, mais également de recenser les enjeux entourant cette dernière.

**Au-delà de son caractère technique, quelles sont les clés pour se saisir des opportunités offertes par le *cloud computing* ? Comment décrypter les notions et concepts couramment utilisés en lien avec cette technologie ?**

## Table des matières

# I. Le cloud et généralités

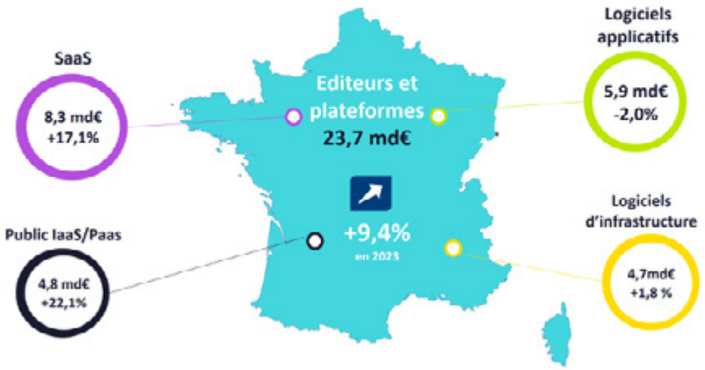
***Le Cloud Computing*** (ci-après cloud) est défini par le National Institute of Standards and Technology (NIST) comme « *un modèle permettant un accès réseau omniprésent, pratique et à la demande à un ensemble partagé de ressources informatiques configurables (par exemple des réseaux, serveurs, stockage, application et services) qui peuvent être rapidement approvisionnées et libérées avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services* ».

Pour les organisations, **la stratégie de migration vers le cloud** consiste à déplacer les applications et environnements informatique habituellement hébergés sur son propre site (« *on premises* ») vers un fournisseur d'infrastructures cloud. Il offre la possibilité d'externaliser « *la gestion de tout ou partie des logiciels, applications et services informatiques existants*[1] ».

Le cloud offre de nombreuses possibilités permettant d'accélérer la transformation numérique des organisations publiques et privées, dans un cadre maximisant la performance des services et leur disponibilité et la flexibilité de leurs usages, tout en ayant l'ambition de réduire les coûts associés à ces services grâce à l'effet de mutualisation des clients sur une même plateforme.

Ce marché est dès lors en pleine croissance, tirant ainsi la croissance du marché des services numériques en 2023. Selon le cabinet Markess by Exaegis[2], le marché français du cloud devrait atteindre les **<u>27 milliards d'euros en 2025</u>**.

## Le marché éditeurs et plateformes cloud




Services Cloud à gauche, services sur site «on premise» à droite

*Source : Enquête Numeum / PAC, 2023*

[1] Avis de l'Autorité de la concurrence portant sur le secteur des nouvelles technologies appliquées aux activités de paiement, 5 avril 2021
[2] Markess by Exaegis prévoit un marché global du Cloud à 27 milliards d'euros en 2025 en France, Ronan Mevel, 11 avril 2022



## Les stratégies de migration vers le cloud

Pour une organisation, démarrer une stratégie de migration vers le cloud nécessite de réaliser une analyse en profondeur des systèmes d'information afin d'établir précisément les besoins en services cloud. Sur cette base, il s'agit alors de décider du périmètre de la migration. Le périmètre de la migration du cloud et la nature du service choisi varient en fonction de chaque usage.

Les stratégies de migration demandent plus ou moins d'efforts de la part du client. Par exemple, l'option de « *réhébergement* », ou « *lift and shift* », est une des stratégies à priori les plus simples à appliquer. Elle « consiste à transférer un environnement existant vers le cloud[3] », avec un minimum de remédiation du système d'exploitation et des bases de données de l'application.

Néanmoins, le réhébergèrent ne permet pas d'utiliser pleinement des avantages du cloud. Le passage au cloud est l'occasion de moderniser les applications et autres services utilisés. D'autres stratégies permettent de valoriser ces bénéfices mais nécessitent des modifications de l'architecture de l'application à migrer et de réécrire une partie de son code afin de bénéficier au mieux des infrastructure et plateforme cloud utilisés. Plusieurs stratégies sont possibles : *replateforming, replateforming, redeploying ou encore rearchitecturing*[4].

Enfin, afin d'optimiser les avantages du cloud, les entreprises doivent mettre en place une nouvelle stratégie de développement des applications en cohérence avec les méthodologies de développement modernes et agiles comme le DevOps ou le CI/CD. C'est tout l'enjeu du développement d'applications « cloud-native » : cela signifie qu'une application a été conçue spécialement pour offrir une expérience cohérente de développement et de gestion automatisée dans l'utilisation du cloud.

## Les trois grandes catégories de services cloud

Il existe trois types de services principaux de *cloud computing*. L'appartenance d'un service à un modèle dépend du degré d'externalisation du service en question. La liste ci-dessous est listée du moins au plus externalisée.

> **IaaS (« Infrastructure as a Service ») :** ce terme est défini par le NIST comme « *la capacité (…) de fournir le traitement, le stockage, les réseaux et d'autres ressources informatiques fondamentales dans lesquelles le consommateur peut déployer et exécuter les logiciels de son choix, qui peuvent inclure des systèmes d'exploitation et des applications. Le consommateur ne gère ni ne contrôle l'infrastructure cloud sous-jacente, mais contrôle les systèmes d'exploitation, le stockage et les applications déployées ; et éventuellement un contrôle limité de certains composants réseau (par exemple, les pare-feu hôtes)* ».
>
> **PaaS (« Platform as a Service ») :** ce terme est défini par le NIST comme « *la capacité fournie au consommateur qui consiste à déployer, sur l'infrastructure cloud, des applications créées ou acquises par le consommateur à l'aide de langages de programmation, de bibliothèques, de services et d'outils pris en charge par le fournisseur. Le consommateur ne gère ni ne contrôle l'infrastructure cloud sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation ou le stockage, mais contrôle les applications déployées et éventuellement les paramètres de configuration pour l'hébergement des applications* ».
>
> **SaaS (« Software as a Service ») :** ce terme est défini par le NIST comme « *la capacité offerte au consommateur qui consiste à utiliser les applications du fournisseur exécutées sur une infrastructure cloud. Les applications sont accessibles à partir de divers dispositifs clients via une interface client légère, telle qu'un navigateur web (par exemple, une messagerie électronique basée sur le web), ou une interface de programme. Le consommateur ne gère ni ne contrôle l'infrastructure cloud sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation, le stockage ou même les capacités des applications individuelles, à l'exception possible des paramètres de configuration d'application spécifiques à l'utilisateur* ».

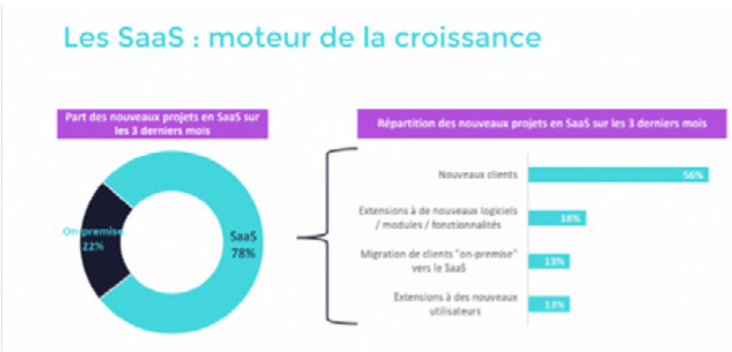
[3] Stratégies de migration du SI dans le cloud, Cigref, novembre 2021
[4] Ibid

Les modèles IaaS et PaaS se distinguent assez fortement du modèle SaaS. Les clients, les usages et les modèles d'affaires diffèrent. Les services proposés par les fournisseurs selon les modèles IaaS et PaaS sont principalement destinés à des professionnels de l'informatique pour leur permettre de construire des solutions pour leur propre usage interne ou externe. **Dans une moindre mesure**, ces services sont aussi proposés sur une base de consommation à l'usage. En revanche, le modèle SaaS est distribué à **tout type de professionnels, composé essentiellement de clients finaux de logiciels**, sur la base d'un abonnement.

Le SaaS correspond au modèle le plus externalisé. Il permet à l'utilisateur d'accéder directement à des applications, gérées intégralement par le fournisseur, depuis tout appareil connecté.

A ces trois modèles, on peut ajouter un quatrième modèle celui du **FAAS** (Function-as-a-Service) : ce service « *permet aux développeurs de créer, de calculer, d'exécuter et de gérer des paquets d'application en tant que fonctions, sans avoir à assurer la maintenance de leur propre infrastructure. Le FAAS est un modèle d'exécution basé sur les événements qui s'exécute dans des conteneurs stateless. Les fonctions proposées « as-a-Service » gèrent les états et la logique côté serveur grâce à des services assurés par un fournisseur* ». C'est souvent associé à ce que l'on appelle le « *computing serverless* » (informatique sans serveur).

# Focus : Le Saas, mode privilégié de déploiement des logiciels



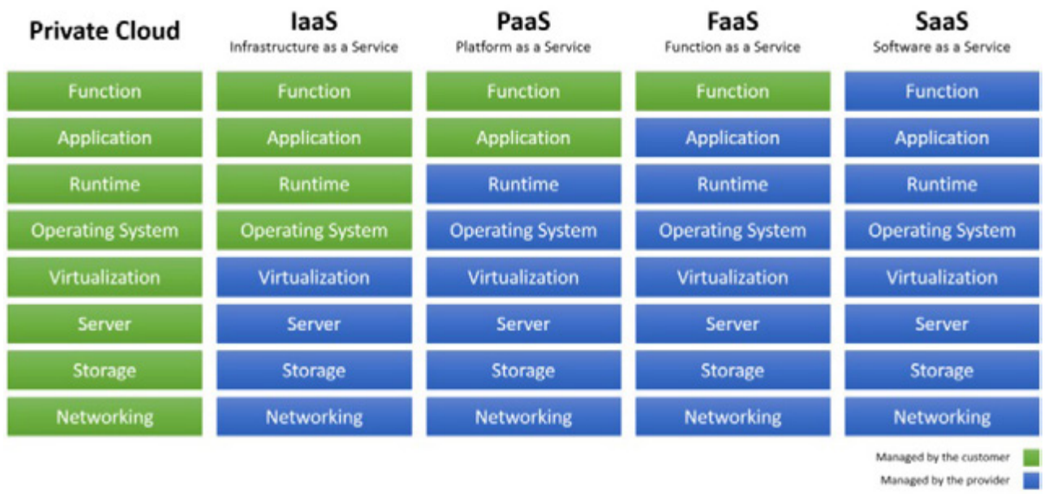

*Source : PAC - Numeum*

Le SaaS est aujourd'hui le mode d'accès aux logiciels le plus plébiscité par les clients. Ainsi, près de 8 nouveaux projets de déploiement de logiciels sur 10 se réalisent en SaaS aujourd'hui contre 2 on-premise.

Les principales caractéristiques du SaaS sont les suivantes :
• Logiciel : il est conçu pour être accessible via Internet et hébergés sur les infrastructures d'un fournisseur de cloud.
• Tarification : la partie licence et la partie hébergement sont confondues si bien qu'il n'est pas possible de différencier frais d'hébergement et coûts de licence.
• Flexibilité : il n'y a pas ou peu de customisation des applications en dehors d'une configuration minimale.

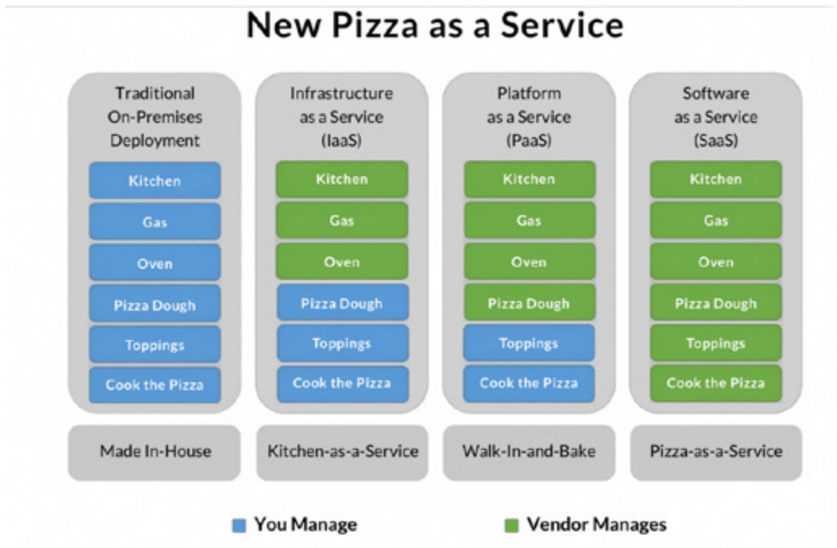
# La répartition des responsabilités entre le fournisseur et le client

L'utilisation du cloud revient à une responsabilité partagée entre le fournisseur de services cloud et le client dans l'exécution des tâches - telles que la gestion des incidents et opérations, des identités et des accès, la sécurité, le contrôle en conformité etc. Par conséquent, le choix du cloud aura un impact sur la répartition des responsabilités entre le fournisseur de cloud et le client Il est alors primordial de définir précisément et contractuellement cette répartition afin de gagner en efficacité et d'éviter tout litige en cas d'accident. Les schéma 1 et schéma 2 soulignent bien ces aspects.




Severless architecture function as a service , Tanmay Terkhedkar, 2019

De manière plus ludique, cette analogie avec une pizzeria pourra faciliter votre compréhension des services de cloud computing :




New Pizza as a service, Caleb Munyasya,2021



# Le cloud public, un modèle en croissance pour la fourniture d'infrastructures

Le cloud public permet le partage des ressources informatiques et l'optimisation du fait de la mutualisation par tous les clients qui souhaitent des services similaires. Les serveurs sous-jacents hébergeant les applications et données sont partagés entre plusieurs clients, on parle d'isolation logique entre les services des clients. A contrario, le cloud privé permet de mettre à disposition des services d'hébergement s'appuyant sur des ressources et serveurs dédiées pour chaque client. On parle dans ce cas d'isolation physique entre les services des clients.

> **Cloud privé :** cette expression regroupe, selon le NIST, des produits et/ou services pour lesquels « *une infrastructure cloud est mise à disposition d'une seule organisation – pouvant comprendre plusieurs consommateurs (par exemple, des unités commerciales)–, pour son utilisation exclusive. L'infrastructure peut être détenue, gérée et opérée par l'organisation, par un tiers ou par une combinaison des deux et elle peut être située dans ou hors des locaux de l'organisation* ».
>
> **Cloud public :** cette expression regroupe, selon le NIST, des produits et/ou services pour lesquels « *l'infrastructure cloud est mise à disposition pour une utilisation ouverte au grand public. L'infrastructure peut être détenue, gérée et exploitée par une entreprise, un établissement universitaire ou une organisation gouvernementale, ou une combinaison de ceux-ci. Elle est située dans les locaux du fournisseur de cloud* ».
>
> **Cloud hybride** cette expression regroupe, selon le NIST, des produits et/ou services pour lesquels « *l'infrastructure est une combinaison de deux ou plusieurs infrastructures cloud distinctes (privées, communautaires ou publiques), qui restent des entités autonomes mais qui sont liées entre elles par une technologie normalisée ou propriétaire permettant la portabilité des données et des applications* ».

Les usages du cloud public sont en très forte croissance avec une progression du chiffre d'affaires engendrée en France par ce type de services estimée à 35 % entre 2020 et 2021. Le cloud privé est lui porté par l'usage des solutions « Bare Metal » où le client conserve un contrôle total de ses serveurs déportés dans le cloud de leur fournisseur. Une autre alternative : les services « Hosted Private Cloud » permettant de faciliter les migrations d'une infrastructure on-premise vers un cloud externalisé sans modifications en profondeurs des applications des clients, tout en apportant une isolation plus poussée que dans le cas d'une hébergement cloud public. Le cloud hybride est quant à lui plébiscité par les organisations souhaitant conserver un haut niveau de maitrise de leurs applications les plus critiques dans un cloud privé, tout en hébergeant dans le cloud public leurs d'autres applications.

# II. Mode de déploiement du cloud : le multi-cloud comme clé de la liberté des choix technologiques

Selon une étude Gartner[5] de 2020 réalisée auprès des utilisateurs du cloud public, 81 % des répondants ont indiqué utiliser les services d'au moins deux fournisseurs.

> **Multi-cloud :** Le multi-cloud est un terme utilisé par les acteurs du secteur pour désigner l'utilisation parallèle des services de plusieurs fournisseurs de services cloud par une même entreprise. Cela peut concerner à la fois le recours à plusieurs fournisseurs pour leurs services IaaS, PaaS ou les deux à la fois (voire SaaS, selon les définitions).

Ce mode de déploiement est utilisée par les organisations, la plupart du temps dans le cadre d'une stratégie de maîtrise des risques. Utiliser plusieurs opérateurs à la fois permet de répartir son usage sur plusieurs fournisseurs, assurer la continuité d'activité en cas d'incident chez l'un des fournisseurs et limiter les dépendances via à vis de ses fournisseurs de cloud.

Malgré l'attente vis-à-vis d'un recours plus important au multicloud, certains freins existent et qui ont notamment été étudié par l'Autorité de la concurrance, qui a publié un Avis sur le fonctionnement concurrentiel de l'informatique en nuage (« cloud ») publié le 29 juin 2023. Il y est souligné en effet que le multicloud n'est pas aujourd'hui une réalité : « *même dans le cas de ces stratégies de multi-cloud, les entreprises ne recourent généralement qu'à un seul fournisseur de services cloud par charge de travail. Ces stratégies multi-cloud se retrouvent ainsi plus fréquemment au sein des grandes entreprises qui ont des besoins internes diversifiés et relativement indépendants et pourront choisir de les répartir entre différents fournisseurs* ». L'avis analyse finement les freins liés au développement du multi-cloud, qui ont pour effet de dissuader les clients de recourir en parallèle d'un service à des fournisseurs de services cloud alternatifs, pour l'exécution d'autres services. A titre d'exemple, d'un point de vue technique, cela se traduit notamment au travers de freins à l'interopérabilité et d'un point de vue économique sur la facturation de frais de sortie.

En décembre 2022, Numeum a interrogé ses adhérents autour de la question de la confiance numérique dans le contexte des offres de cloud. Ce questionnaire[6], qui a réuni plus de 420 répondants a également permis de noter un intérêt grandissant à l'égard des stratégies multi cloud. Cette considération s'inscrit dans la lignée de la position de **Numeum de défendre la question centrale de la liberté de choix technologique pour l'utilisateur, en fonction de ses besoins.**

Pour maintenir la liberté de choix dans le temps, la possibilité de changer de fournisseur de cloud doit être facilitée. Le questionnaire de Numeum mentionné ci-dessus a soulevé que la liberté du choix technologique est actuellement une préoccupation majeure, exprimée davantage dans les grands groupes (74% dont 34% très important) que les ETI et les TPE/PME. Les grands groupes possèdent une plus forte capacité à choisir leurs technologies par connaissance et expertise des solutions proposées mais également par coûts et investissements possibles.

Les conditions nécessaires citées par les clients pour atteindre une véritable liberté de choix d'une solution cloud est la **réversibilité effective des offres** pour 70% des répondants. En seconde position, l'**interopérabilité** entre les différents environnements sont évoqués et jugés importants par les clients dans le choix d'une solution cloud pour 68%. Ainsi de façon logique, les garanties de réversibilité sont des exigences au moment de la souscription exprimées systématiquement ou régulièrement dans 77% des cas par les clients et sur lesquelles les entreprises du numérique apportent des réponses (96% des entreprises dont 59% sur l'ensemble des services). La portabilité est plus rarement exigée avec seulement 35% des clients qui la demandent systématiquement à régulièrement. Pourtant 77% entreprises du numérique peuvent proposer cette garantie sur une partie ou l'ensemble des services fournis.

**TOP 5**
**des actions pour mieux répondre aux besoins des clients :**

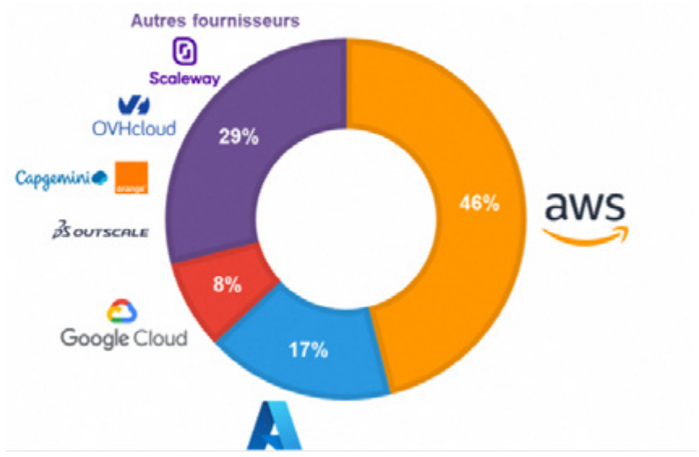
1. Adopte une stratégie modulaire et de micro-services
2. Adopter une stratégie multicloud
3. Elever les normes et standards garantissant cette liberté de choix
4. Favoriser le recours à des tiers de confiance
5. Se tourner vers les offres visant la qualification Sec Num Cloud

Source : Souveraineté Numérique - synthèse des résultats de l'étude - mars 2023



# III. Une réflexion plus transverse sur la confiance numérique

Le marché français du cloud computing reste largement capté par des entreprises américaines.




Source : Markess by Exaegis, 2021

Dans son analyse « MarketScape Worldide Public Cloud Infrastructure as a Service, 2022 », IDC n'a sélectionné qu'un seul fournisseur européen dans son comparatif où figurent aussi trois fournisseurs chinois, tous les autres étants de fournisseurs américains.


**Dans ce contexte, l'Union européenne cherche à développer son écosystème cloud et préserver sa souveraineté technologique.**

De nombreuses initiatives ou projets ont émergé dans ces dernières années. Au niveau européen, c'est notamment le cas du projet Gaia-X lancé en juin 2020 par la France et l'Allemagne. L'ambition de Gaia-X est de faciliter la coopération entre les acteurs souhaitant construire la nouvelle génération d'architecture cloud : distribuée, ouverte et transparente où les utilisateurs sont en mesure de faire des choix éclairés quant à la confidentialité, la sécurité et la souveraineté de leurs données.

En France, la notion de « cloud de confiance » a été intégrée au cœur de la stratégie cloud[7] de l'Etat, mettant au centre des enjeux le développement d'un cloud de confiance. L'objectif principal de la stratégie cloud vise *« à écarter les failles techniques et juridiques induites par l'extraterritorialité des grands fournisseurs du marché qui ne sont pas soumis aux réglementations françaises. Pour maintenir leur prestation en France, ces entités devront donc se conformer aux exigences du visa de sécurité SecNumCloud[8] de l'ANSSI (agence nationale de la sécurité des systèmes d'information). Concrètement, la France a lancé le label « cloud de confiance »* qui clarifie ce qui est attendu pour atteindre un niveau de protection élevé des données d'une sensibilité particulière de l'administration. L'objectif vise à protéger les données des entreprises, des administrations et des citoyens tout en assurant la performance des solutions cloud.  Les critères sont les suivants :

- *respecter un référentiel  technique édicté par l'ANSSI,*
- *localiser leurs infrastructures en Europe,*
- *faciliter les échanges avec les prestataires cloud européens.».*

**La stratégie cloud de l'Etat français, ainsi que d'autres réflexion, soulèvent la question de la protection des données sensibles.** Si certaines catégories de données sensibles bénéficient de protections spécifiques (protection du secret de la défense nationale, protection du secret des affaires, protection du secret de la correspondance avec les avocats, les données à caractère personnel etc.), l'essentiel des données est régi par le droit commun. Beaucoup de règlementations et documents nationaux et internationaux en cours ont un impact sur le régime de ces données dans le contexte du cloud.

Exemples d'initiatives auxquelles se référer :

- **Au niveau national :**
  - o Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
  - o Circulaire de la Première ministre datée du 31 mai 2023 qui actualise la doctrine «cloud au centre» et définit la notion de données d'une sensibilité particulière concernées par cette dernière
  - o Qualification SecNumCloud : ensemble de règles de sécurité garantissant un haut niveau d'exigence tant du point de vue technique, qu'opérationnel ou juridique
  - o Certification HDS visant à renforcer la protection des données de Santé à caractère personnel.
  - o (non contraignant) : Guide Medef/Afep d'identification des données sensibles à destination des entreprises

- **Au niveau européen :**
  - o Règlement Général sur la Protection des Données
  - o Règlement européen sur la donnée ou « Data Act » qui acte un principe de transparence l'information des fournisseurs de cloud sur la juridiction applicable à leurs services
  - o Standards de sécurité dans le cloud mis en place par différents pays européens comme le Catalogue des Critères de Conformité du Cloud Computing (C5) de l'Office fédéral allemand de la sécurité des technologies de l'information, la qualification AgID italienne ou la certification ENS espagnole.
  - o (non réglementaire) CSPCERT (The European Cloud Service Provider Certification Working Group)
  - o A venir : (non réglementaire) Cloud Rulebook (en cours de préparation - publication fin 2023/ début 2024)
  - o A venir : le schéma de certification Cloud européen EUCS, porté par l'ENISA

- **Au niveau international**
  - o ISO/IEC 17788, ISO/IEC 27701, ISO/IEC 27001, ISO/IEC 27017, ISO 27018, ISO/IEC 17000
  - o Contrôles système et d'organisation (SOC)
  - o Payment Card Industry Data Security Standard (PCI DSS)
  - o TISAX, Trusted Information Security Assessment Exchange (TISAX)



En fonction de la nature des données et des secteurs en jeu, il peut être nécessaire de se tourner vers un certain type de fournisseur, ce qui suppose que ces derniers soient transparents sur leurs qualifications en matière de cybersécurité et sur les juridictions applicables à leurs services.

Les notions de confiance et de souveraineté sont dès lors de plus en plus présentes dans le débat public. La prédominance de ces notions démontrent un changement de paradigme. L'apport de Numeum pour renforcer la confiance dans le numérique ne vise pas tant à s'immiscer dans la réflexion relative à la confiance qui relève des pouvoirs publics, mais de **rayonner par son exemplarité et sa proactivité sur l'ensemble du cycle de vie de la donnée.**

Aujourd'hui, il n'existe pas de définition qui fasse consensus sur ces notions. Nous avons proposé aux adhérents de Numeum de nous partager les thèmes clés qui se rattachent à ces termes afin d'identifier les tendances qui se dégagent.

# IV. Analyse PESTEL

**Dans l'objectif de mieux comprendre les changements de paradigme générés par cette technologie, voici une analyse PESTEL présentant brièvement les principaux enjeux et débats futurs autour du Cloud computing.**

## P. Politique :

Le Cloud étant un outil fondamental de puissance économique, technologique ou d'innovation, l'Union européenne cherche à développer son écosystème. Cette dynamique se traduit notamment par l'émergence de la notion de « cloud souverain » et par différentes initiatives visant à promouvoir cette technologie, assurer son développement et proposer des solutions conformes aux règles de l'Union.

Le projet Gaia-X a ainsi été lancé en juin 2020 par la France et l'Allemagne. Son ambition est de faciliter la coopération entre les acteurs souhaitant construire la nouvelle génération d'architecture cloud : distribuée, ouverte et transparente, où les utilisateurs sont en mesure de faire des choix éclairés quant à la confidentialité, la sécurité et la souveraineté de leurs données.

Le cloud de confiance est un terme plus récent, introduit dans le cadre de la stratégie « cloud » de l'Etat français, qui a alors développé un label « cloud de confiance ». Sa finalité est d'assurer la protection des données des entreprises, des administrations et des citoyens, sans pour autant affaiblir la qualité du service.

L'Autorité de la concurrence a rendu en juin 2023 un avis[9] portant sur le fonctionnement concurrentiel de l'informatique en nuage (« cloud »). L'Autorité propose une grille d'analyse présentant de possibles marchés pertinents dans ce secteur et analyse différentes pratiques mises en œuvre, ou susceptibles de l'être, pouvant restreindre la concurrence.

Il existe enfin un vif débat au sein de l'Union européenne relatif à l'extra-territorialité des lois étrangères, notamment dans le cadre de l'élaboration du schéma européen de cybersécurité des services cloud.

## E. Économique :

Le cloud computing est considéré comme un des principaux leviers de croissance du marché des services numériques en 2023.

Ainsi, le cabinet Markess by Exaegis estime que le marché français du cloud devrait atteindre les 27 milliards d'euros en 2025. Au niveau européen, ce chiffre devrait franchir la barre des 500 milliards d'euros d'ici 2030 et entrainer la création de plus de 550 000 emplois. On estime d'ailleurs qu'environ la moitié de l'économie européenne repose sur le cloud ou utilise celui-ci.

Le marché du cloud demeure très concentré puisque les entreprises américaines et chinoises restent majoritaires au niveau mondial. En outre, quelques « hyperscalers » concentrent l'essentiel du marché en volume et en croissance au cours des dernières années. La France ne fait pas figure d'exception puisqu'à l'image du marché mondial, son marché demeure largement capté par quelques entreprises américaines.

Cependant, les ambitions européennes en matière de numérisation sont à mettre en adéquation avec ceux du « Green Deal ». Tout l'enjeu résidera ainsi à opérer une juste conciliation entre la forte croissance de l'économie numérique et les nécessaires objectifs de transition écologique. Cette conciliation nécessitera l'instauration de politiques, stratégies, normes et innovations adaptées.

[9] Avis de l'autorité de la concurrence sur le fonctionnement concurrentiel du secteur du cloud, 29 juin 2023



## S. Socio-culturel :

Le fort développement du *cloud computing* soulève également un important besoin en recrutement.

Cependant, le développement de formation répondant aux besoins du terrain s'avère particulièrement complexe car les technologies évoluent très rapidement. Pour résoudre cette difficulté, Numeum a participé activement à la publication d'une étude prospective portée par l'Opiiec sur les besoins en compétences, emplois et formations en matière de Cloud computing et Data en France. Celle-ci sera publiée en septembre 2024. On peut également remarquer que les compétences requises pour les emplois du secteurs sont très variées. A titre d'exemple, on observe un besoin grandissant autour des enjeux de transition écologique et énergétique en matière de *cloud computing*, ce qui impacte directement les besoins métiers et compétences du secteur.

Le cloud public demeure particulièrement plébiscité avec une croissance du chiffre d'affaires de 35 % entre 2020 et 2021, contre 5,7 % pour le cloud privé. Il existe ainsi une tendance croissante à l'adoption du cloud public.

Le SaaS est aujourd'hui le mode d'accès aux logiciels le plus apprécié, avec près de 8 nouveaux projets sur 10 se réalisant en SaaS.

## T. Technologique :

Le cloud computing est à la base de tout nouveau service numérique et des nouvelles technologies numériques (IA, quantique). Plusieurs enjeux émergent ainsi :
- L'évolution rapide des technologies du *cloud computing*.
- Définition et explications autour du *cloud computing* par le NIST.
- Les différentes offres de cloud : public, privé et hybride.
- Les trois grandes catégories de services cloud : IaaS, PaaS, et SaaS.
- L'enjeu central de la liberté de choix technologique.

## E. Environnemental :

Si la consommation énergétique des datacenters est un enjeu pour les fournisseurs de cloud, l'impact de cette technologie sur l'environnement est loin d'être uniquement négatif. Ces services s'inscrivent notamment au service de l'optimisation environnementale des autres secteurs. En effet, recourir au cloud, permet tout d'abord de ne plus recourir aux serveurs sur site, qui sont très énergivores. Les applications du cloud consomment moins d'infrastructure, d'espace physique et d'énergie par utilisateur.

Toutefois, à l'image du numérique, le cloud a un impact environnemental non négligeable. « L'étude ADEME – ARCEP sur l'empreinte environnementale du numérique en 2020, 2030 et 2050 » se focalise sur quatre indicateurs pour quantifier l'impact environnemental du numérique : la taille du parc des équipements ; la durée de vie des équipements ; la consommation énergétique des équipements et outils numériques ; la quantité de données qui transitent via les réseaux et infrastructures numériques. Ces indicateurs sont pertinents dans le domaine du cloud également.

En matière de cloud, l'accent est souvent mis sur les data centers, qui sont nécessaires pour le stockage. La feuille de route décarbonation de la filière numérique propose six fiches sur les sujets data et cloud : Efficacité énergétique – Refroidissement et fluides frigorigènes ; Efficacité énergétique – Urbanisation des salles ; Économie circulaire ; Efficacité énergétique – Récupération de chaleur fatale ; Outils et méthodologie en matière d'information environnementale à destination des clients ; Énergies renouvelables.

Notons également que les indicateurs les plus utilisés sur en matière de data centers sont :
- **PUE – Power usage efficiency :** mesure de l'efficacité de l'utilisation de l'énergie dans les datacenters
- **WUE – Water usage efficiency :** mesure de l'efficacité de l'utilisation de l'eau dans le datacenter à partir de la quantité d'eau utilisée pour le refroidissement et d'autres besoins opérationnels.
- **CUE – Carbon usage effectiveness :** mesure des émissions de carbone d'un datacenter.

Le critère de l'impact environnemental sera sans aucun doute un critère de compétitivité dans les prochaines années. D'autant plus que pour le secteur du numérique la rentabilité économique va de pair avec la rentabilité écologique. A titre d'exemple, la consommation énergétique représente jusqu'à 50% du coût global de fonctionnement d'un datacenter sur 10 ans. En matière d'économie d'énergie, l'intérêt est donc environnemental mais aussi financier pour les entreprises.

L'avenir du cloud se situe dans l'optimisation de l'ensemble de la chaine globale et ne se limite pas aux enjeux relatifs aux data centers. Il est nécessaire de lancer une réflexion sur des indicateurs qui prennent en compte la granularité des services

proposés, y compris en ce que le cloud apporte comme bénéfices aux autres secteurs.

Enfin, se pose ensuite la question du passage à l'échelle de réflexion de l'impact environnemental du cloud afin qu'elle bénéficie à l'ensemble du cloud.

### L. Légal :

Les débats sur la confiance dans l'économie numérique et l'équité concurrentielle au sein du marché européen ont des implications légales concernant la protection des données et la conformité des services :
- Les législations sur la protection des données à caractère personnel.
- Les législations relatives à la cybersécurité des organisations et leurs déclinaisons sectorielles
- Les législations relatives à la donnée (notamment le Data Act, le DGA…)
- La localisation et le traitement des données hébergées qui impactent les lois applicables.
- L'immunité au regard de l'extra-territorialité des lois étrangères.



# V. Les clés pour garder le contrôle de sa stratégie cloud

Les principaux avantages et motivations à développer une stratégie cloud :

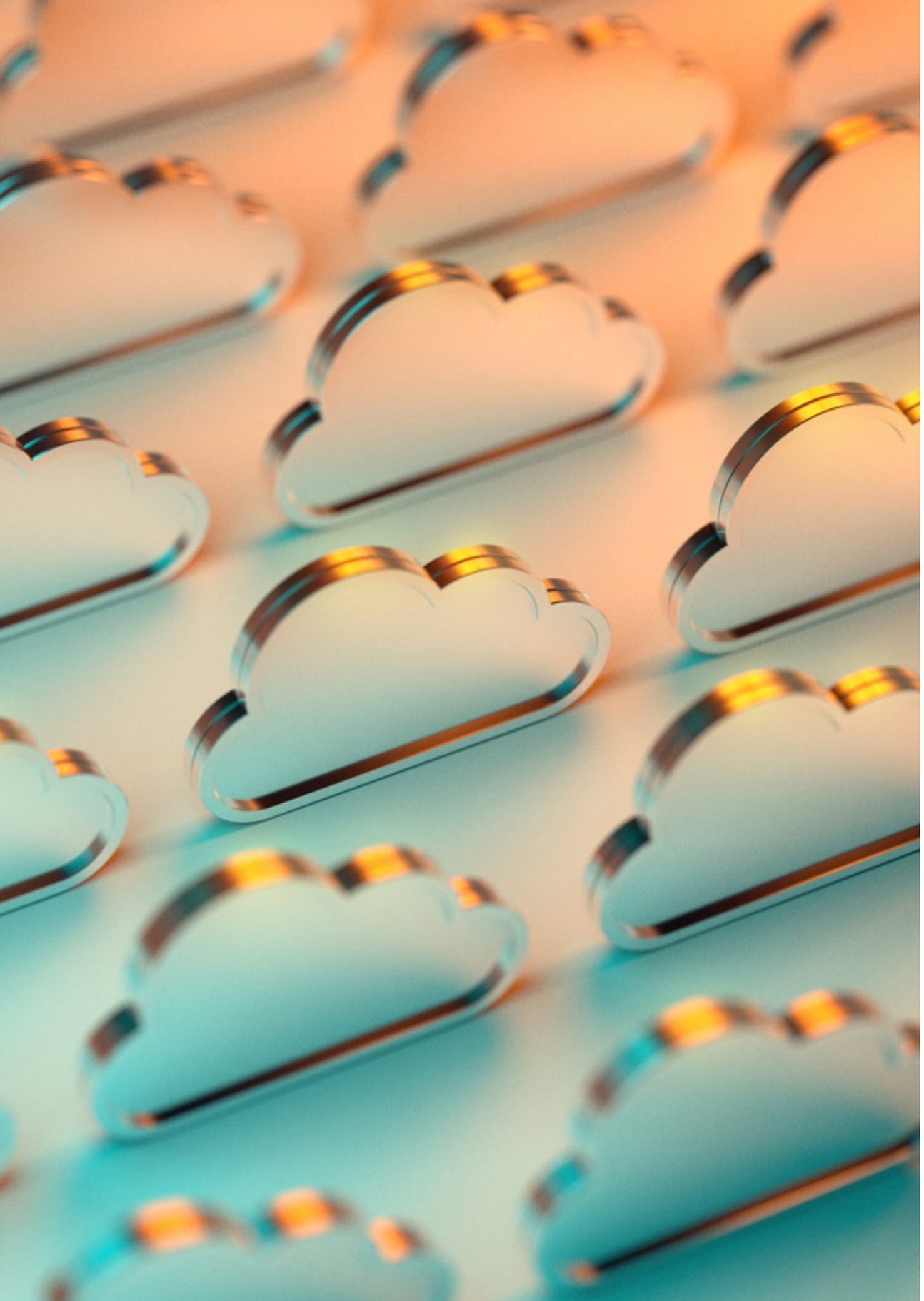
- **Gagner en agilité et flexibilité** grâce à des services disponible à la demande, déployés en quelques secondes ou quelques minutes et adaptés aux approches de développement modernes comme le DevOps, le CI/CD ou encore les micro-services.
- **Harmoniser les infrastructures et réduire les coûts** avec des fournisseurs cloud bénéficiant d'un effet mutualisation et d'économies d'échelle. Les utilisateurs peuvent ajuster rapidement la consommation de leurs ressources en fonction de leurs besoins.
- **Utiliser des serveurs informatiques à distance** pour stocker des données et accéder à des logiciels ou mobiliser de la puissance de calcul ce qui permet de monter en charge rapidement sans investissement dédié. Cela permet de **centraliser le coût, mais également l'impact carbone** lié aux matériaux, en réduisant la surface des data centers.
- Le cloud permet d'aider les organisations de **renforcer de leur protection face aux attaques informatiques.** Cela explique également que la migration vers le cloud soit particulièrement importante dans les secteurs les plus régulés et dans lesquels la sécurité des données est une priorité absolue, comme les services financiers ou la santé.
- **Améliorer la maîtrise et la sécurité des données.** Les fournisseurs de cloud mutualisent à grande échelle les investissements dans la sécurité, dans la résilience et dans une infrastructure distribuée géographiquement, qui surpassent les ressources qu'une organisation pourrait mobiliser individuellement pour des solutions sur sites, en particulier pour des organisations de petite taille.
- **Réduire des coûts de maintenance des infrastructures** informatiques au travers de la mutualisation des ressources.
- **Gérer les serveurs, le réseau, le stockage, les sauvegardes, le système d'exploitation, les bases de données et les applications via un fournisseur,** ce qui permet aux entreprises de concentrer ses ressources sur la valeur ajoutée de leurs services plutôt que la gestion des infrastructures.

Au-delà de cette proposition de valeur, le développement d'une stratégie cloud crée nécessairement une dépendance vis-à-vis du fournisseur, risque que l'utilisateur est en mesure d'atténuer en s'appuyant sur des technologies ouvertes et réversibles. Le ratio risques/ bénéfices ne peut être analysé qu'au travers d'une étude globale qui ne peut se faire qu'au cas par cas en vue de la manière dont le service répond à un usage précis. Pour rappel, une stratégie cloud ne vise pas nécessairement toutes les activités d'une entreprise, cette stratégie s'inscrit pour répondre à un besoin particulier, qui ne peut viser qu'une partie de l'entreprise.

Voici quelques critères pour permettre à l'utilisateur de répondre à la finalité recherchée tout en gardant le contrôle :

- **S'assurer de la compréhension et de la maturité interne ( équipe et direction)**
- **Anticiper l'investissemnt nécessaire** (temps, moyens, ressources) pour obtenir les gains
- **S'assurer de la visibilité des tarifs de manière à anticiper les coûts**
- **Tenir compte du déséquilibre dans les relations** avec certains fournisseurs dont l'organisation peut être dépendante
- **S'assurer d'avoir une vision complète des systèmes et des données** pour protéger l'organisation
- **Veiller à la traçabilité des actions** et des acteurs en charge des différentes taches, notamment entre fournisseur et client
- **Prendre en compte les exigences réglementaires** (secteurs régulés, OIV ou OSE en particulier), notamment concernant l'exposition aux lois extraterritoriales lors du choix d'un fournisseur international
- **Intégrer l'impact environnemental du cloud (positif et négatif)** dans l'impact environnemental de l'entreprise

A noter, l'examen des vigilances ne vise pas seulement le manque de protection de la part des fournisseurs du cloud. La manière dont les services sont utilisés par les clients est un élément essentiel. Ainsi, les infrastructures choisies et la répartition des rôles entre les fournisseurs de cloud et les clients sont des éléments essentiels pour renforcer la sécurité.



**Remerciements :**
Numeum tient à remercier particulièrement les membres de la Commission Intelligence Artificielle de Numeum, Berger-Levrault, Naelan, Data LegalTech, Visiativ, Synox, Cegid, Wavestone, Oracle, Sfeir, Wenvision, Sopra Steria, Ethical AI, le Hub France IA et le Cigref. Nous souhaitons également souligner le soutien et l'aide précieuse de M.Charles Depaepe, sans qui ce livrable n'aurait pas pu voir le jour.

**Ours :**
Directrice de la publication
Véronique Torner

Conception et coordination
Katya Lainé, Atef Ben Othman, Olivier Robillart

Rédaction
Olivier Robillart

Conseils techniques
Katya Lainé, Charles Depaepe

Graphisme
Laura Pineau

Photographies
crédit IStock

Réalisé et édité par
Numeum, 22/28 rue Joubert, 75009 Paris, 2023

numeum.fr