

## Résumé de l'avis n° 23-A-08 du 29 juin 2023 portant sur le fonctionnement concurrentiel de l'informatique en nuage (« cloud »)

L'informatique en nuage, ou « *cloud* », constitue une des évolutions technologiques au cœur de la numérisation de l'économie. Le *cloud* comprend l'ensemble des services mutualisés, accessibles via internet, à la demande, payés à l'usage et, par extension, certaines des infrastructures sous-jacentes (centres de données notamment). En comparaison avec l'informatique traditionnelle, le *cloud* offre de multiples avantages économiques pour les entreprises. Il permet notamment de nouvelles organisations du travail, sur la base de ressources partagées et accessibles à distance. Ces caractéristiques peuvent constituer des sources de gains de productivité pour les entreprises et de création de valeur pour l'économie.

Au regard du fonctionnement des marchés, de leur importance pour l'économie et des potentiels avantages concurrentiels de certains acteurs, il apparaît primordial qu'une concurrence par les mérites s'exprime pleinement dans le secteur du *cloud*.

Au-delà de défaillances de marché qui peuvent être identifiées et potentiellement réglées par les initiatives réglementaires en cours, l'Autorité a analysé sous forme de scénarios plusieurs risques susceptibles de soulever des problématiques concurrentielles. Ces risques peuvent être de nature transversale, dans la mesure où ils affectent globalement la concurrence du secteur (c'est le cas par exemple des crédits *cloud* ou des frais de sortie ou « *egress fees* »). D'autres s'inscrivent davantage dans des scénarios spécifiques lors de la primo-migration vers le *cloud*, en cas de migration d'un fournisseur de services *cloud* à un autre. Le dernier scénario examine les risques liés aux freins à l'expansion des concurrents des *hyperscalers*. Pour faire face à ces risques, l'Autorité rappelle qu'elle dispose de plusieurs outils efficaces et rapides pour agir et protéger la concurrence.

### Les services *cloud*

Le *cloud public*<sup>1</sup> (ou *hybride*<sup>2</sup>), sur lequel se concentre cet avis, correspond à des offres commerciales permettant au client d'accéder directement à un ensemble de services. On

---

<sup>1</sup> *Cloud public* : cette expression regroupe, selon le National Institute of Standards and Technology (« 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* ». Par contraste, le *cloud privé* 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* ».

<sup>2</sup> *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,*

distingue généralement trois grandes catégories de services *cloud*, nommées IaaS, PaaS et SaaS, qui correspondent chacune à différents partages de responsabilité entre le fournisseur de services *cloud* et l'entreprise cliente.

- l'IaaS (« *Infrastructure as a Service* », ou services d'infrastructure) correspond au modèle le moins externalisé, dans lequel le fournisseur met à disposition de l'utilisateur les infrastructures informatiques, notamment des serveurs ou du stockage ;
- le PaaS (« *Platform as a Service* », ou services de plateforme) constitue un modèle intermédiaire. Il fournit un environnement permettant aux clients de bénéficier de logiciels et d'outils pour développer leurs applications sans avoir à créer ni entretenir l'infrastructure ou la plateforme associée au processus ;
- le SaaS (« *Software as a Service* », ou services de logiciels) 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.

Les modèles IaaS et PaaS se distinguent du modèle SaaS par leurs clients, leurs usages et leurs modèles d'affaires. En effet, les services appartenant aux modèles IaaS et PaaS sont principalement destinés à des professionnels de l'informatique pour construire des solutions pour leurs propres usages internes et/ou externes alors que les services SaaS concernent toutes les catégories d'utilisateurs.

Les services IaaS sont les plus standardisés des services *cloud*. Ils représentent une part réduite, en nombre, de l'ensemble des services du *cloud* public mais la plus grande part de l'activité et des revenus liés aux services *cloud*. Les services proposés sur le PaaS sont quant à eux très variés et plus différenciés.

### L'usage des services *cloud*

Les clients professionnels ayant aujourd'hui recours à des services *cloud* sont issus de l'ensemble des secteurs d'activité. Toutefois, certains clients font face à des contraintes réglementaires pouvant affecter leur recours au *cloud* public. C'est notamment le cas des acteurs du secteur public, des services financiers ou du secteur de la santé ainsi que les opérateurs de services essentiels (OSE) et d'importance vitale (OIV).

Parmi l'ensemble de ces clients, deux catégories d'acteurs peuvent en particulier être distingués en fonction de leur stade d'adoption du *cloud* :

- Les entreprises ayant fait le choix de recourir à ces services pour certaines ou l'ensemble de leurs charges de travail, préalablement réalisées depuis une infrastructure sur site ;
- Les entreprises dites « *cloud native* », relativement jeunes, qui ont construit directement leurs ressources informatiques dans le *cloud*. Elles utilisent les services *cloud* depuis leur création et ont conçu directement leurs charges de travail en recourant à ces services. Ces entreprises n'ont donc pas à gérer la migration de leur système informatique vers le *cloud*.

---

*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 ».*

La migration vers le *cloud* concerne des entreprises de toutes tailles (des TPE aux grands groupes) ainsi que les entités publiques, même si les critères sur lesquels repose le choix de fournisseur de services *cloud* tendent à varier selon la catégorie de client.

En France, le secteur du *cloud* devrait connaître une croissance annuelle d'environ 14 % par an pour atteindre 27 milliards d'euros en 2025. Toutefois, l'adoption des services *cloud* en France connaît un certain retard, notamment en raison d'une migration des PME et TPE plus lente que dans le reste de l'Europe au cours des dernières années.

Parmi les entreprises françaises utilisatrices de services *cloud* (SaaS inclus) en 2021, les principaux usages concernent le stockage de documents (76 %) et le courrier électronique (67 %).

Enfin, les entreprises ne recourent généralement qu'à un seul fournisseur de services *cloud* pour une charge de travail donnée. Cette absence de multi-domiciliation (dite « multi-homing ») provient des investissements nécessaires en temps, en argent et en technologie, de la structure tarifaire adoptée par les fournisseurs et de la complexité de tels projets, par exemple pour assurer le nécessaire respect de normes réglementaires. Les entreprises peuvent aussi faire appel à plusieurs fournisseurs de services *cloud* (modèle dit « multi-cloud ») pour des charges de travail distinctes.

### Les acteurs de la chaîne de valeur du *cloud*

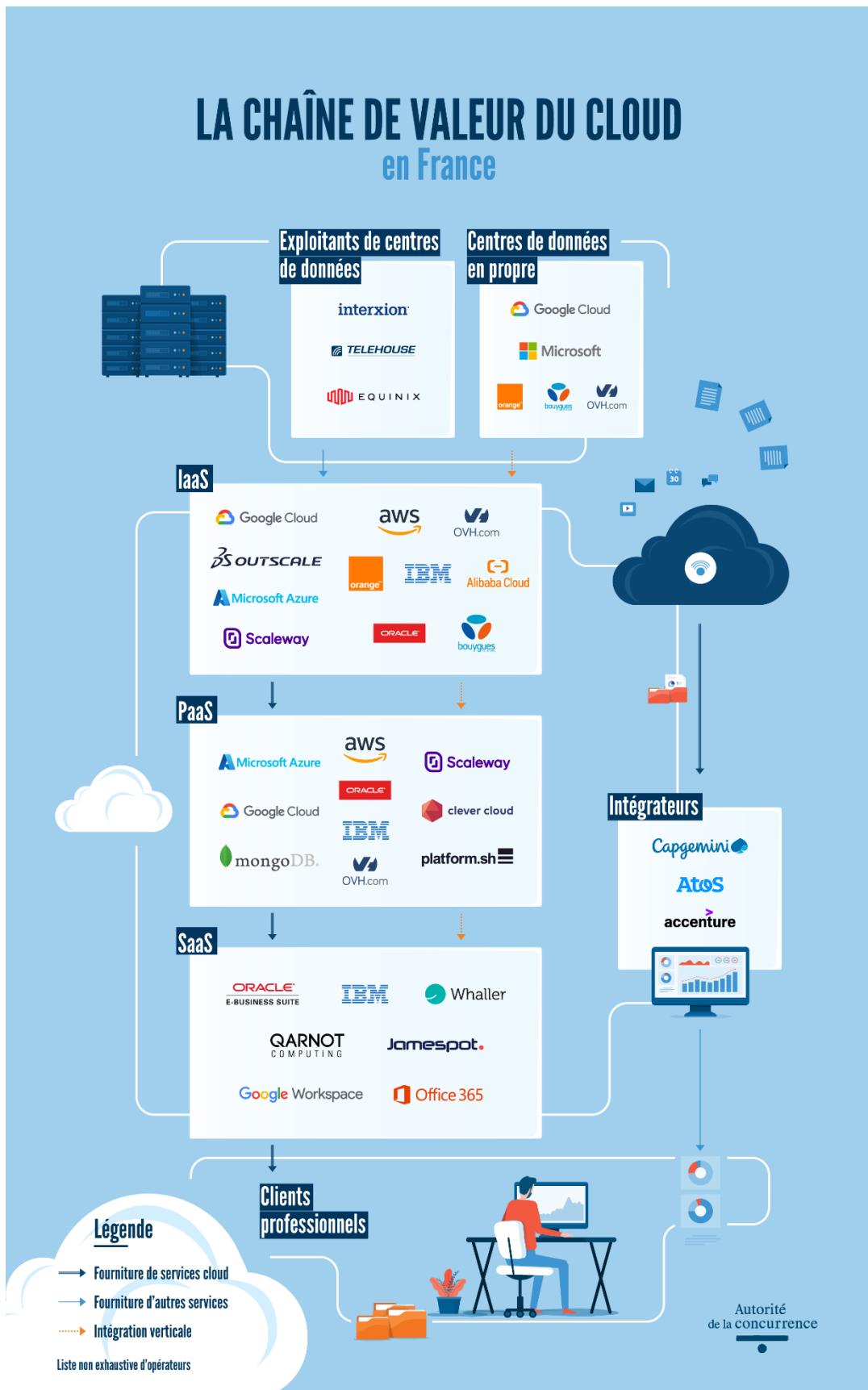
Les acteurs présents sont :

- les exploitants de centres de données, qui construisent et exploitent ces infrastructures, nécessaires ensuite à la fourniture de services *cloud* ;
- les fournisseurs présents dans le secteur du numérique avant leur entrée dans le secteur du *cloud*, tels que les grands acteurs du numérique comme Amazon, Alphabet (Google) et Microsoft qui disposent de capacités massives de stockage et de calcul (dits « hyperscalers »), des entreprises issues du secteur des logiciels et systèmes d'information d'entreprises ou des opérateurs de communications électroniques ;
- les fournisseurs actifs seulement dans le *cloud*, dits « pure players », dans la mesure où leurs activités concernent principalement le *cloud*, et où ils ne sont pas ou peu présents sur d'autres marchés. C'est le cas par exemple de 3DS Outscale, OVHcloud ou Scaleway ;
- les fournisseurs visant à proposer des offres certifiées « *cloud* de confiance » (cf. *infra*) ;
- des entreprises de services du numérique qui jouent le rôle d'intégrateurs (et de prescripteurs) ou d'accompagnateurs des clients dans leurs démarches auprès des fournisseurs de services *cloud*.

Enfin, une grande partie des fournisseurs de services *cloud* proposent des « places de marché *cloud* » accessibles à des vendeurs tiers. Les vendeurs tiers peuvent généralement proposer des services similaires à ceux des opérateurs de la place de marché.



**Figure 1 – La chaîne de valeur du *cloud* en France**



## Les relations entre fournisseurs de services *cloud* et clients

Les fournisseurs de services *cloud* concluent deux principaux types de contrats avec leurs clients : d'une part dans l'immense majorité des cas, des contrats standards conclus directement sur le site Internet du fournisseur, d'une durée indéterminée et résiliables à tout moment ; d'autre part, des contrats plus personnalisés pour quelques clients grands comptes, généralement des contrats à durée déterminée, de un à trois ans.

Chaque fournisseur publie directement ses grilles tarifaires sur son site Internet. La tarification des services se fait à la demande et selon l'usage (modèle « *pay-as-you-go* »), tandis que les services informatiques traditionnels facturent l'achat de licences.

Deux pratiques tarifaires, mentionnées dans le cadre de l'avis n° 23-A-05 de l'Autorité sur le projet de loi visant à sécuriser et réguler l'espace numérique, sont spécifiques au secteur :

- Les crédits *cloud*, qui permettent aux clients de bénéficier d'une réduction de dépenses pour certains services *cloud* éligibles. Les fournisseurs de services *cloud* recourent à deux grands types de crédits *cloud*, lesquels n'ont ni les mêmes durées ni les mêmes valeurs. La quasi-totalité des fournisseurs accordent des crédits *cloud* sous forme de tests de services *cloud*. Leurs montants peuvent varier de quelques dizaines à un millier d'euros, pour une durée ne dépassant pas, en général, trois mois. Ils peuvent avoir un caractère fréquent ou récurrent, un fournisseur de services *cloud* pouvant proposer des nouveaux crédits *cloud* à chaque fois qu'il propose un nouveau service. Les crédits *cloud* offerts sous forme de programmes d'accompagnement sont quant à eux proposés principalement par des fournisseurs de services *cloud* plus importants à destination d'utilisateurs à fort potentiel d'innovation, tels que les *startups*, concernent des montants beaucoup plus élevés (jusqu'à plusieurs centaines de milliers d'euros) et peuvent durer plusieurs années ;
- Certains fournisseurs de services *cloud*, en particulier les *hyperscalers*, mettent en place un modèle de fourniture de services *cloud* fondé notamment sur la facturation des transferts de données que ce soit vers un autre fournisseur ou vers les infrastructures sur site de l'entreprise. Ces structures de tarification sont appelées « *egress fees* ».

## Le contexte législatif et règlementaire

Le présent avis s'inscrit dans un contexte règlementaire riche, avec notamment le règlement européen sur les marchés numériques (« *Digital Markets Act* » ou « DMA ») adopté en 2022 pour encadrer les pratiques des géants du numérique ou le règlement européen sur les données (« *Data Act* »), en cours d'adoption, dont l'objectif est de favoriser notamment la portabilité et l'interopérabilité dans ce secteur. Le projet de loi visant à sécuriser et réguler l'espace numérique comprend également des dispositions relatives au *cloud*.

## Le fonctionnement du secteur du *cloud*

L'Autorité relève que les acteurs déjà fortement présents dans d'autres secteurs de l'économie numérique, tels qu'Amazon, Google ou Microsoft, disposent d'avantages concurrentiels

importants en comparaison de leurs concurrents français ou européens. Ces *hyperscalers* bénéficient d'une puissance financière considérable, qui leur permet notamment d'effectuer les lourds investissements nécessaires pour lancer des activités dans le secteur du *cloud*, tels que les centres de données ou les infrastructures informatiques et de réseau. Ils peuvent bénéficier d'économies d'échelle et de gammes liées aux différents services offerts dans leurs « écosystèmes ». Ils ont enfin accès à une base de clientèle préexistante leur permettant de bénéficier d'effets de réseaux très importants et qui peut leur servir de levier pour se développer rapidement dans le secteur du *cloud*.

Le marché français des services *cloud*, notamment pour les services de type IaaS et PaaS, est aujourd'hui très concentré. Selon les sources de données analysées par l'Autorité, les deux principaux fournisseurs, Amazon et Microsoft, auraient ainsi capté respectivement 46 % et 17 % des revenus des services IaaS et PaaS en 2021.

Par ailleurs, les grands écosystèmes d'*hyperscalers* bénéficient de l'essentiel de la forte croissance du marché. Les trois entreprises citées ci-dessus auraient ainsi capté 80 % de la croissance des dépenses en infrastructures et applications de services *cloud* public en France en 2021. Au cours des prochaines années, la concentration du marché français pourrait ainsi se poursuivre, à leur bénéfice.

La probabilité qu'un nouvel acteur puisse être en mesure de gagner rapidement des parts de marché apparaît limitée s'il n'est pas d'ores et déjà puissant sur d'autres marchés du numérique. Cette probabilité pourrait encore diminuer à mesure que les entreprises réalisent leur migration et choisissent un écosystème. En effet, les grands *hyperscalers* constitués en écosystèmes bénéficient d'avantages concurrentiels par rapport à des fournisseurs proposant des catalogues de services plus restreints. La mise en concurrence conduira généralement à sélectionner un fournisseur qui couvrira l'intégralité du besoin du client, ce qui s'apparente à une concurrence *pour* le marché plus que *sur* le marché.

Ces caractéristiques du secteur favorisent et renforcent la position des fournisseurs en place. Elles appellent à une vigilance particulière sur l'évolution de la structure concurrentielle du marché et les pratiques susceptibles d'être mises en œuvre par les *hyperscalers*.

## Analyse des marchés pertinents dans le secteur du *cloud*

L'Autorité constate que la formulation des besoins des clients en services *cloud* pourrait s'effectuer par « charges de travail », c'est-à-dire pour l'ensemble des ressources informatiques ou des processus métier répondant à un besoin ou objectif spécifique du client. S'il existe des offres avec des degrés de valeur ajoutée différents pour une même charge de travail, l'analyse de leur substituabilité devra forcément se faire *in concreto*. Il serait en outre nécessaire de prendre en compte, dans la définition des marchés pertinents, une possible substituabilité du côté de l'offre. En particulier, il pourrait être envisagé de tenir compte des écosystèmes *cloud* ou hors *cloud* dans l'analyse des marchés pertinents.

Une segmentation fondée sur la certification SecNumCloud, ou « *cloud* de confiance », pourrait par ailleurs être retenue. En effet, la doctrine « *cloud* au centre », publiée le 17 mai 2021, prévoit désormais que le *cloud* devienne la méthode d'hébergement par défaut de tous les services numériques de l'État. Dans ce cadre, la circulaire n°6282-SG du 5 juillet 2021 précise que les services numériques des administrations seront hébergés sur l'un des deux *cloud*

interministériels internes de l'État ou sur les offres de services *cloud* proposées par les industriels satisfaisant des critères stricts de sécurité. L'autorité nationale en matière de sécurité et de défense des systèmes d'information (ANSSI) a ainsi élaboré en 2016 le référentiel SecNumCloud pour permettre la qualification de prestataires de services d'informatique en nuage. Dans le cadre de l'appréciation d'une éventuelle segmentation du marché, l'Autorité pourrait prendre en compte l'ensemble des circonstances de l'espèce, comme l'existence de fonctionnalités spécifiques, les différenciant d'offres non certifiées ou un éventuel différentiel de prix.

En revanche, une segmentation en fonction des secteurs d'activité ne semble pas, pour l'instant, pertinente.

L'Autorité a enfin analysé trois types de marchés connexes : le marché des services de colocation dans des centres de données, les marchés des logiciels sur site, sur lesquels certaines entreprises présentes sur les marchés du *cloud* sont également actives et les marchés de l'intermédiation du conseil et de l'intégration de solutions *cloud*. Il apparaît que ces marchés, et notamment ceux des logiciels, devraient faire l'objet d'une particulière vigilance de la part des autorités de concurrence, au regard notamment de leurs relations avec les marchés des services *cloud*. En particulier, des effets de levier pourraient jouer entre ces marchés et les marchés du *cloud*, compte tenu de la position dominante de certains acteurs du logiciel également présents sur le *cloud*.

### Les risques concurrentiels transversaux

L'Autorité a analysé différentes pratiques transversales mises en œuvre ou susceptibles d'être mises en œuvre dans ce secteur, qui pourraient restreindre la concurrence par les mérites.

D'une part, le déséquilibre des relations entre les clients et les *hyperscalers* se manifeste par la présence sur le marché de certains acteurs incontournables qui peut rendre difficile la négociation des clauses des contrats par les clients, même puissants. D'autre part, il peut être difficile pour les clients d'anticiper les coûts futurs du *cloud*, compte tenu de la complexité des offres et du manque de lisibilité des tarifs.

Les crédits *cloud* et les *egress fees*, ont par ailleurs retenu l'attention de l'Autorité.

Les crédits *cloud* revêtent une réelle utilité et sont synonymes de valeur ajoutée pour de nombreuses entreprises, en particulier pour les *startups* qui s'épargnent de lourds investissements susceptibles d'entraver leur développement, mais également pour les fournisseurs de services *cloud* qui, grâce à eux, diffusent et encouragent l'adoption de leur technologie.

L'Autorité considère toutefois que les crédits *cloud* sous forme d'offres ciblées d'accompagnement doivent faire l'objet d'une attention particulière. Les montants proposés parfois élevés, le vaste écosystème d'entreprises qu'ils concernent et leur durée de validité, les distinguent significativement des essais gratuits qui peuvent être traditionnellement observés dans d'autres industries. Cela soulève des doutes quant à la capacité de tous les fournisseurs de services *cloud* à les proposer de manière rentable.

En outre, compte tenu des développements longs et coûteux mis en œuvre par les clients pour mettre en place une architecture *cloud* chez un fournisseur spécifique, et des coûts techniques

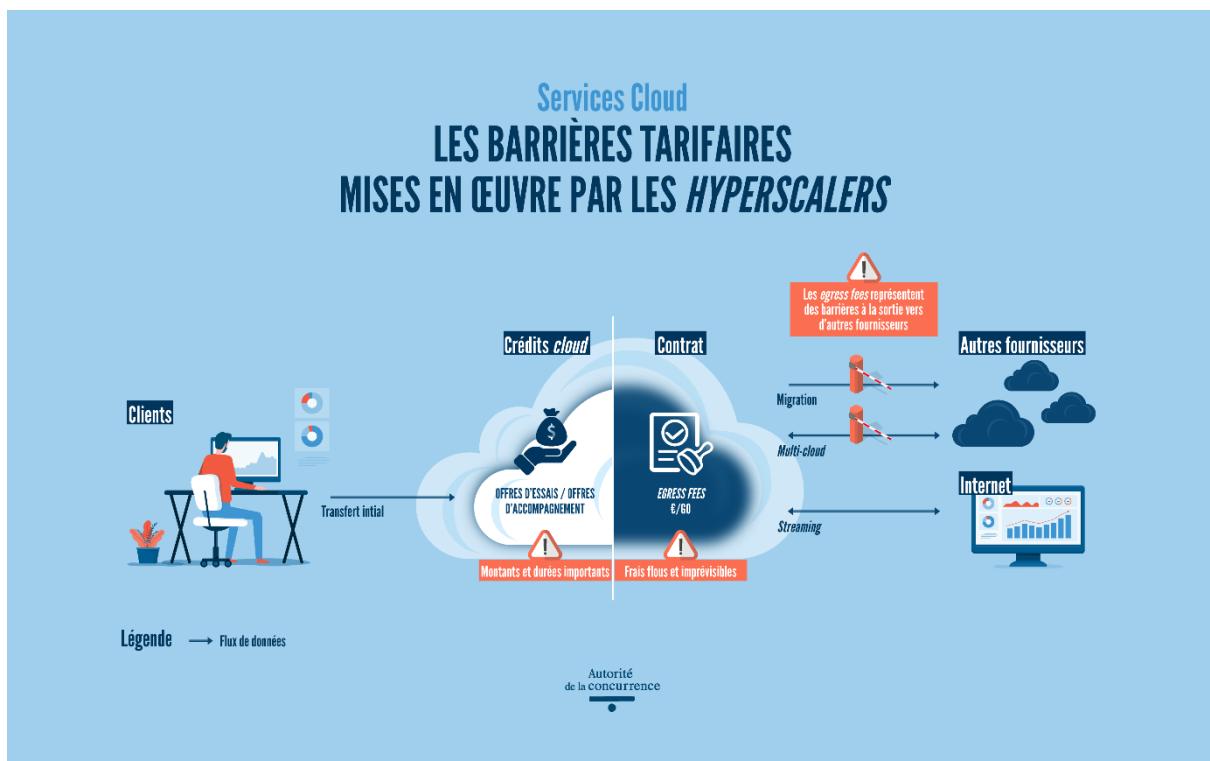
et financiers associés à la migration, il existe un risque de verrouillage par les grands fournisseurs du marché. Cette pratique, qui suscite des inquiétudes parmi les acteurs du marché, aurait des effets d'autant plus négatifs qu'elle ciblerait avant tout les clients à haut potentiel de développement et d'innovation. Ce verrouillage pourrait être renforcé par la présence de clauses ou pratiques limitant la possibilité de changer de fournisseur ou de recourir simultanément à plusieurs fournisseurs.

Afin de garantir le bénéfice de ces crédits *cloud*, il convient donc de s'assurer que des fournisseurs concurrents de services *cloud* aussi efficaces puissent être en mesure d'en proposer de manière profitable.

L'instruction a montré que les *egress fees* sont potentiellement déconnectés des coûts directement supportés par les fournisseurs lors de transferts de données. Ils constituent une préoccupation majeure pour le secteur, en raison de leur structure de prix proportionnelle au volume de données transférées, les clients n'ayant pas la possibilité d'anticiper en amont leurs besoins futurs en trafic de données et en usage de la bande passante.

Ces frais, dans leur structure actuelle, pourraient engendrer un risque de verrouillage de la clientèle sur un marché en pleine expansion, en rendant plus difficile pour les utilisateurs de services *cloud* de quitter leur primo-fournisseur ou de recourir à plusieurs fournisseurs dans un environnement multi-*cloud*, pour une même charge de travail ou pour des charges de travail qui impliquent des transferts de données récurrents entre elles.

**Figure 2 – Les barrières tarifaires mises en œuvre par les hyperscalers**



## Les risques concurrentiels spécifiques

L'Autorité a identifié des risques concurrentiels spécifiques selon trois scénarios : la primo-migration, c'est-à-dire la migration des systèmes d'information sur site vers le *cloud*, la migration d'un fournisseur de services *cloud* à un autre, et les barrières à l'expansion des concurrents des *hyperscalers*.

- **Les risques concurrentiels liés à la migration des systèmes d'information sur site vers le *cloud***

La migration des clients de solutions sur site vers le *cloud* est complexe et coûteuse, ce qui peut les inciter à se tourner vers leurs fournisseurs historiques de services informatiques lorsque ceux-ci proposent aussi des services *cloud*.

L'instruction a également mis en évidence des pratiques susceptibles de renforcer les freins au recours par un client à un fournisseur de services *cloud* alternatif, comme des clauses contractuelles restrictives, des ventes liées, des avantages tarifaires favorisant leurs produits ainsi que des restrictions techniques. Si elles étaient mises en œuvre par un opérateur en position dominante, ces pratiques pourraient constituer des pratiques abusives. Plusieurs plaintes sont en cours devant la Commission européenne sur le fondement de pratiques similaires.

- **Les risques concurrentiels spécifiques liés à la migration d'un fournisseur de services *cloud* à un autre**

Les freins à la migration vers un autre fournisseur des charges de travail déjà hébergées dans le *cloud* peuvent nuire au fonctionnement de la concurrence, en empêchant le client de changer de fournisseur de services *cloud*.

Si de nombreuses entreprises sont encore dans une phase de primo-migration ou de développement de leurs solutions sur le *cloud* et n'ont pas encore envisagé de migration vers un autre fournisseur, il apparaît d'ores et déjà que la migration d'un fournisseur de services *cloud* à un autre peut être freinée non seulement par des barrières techniques mais également par des pratiques volontaires de la part des fournisseurs.

Des freins technologiques à la migration peuvent apparaître à différents niveaux, liés en particulier aux spécificités de l'architecture et des solutions utilisées. En effet, la variété des produits et services, notamment s'agissant des services PaaS, l'interconnexion des services informatiques et le manque de portabilité des données et des applications peuvent entraîner des coûts de migration non négligeables. Au-delà des freins techniques, les fournisseurs peuvent aussi augmenter les coûts de migration pour renforcer leur position. Cela pourrait être le cas, par exemple, d'une entreprise utilisant volontairement un format de données spécifique afin d'empêcher la portabilité des données d'un client vers un fournisseur de services *cloud* alternatif. Les fournisseurs pourraient également imposer des conditions commerciales contribuant au verrouillage des clients au sein de leur écosystème.

- **Les risques concurrentiels spécifiques liés aux barrières à l'expansion pour les concurrents des *hyperscalers***

Le secteur est aussi marqué par des freins techniques à l'interopérabilité. Ceux-ci affectent l'ensemble des concurrents et particulièrement les fournisseurs de taille modeste, compte tenu de l'attractivité des écosystèmes *cloud* au moment de choisir un primo-fournisseur. Ces freins sont illustrés dans l'avis par des exemples concrets comme les implications techniques de l'interopérabilité en ce qui concerne le service de stockage objet Amazon S3 (IaaS). L'interopérabilité avec les services PaaS est encore plus complexe, puisque, par exemple, le changement d'un service PaaS de base de données nécessite de réécrire la partie du code de l'application qui utilise ce service.

Plusieurs risques concurrentiels peuvent également être identifiés.

Premièrement, des risques liés à la présence d'un fournisseur sur plusieurs marchés connexes :

- des restrictions d'accès des concurrents aux logiciels nécessaires à la fourniture de services *cloud* : un éditeur de logiciels qui se trouve être fournisseur de services *cloud*, pourrait mettre en œuvre des pratiques visant à augmenter les tarifs des licences nécessaires pour ses concurrents ou subordonner l'utilisation de ses logiciels à l'achat d'un grand nombre de licences. Ainsi, par effet de levier, un éditeur en position dominante sur un logiciel pourrait évincer une partie de la concurrence pour conquérir la clientèle sur les services *cloud* ;
- des conditions commerciales ou techniques plus avantageuses pour les propres produits ou services du fournisseur : grâce à leur structure conglomérale, les *hyperscalers* peuvent notamment mettre au point des systèmes de remises, avantages tarifaires et non tarifaires ou subventions croisées, utilisant ainsi leur pouvoir de marché sur des marchés connexes pour accélérer le développement de leur activité de activité de fournisseur de services *cloud* ;
- un accès privilégié aux données : les *hyperscalers* bénéficient d'un accès privilégié, voire exclusif, à des données difficilement reproductibles par leurs concurrents et susceptibles de leur conférer un avantage concurrentiel déterminant. Cet accès privilégié peut notamment provenir du fait que de nombreux services *cloud* utilisent l'intelligence artificielle pour exploiter les données et fournir des services d'analyse plus élaborés à leurs utilisateurs. Cela peut permettre un meilleur ciblage commercial et une connaissance fine des besoins des clients, mais également une amélioration des fonctionnalités des services et le développement de nouveaux outils innovants, par exemple d'intelligence artificielle ou d'apprentissage automatique. Ces évolutions peuvent avoir des effets favorables pour les consommateurs et l'innovation. Toutefois, elles peuvent également conduire à un déséquilibre concurrentiel important entre acteurs, dans la mesure où les concurrents des *hyperscalers* ne peuvent pas reproduire ce volume de données aisément ni à la même échelle.

Deuxièmement, au-delà de l'impossibilité de répliquer à l'identique les offres de crédit *cloud*, notamment pour les plus petits fournisseurs et de l'impact des *egress fees* sur les stratégies de multi-*cloud*, l'Autorité identifie d'autres risques.

Si le rôle des places de marché dans le secteur du *cloud* reste à ce jour mineur, celles-ci tendent à se développer et à gagner en importance, à la fois pour les fournisseurs de ces plateformes et pour les éditeurs qui y proposent leurs services. L'Autorité considère que plusieurs risques

concurrentiels pourraient émerger, en particulier liés aux conditions fixées par les fournisseurs pour l'accès à ces places de marché et à leur fonctionnement :

- plusieurs acteurs considèrent par exemple que certains fournisseurs, à l'instar d'AWS et d'Oracle, empêchent les éditeurs tiers de communiquer ou promouvoir leurs offres au travers de leurs services acquis via la place de marché ;
- à travers la place de marché, le fournisseur peut également favoriser ses propres solutions, à la fois dans les conditions de commercialisation et de mise en valeur auprès des clients, au détriment des autres services proposés par des tiers ;
- des clauses de parité tarifaire peuvent également être imposées. À travers ces clauses, le fournisseur peut retirer de la vente le service de l'éditeur tiers lorsque le prix sur sa place de marché est plus élevé que sur les autres canaux de commercialisation utilisés ;
- il conviendra enfin de rester vigilant sur les taux de commission, qui constitueront un indicateur intéressant du caractère incontournable de certaines places de marché.

Des freins volontairement mis en place pour entraver l'interopérabilité ne sont enfin pas exclus. Des fournisseurs de services *cloud* proposant des produits ou services particulièrement populaires seraient susceptibles d'empêcher ou de restreindre l'accès à des informations essentielles permettant d'assurer l'interopérabilité de ces produits ou services avec ceux de leurs concurrents. Cette pratique pourrait avoir pour effet de restreindre la compatibilité de solutions concurrentes et donc leur attractivité vis-à-vis des clients.

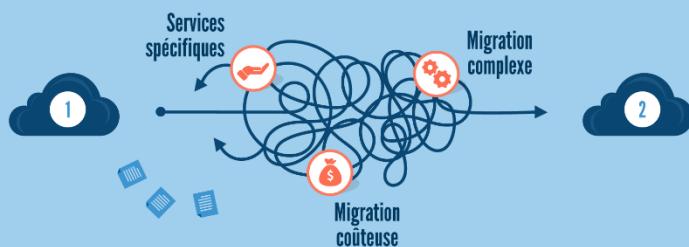
**Figure 3 – Les risques concurrentiels spécifiques**

## Services Cloud LES RISQUES CONCURRENTIELS SPÉCIFIQUES

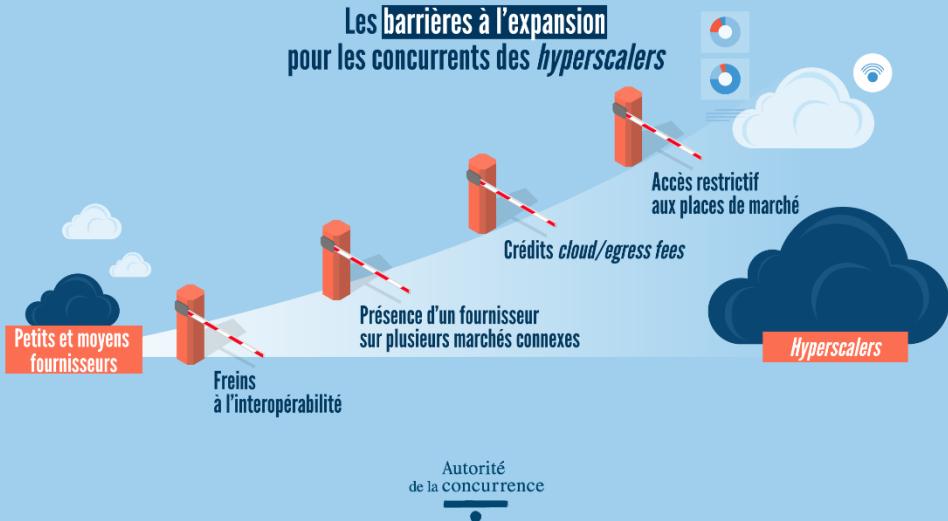
La migration vers le *cloud*  
un avantage pour les opérateurs déjà présents sur site



La migration *cloud à cloud*  
les différents obstacles



Les barrières à l'expansion  
pour les concurrents des *hyperscalers*



## Les réponses du droit de la concurrence

Afin de répondre aux enjeux du *cloud*, il pourrait être envisagé d'utiliser, aux côtés des outils classiques de droit de la concurrence que sont l'abus de position dominante, la lutte contre les ententes illicites, le contrôle des concentrations, et l'abus de dépendance économique, d'autres instruments du Livre IV du code de commerce, comme le droit des pratiques restrictives de concurrence.

Les autorités de concurrence ont une pratique décisionnelle riche, pouvant de servir de référence en cas d'action fondée sur l'abus de position dominante mise en œuvre dans le secteur du *cloud*. À titre d'exemple, il est possible de citer l'affaire Google Shopping en 2021 (dans laquelle le Tribunal de l'Union européenne a apporté des précisions sur la question de la discrimination et de l'auto-préférence), l'affaire Nespresso de l'Autorité sur les pratiques de ventes liées (2014) ou encore l'affaire Microsoft (2007), dans laquelle la Commission européenne a posé un certain nombre de principes importants relatifs au refus de fournir des informations relatives à l'interopérabilité de la part d'entreprises dominantes. Au-delà du refus de fournir des informations relatives à l'interopérabilité, le partage d'informations dégradées ou discriminatoires a également été examiné par les autorités de concurrence. Ainsi, l'Autorité a soulevé des préoccupations de concurrence concernant une pratique de Meta consistant à dégrader la capacité des intermédiaires à fournir aux annonceurs des services à partir de leurs propres technologies publicitaires (en retirant par exemple l'accès de Criteo à une interface de programmation d'applications nécessaire à ses activités). Plus récemment, en mai 2023, l'Autorité a constaté que Meta n'avait pas défini des critères d'accès transparents, objectifs et non discriminatoire à ses partenariats relatifs à la vérification publicitaire. L'Autorité a donc enjoint à Meta de mettre en place de nouveaux critères d'accès et de maintien à ces partenariats.

Pour faire face à ces situations, l'Autorité a su utiliser des outils procéduraux efficaces et rapides comme les mesures conservatoires, utilisées en 2023 contre Meta dans le secteur de la vérification publicitaire, ou les engagements, utilisés à deux reprises en 2022 dans des affaires impliquant respectivement Meta et Google.

Le droit des ententes peut aussi dans certains cas être un instrument pertinent. De nombreux groupements et associations de fournisseurs de services *cloud* se sont formés au cours des dernières années, ou sont en voie de l'être, avec ou sans création d'une structure juridique commune, notamment :

- des structures communes entre acteurs du *cloud* pour présenter des offres « *cloud de confiance* » ;
- des partenariats notamment technologiques entre des grands fournisseurs de logiciels liés aux données et des fournisseurs de services *cloud*. Ainsi, en 2019, Microsoft et Oracle ont annoncé un partenariat d'interopérabilité de leur *cloud*, permettant aux clients de faire migrer et d'exécuter les charges de travail critiques de l'entreprise vers Microsoft Azure et Oracle *Cloud* ;
- des alliances ou des partenariats technologiques entre intégrateurs et la majorité des fournisseurs de services *cloud*, notamment *hyperscalers* ;
- des partenariats spécifiques dans certains secteurs.

Le fait, d'une part, que ces entités regroupent des entreprises autonomes et parfois concurrentes et, d'autre part, que leur fonctionnement suppose des contacts entre ces mêmes entreprises les expose à des risques au regard des règles prohibant les ententes.

Des solutions de standardisation, qui favorisent à première vue l'interopérabilité et donc le changement de fournisseur, peuvent également, dans certains cas, devenir problématiques pour la concurrence, si elles visent à empêcher l'émergence de solutions alternatives et paralyser l'innovation par le biais de pratiques de verrouillage technique.

Les opérations de concentration appellent enfin à une vigilance particulière des autorités de concurrence.

Au cours des dernières années, plusieurs opérations d'importance concernant des fournisseurs de services *cloud* ont eu lieu à travers le monde, comme l'acquisition du fournisseur de logiciels Red Hat par la société IBM en juillet 2019, le projet du groupe américain Broadcom de racheter l'entreprise VMware, qui fait actuellement l'objet d'un contrôle par plusieurs autorités de concurrence, ou encore le rachat d'Activision Blizzard par Microsoft, qui soulève des inquiétudes sur le marché émergent du *cloud gaming* et a entraîné des réponses contrastées des autorités de concurrence.

Lors de la consultation publique, plusieurs acteurs ont exprimé des inquiétudes liées à d'éventuelles nouvelles concentrations dans le secteur du *cloud*. Parmi les principaux risques identifiés, ils ont mentionné la réduction du nombre d'acteurs, de potentielles ventes groupées ou liées, l'assèchement de l'innovation et des alternatives pour les clients ainsi que de potentielles augmentations des prix. Plusieurs entreprises ont également mentionné des cas où des solutions technologiques pouvant auparavant s'intégrer auprès de multiples fournisseurs ont été transformées en technologies propriétaires après rachat.

Les parties prenantes ont plus généralement exprimé le sentiment qu'une dynamique de concentration était en cours dans le secteur du *cloud*, notamment sur le marché français, et pourrait se poursuivre dans les prochaines années. Cependant, si les plus grands fournisseurs de services *cloud*, en particulier les *hyperscalers*, ont tous réalisé des acquisitions au cours des dernières années, cela n'a été que rarement le cas de la part des plus petits acteurs, notamment européens.

Enfin, la création de nouvelles entités sous la forme de co-entreprises pour proposer, par exemple, des offres labellisées « *cloud de confiance* », constitue une autre forme de concentration susceptible de soulever des préoccupations de concurrence. Plusieurs acteurs ont considéré que la communication et les moyens marketing déployés pour le lancement commercial des offres et l'obtention du label « *cloud de confiance* » soulevaient des risques pour la concurrence.

Enfin, il peut être opportun d'envisager ces problématiques sous un angle plus large.

L'abus de dépendance économique peut être une autre voie intéressante. Pour mémoire, il sanctionne l'exploitation abusive, par une entreprise ou un groupe d'entreprises, de l'état de dépendance économique dans lequel se trouve à son égard une entreprise cliente ou fournisseur, dès lors qu'elle est susceptible d'affecter le fonctionnement ou la structure de la concurrence. Ce fondement juridique a été mis en œuvre par l'Autorité pour sanctionner l'entreprise Apple en 2020.

La mise en œuvre par la direction générale de la concurrence, de la consommation et de la répression des fraudes des dispositions relatives aux pratiques restrictives de concurrence pourrait enfin se justifier, notamment sous l'angle du déséquilibre significatif ou de l'avantage sans contrepartie.

### **Les autres réponses en cas de défaillance de marché**

L'Autorité a aussi constaté l'existence de défaillances de marché qui pourraient justifier le recours à la régulation.

En effet, si les solutions techniques existent pour faciliter le changement de fournisseur ou recourir au *multi-cloud* (services standards ou solutions *open-source* par exemple), l'autorégulation n'a pas permis la mise en place de standards techniques communs. Les acteurs en place, notamment les *hyperscalers*, ne sont en effet pas nécessairement incités à développer les solutions les plus performantes ou au meilleur prix dès lors qu'elles sont susceptibles d'éroder leurs parts de marché. Plusieurs clients ont ainsi confirmé que les principaux fournisseurs de services *cloud* ne cherchaient pas forcément à offrir des solutions standards pour accéder à leurs services *cloud*.

Par ailleurs, les initiatives conjointes visant à développer des standards communs rencontrent des difficultés de mise en œuvre, qu'il s'agisse de Gaia-X, fondée initialement par 22 organisations françaises et allemandes, ou de l'initiative européenne SWIPO. En effet, la présence des *hyperscalers* dans les groupes de travail techniques et leur volonté supposée de ralentir ou complexifier les discussions sont très critiquées et contribuent, selon certaines parties prenantes, au manque de résultats de ces initiatives.

Une approche règlementaire paraît donc davantage adaptée pour remédier aux défaillances de marché identifiées, ce que les autorités de régulation européennes et nationales ont commencé à mettre en œuvre ces derniers mois avec le DMA et le projet de Data Act ou encore le projet de loi visant à sécuriser et réguler l'espace numérique récemment présenté par le Gouvernement. Dans son avis précité n°23-A-05 du 20 avril 2023 concernant ce projet, l'Autorité, tout en partageant la plupart des préoccupations auxquelles répond ce projet de loi, a formulé plusieurs recommandations destinées notamment d'une part à s'assurer que ses dispositions seront alignées avec celles du Data Act, d'autre part à renforcer l'effectivité de ses dispositions.

Le trilogue s'étant achevé le 27 juin 2023, il n'est pas pertinent pour l'Autorité de formuler des propositions d'amélioration du texte actuel du Data Act. Cependant, la Commission devant mener un exercice d'évaluation dans trois ans, l'Autorité considère qu'il est pertinent de soumettre des points de vigilance aux parties concernées (distinguer le régime applicable aux *egress fees* des autres frais de migration, réaliser une étude d'impact sur les crédits *cloud* et préciser les mesures en faveur de la portabilité et de l'interopérabilité).

### **Perspectives et conclusion**

Plusieurs évolutions susceptibles d'avoir un impact sur le fonctionnement concurrentiel du secteur doivent être prises en considération.

Tout d'abord, le fonctionnement concurrentiel du secteur du *cloud* se caractérise par une concurrence *pour* le marché plus que *sur* le marché, dans la mesure où, pour un besoin ou une charge de travail spécifique, les clients ont tendance à contracter avec un fournisseur unique, en particulier ceux disposant d'un écosystème attractif. Compte tenu du risque de verrouillage des clients dans ces écosystèmes, la demande des clients devrait se répartir entre les principaux écosystèmes et une fois l'essentiel du stock de charges de travail conquis, il est à prévoir de faibles variations de parts de marché, ce qui pourrait conduire à une diminution de l'intensité concurrentielle.

Dans le même temps, de nouvelles technologies améliorant les performances des produits et services devraient émerger et, potentiellement, modifier la structure et l'équilibre concurrentiel des marchés du *cloud*. Les autorités de concurrence devront être vigilantes à ce que les acteurs déjà établis n'entraînent pas le développement de plus petits ou de nouveaux acteurs à partir de ces technologies.

Tout d'abord, la multiplication des usages de l'intelligence artificielle va servir de moteur à la croissance de la demande en services *cloud*. En effet, les nombreuses évolutions vers des modèles de plus en plus complexes, comme par exemple les grands modèles de langage (« *Large Language Models* »), demandent des ressources en puissance de calcul très importantes.

C'est le cas également du calcul à la périphérie de réseau (« *edge computing* »), innovation qui aura un fort impact dans un horizon de temps proche. La capacité des fournisseurs de services *cloud*, notamment autres que les *hyperscalers*, à se positionner sur ces défis technologiques pourrait leur permettre de surmonter certaines des barrières à l'entrée et à l'expansion identifiées. D'autres usages émergent comme le jeu en nuage ou « *cloud gaming* ».

Les développements dans le secteur du *cloud* seront probablement également influencés par des considérations plus générales, comme les changements géopolitiques, qui auront potentiellement un impact sur l'innovation en matière de sécurité dans le *cloud*, ou l'importance croissante de l'empreinte environnementale.

Les risques concurrentiels et défaillances de marché exposés dans le présent avis seront analysés avec attention par les services de l'Autorité. Cette vigilance pourra le cas échéant se traduire par l'ouverture d'enquêtes de nature contentieuse. Cet examen s'avère indispensable pour préserver l'innovation et minimiser les coûts dans un secteur qui représente un vecteur important de croissance économique pour les entreprises.