

**Réponse à la consultation
publique de l'Arcep :
« *Régulation des services
d'informatique en nuage
(cloud)* »**

A propos d'OVHcloud

OVHcloud se réjouit de la possibilité de participer à la consultation publique de l'Arcep sur la régulation des services d'informatique en nuage (cloud).

Créé en France en 1999, OVHcloud est un fournisseur européen de services cloud qui offre aux organisations, publiques comme privées, une suite complète de solutions conçues pour répondre à leurs demandes de transformation numérique, à travers 3 univers produits : le cloud public, le cloud privé et le web cloud.

OVHcloud s'appuie sur un modèle intégré qui lui confère la maîtrise complète de sa chaîne de valeur, de la conception de ses serveurs à celle des solutions de plateforme cloud qu'il met à la disposition de ses clients, en passant par la construction et le pilotage de ses centres de données ("datacenters") ou l'orchestration de son réseau de fibre optique. Cette approche unique lui permet de couvrir en toute indépendance l'ensemble des usages de ses clients.

OVHcloud exploite 43 datacenters dans 9 pays à travers le monde, abritant plus de 450 000 serveurs fabriqués par OVHcloud.

2. Encadrer les frais de transfert de données et de changement de fournisseur de services *cloud*

Q1 : Avez-vous des observations sur les éléments de contexte liés aux pratiques tarifaires présentées ci-avant ?

Nous n'avons pas d'observation supplémentaire.

Il convient toutefois de noter que les annonces de retrait des « egress fees » effectuées par les hyperscalers ne sont que partielles et ne constituent en réalité pas la fin de facturation de tels frais à leurs utilisateurs. En effet ces « retraits » : présentent les limites suivantes :

- Les frais de transfert de données ne sont pas retirés mais seulement compensés par un montant de crédits déterminé par le fournisseur.
- L'octroi de ce crédit est fait après un processus complexe, et selon le bon vouloir du fournisseur.
- Ils ne s'appliquent pas au multicloud.
- Ils ne s'appliquent qu'à une sélection de services de ces fournisseurs.
- Ils ne s'appliquent qu'aux projets de migration de moins de 60 jours et excluent de fait les projets de migration des utilisateurs ayant des besoins importants.

Q2 : Partagez-vous la description présentée ci-avant des transferts de données et des éléments de l'infrastructure qui les supporte ? Identifiez-vous d'autres éléments d'infrastructure mobilisés dans le cadre des transferts de données ?

De manière générale, nous partageons la description présentée. Il est à noter que les différents coûts identifiés par l'Autorité (ex : fibre optique, réseau etc.) sont inhérents aux activités habituelles d'un fournisseur de services cloud. Leur facturation à l'utilisateur, en particulier lorsque ce dernier cherche à quitter les services d'un fournisseur, n'est donc pas justifiée d'un point de vue technique et économique mais relève de stratégies commerciales pour enfermer les utilisateurs dans leurs services, tel qu'observé par l'Autorité de la concurrence dans son avis sur le cloud.

Les réponses suivantes viennent apporter des précisions quant aux différents postes de coûts identifiés dans le cadre du multi-cloud ou d'un changement de fournisseur.

Q3 : Partagez-vous l'analyse de l'Autorité selon laquelle le transport des données et l'interconnexion sont les principaux déterminants des coûts supportés par les fournisseurs relativement aux transferts de données ? Au-delà de ces deux catégories, identifiez-vous d'autres postes de coûts pertinents à prendre en compte du fait de leur rôle dans les transferts de données ? Le cas échéant, précisez quels sont selon vous les plus significatifs.

Nous partageons l'analyse de l'Autorité selon laquelle le transport des données et l'interconnexion sont les principaux déterminants des coûts supportés par les fournisseurs relativement aux transferts de données.

Les 2 principaux postes de coûts sont en effet : la connexion des datacenters à internet et les coûts de transport entre les datacenters. Comme précisé précédemment, ces coûts correspondent à des investissements préalables et des partenariats avec les différentes intermédiaires et opérateurs télécoms nécessaires à la construction d'une infrastructure cloud robuste et résiliente pour les utilisateurs.

Ces coûts incluent notamment les frais de transit et peering, l'achat puis la maintenance équipements d'interconnexion (routeurs, commutateurs, transpondeurs optiques, répéteurs), ainsi que les dépenses liées à la location d'espace dans les centres d'interconnexion et à la collaboration avec les opérateurs (télécommunication / colocation).

Au-delà de ces deux catégories, d'autres postes de coûts sont à considérer : les coûts des adresses IP, les infrastructures de sécurité (notamment la protection contre les attaques DDoS sur les points de présence majeurs), les coûts opérationnels (notamment le personnel nécessaire pour déployer et maintenir le réseau), la location d'espaces pour opérer le matériel dans les centres d'interconnexion, la mise en place de liens de connexion sécurisée dans certains cas identifiés. Encore une fois, il convient de souligner que ces coûts sont inhérents aux activités d'un opérateur cloud et au cœur de la promesse de performance et de résilience.

Les coûts liés au transport des données et à l'interconnexion demeurent les plus significatifs.

Q4 : Quelle serait selon vous une bonne façon d'estimer et de quantifier chacun de ces postes de coûts ? Précisez dans votre réponse si certaines données de référence vous sembleraient pertinentes pour réaliser un tel exercice.

Ces postes de coûts évoluent en fonction de la distance du transfert. Un transfert local sera moins important qu'un transfert longue distance en raison de la différence de coût qui intervient d'une région à une autre. L'estimation pourrait être faite à l'€/Gbits de données clients transférées en prenant en compte le franchissement de plaques géographiques (Europe, APAC, Etats-Unis, etc.).

Q5 : Dans quelle mesure la stratégie choisie par le fournisseur de cloud en termes d'investissements et de dépenses d'exploitation (degré d'internalisation des éléments de réseaux du fournisseur, stratégie propre aux accords d'interconnexion, etc.) a une influence sur les coûts de transfert de données ? Le cas échéant, pouvez-vous détailler votre réponse, en particulier les postes de coûts qui peuvent être concernés.

La stratégie d'investissement et notamment d'internalisation des éléments a un impact sur certains coûts supportés par le fournisseur de cloud. En effet, lorsqu'un fournisseur possède et exploite son propre réseau, comme une fibre propriétaire, il peut s'affranchir des coûts supplémentaires liés à l'utilisation d'acteurs intermédiaires. Cette internalisation, qui correspond à des investissements initiaux importants et des frais de maintenance d'infrastructure sur la durée, permet aussi de réduire certaines dépenses telles que les frais d'interconnexion. Il convient néanmoins de noter que cette stratégie relève d'un choix et non d'une obligation pour un fournisseur, par exemple pour fournir des solutions plus performantes et ainsi se différencier sur le marché.

Ces stratégies ne viennent pas modifier substantiellement les coûts de transfert de données en eux-mêmes.

Q6 : Partagez-vous l'analyse de l'Autorité selon laquelle les coûts afférents au transfert de données correspondent à la détention d'une capacité d'utilisation de bande passante ?

Nous partageons l'analyse de l'Autorité. Cela rend d'autant plus injustifié la facturation au volume de données à transférer effectué par certains fournisseurs de cloud lorsqu'un utilisateur souhaite quitter ses services. En effet, les coûts imputés au fournisseur ne varient pas en fonction du volume transféré mais en fonction de la capacité d'utilisation de bande passante.

Q7 : Partagez-vous l'analyse de l'Autorité sur le fait que la gestion des pics de demande en trafic de ses clients constitue une contrainte fondamentale pour le fournisseur dans le dimensionnement de son réseau ?

Nous partageons l'analyse de l'Autorité selon laquelle la gestion des pics de demande en trafic des clients représente une contrainte majeure pour les fournisseurs dans le dimensionnement de leur réseau. En effet, des pics soudains de trafic peuvent provoquer une surcharge de l'infrastructure, entraînant une dégradation des performances, voire une indisponibilité du service pour les utilisateurs. C'est la raison pour laquelle les fournisseurs cloud anticipent et dimensionnent en conséquence leur infrastructure pour supporter ce type d'évènement sur le réseau.

Q8 : Partagez-vous l'analyse selon laquelle le fournisseur n'est pas en mesure d'identifier, ni la finalité d'un transfert de données (e.g. pour effectuer une migration ou pour un usage multi-cloud), ni la route exacte qu'empruntera le trafic pour un transfert particulier ? Dans le cas contraire, quelle méthode pourrait selon vous permettre de connaître la finalité d'un transfert de données particulier ?

Nous partageons l'analyse de l'Autorité selon laquelle le fournisseur n'est pas toujours en mesure d'identifier la finalité d'un transfert de données. Le fournisseur est cependant en

mesure de déterminer le point de départ et une partie de la route qui est empruntée, sans visibilité sur la sortie.

Néanmoins, lors d'une migration totale hors des infrastructures, le fournisseur peut être amené à en prendre connaissance grâce à une faisceau d'indices parmi lesquels : la fin du contrat, des demandes spécifiques du client liées à la migration, etc.

Q9 : Partagez-vous l'analyse selon laquelle le transfert de données dans le cas d'un changement de fournisseur constitue un événement non récurrent, faisant intervenir une quantité définie de données et pouvant être réalisé avec une certaine flexibilité (e.g. possibilité de lisser dans le temps), de telle sorte qu'il n'implique pas pour le fournisseur d'augmentation de la capacité de son réseau ? Si non, expliquez pourquoi.

Nous partageons l'analyse de l'Autorité. Il est fréquent que les transferts de données lors de migration, qui constituent un événement non récurrent, soient en effet lissés sur plusieurs semaines - voir mois - en raison de la complexité technique de certains projets de migration. Comme évoqué dans la réponse précédente, ce pic ou le transfert de données induit n'a pas d'impact sur l'infrastructure d'un fournisseur de cloud, prévue pour anticiper ces situations. Il n'est donc pas nécessaire d'augmenter la capacité du réseau et de supporter des coûts additionnels.

Q10 : Partagez-vous l'analyse qu'un transfert de données intervenant dans le cadre d'un changement de fournisseur n'implique pas le déploiement d'équipements supplémentaires et, partant, de coûts spécifiques ? Si non, expliquez pourquoi.

Nous partageons l'analyse selon laquelle un transfert de données intervenant dans le cadre d'un changement de fournisseur n'implique pas le déploiement d'équipements supplémentaires et de coûts spécifiques.

Comme évoqué précédemment, le transport de donnée en lui-même est anticipé par tout fournisseur de cloud lorsqu'il dimensionne sa propre infrastructure. Un transfert de donnée qui intervient par exemple dans le cas d'une migration d'un client n'implique aucun équipement ou coût supplémentaire à ces investissements initiaux.

Q11 : Partagez-vous l'analyse selon laquelle le coût incrémental d'un transfert de données dans le cas d'un changement de fournisseurs est nul ? Si non, expliquez pourquoi.

Nous partageons l'analyse de l'Autorité. Les frais de transfert de données sont des frais artificiels, décorrélés de coûts réels, facturés par certains fournisseurs afin de dissuader les utilisateurs de quitter leurs services. Les justifications parfois mises en avant par ces fournisseurs pour justifier cette facturation (investissements réseau, déploiement de fibre

optique etc.) renvoient en réalité à des coûts de fonctionnement habituels pour un fournisseur de cloud, décorrélé du changement de fournisseur en lui-même.

Q12 : Identifiez-vous des cas qui justifieraient de facturer le transfert de données intervenant dans le cadre d'un changement de fournisseur, par exemple des clients présentant des besoins particuliers, pour lesquels un tel transfert entraînerait des coûts spécifiques directement liés au transfert de données ? Le cas échéant, quels seraient ces cas et quels postes de coûts spécifiques, induits par les transferts concernés, pourraient être facturés ?

Les migrations d'applications avec de grand volumes de données (Streaming, Imagerie, Gestions documentaire...) dans des délais restreints, peuvent en effet impliquer des coûts spécifiques de transfert de données qui peuvent être partiellement supportés par le fournisseur source et le fournisseur cible. Néanmoins, généralement, ces migrations de grands volumes sont gérées avec des outils matériels spécifiques qui peuvent être déployés à la demande d'un client – voir réponse à la question 17

Q13 : L'hypothèse d'un plafond des frais de transfert de données dans le cadre d'un changement de fournisseur fixé à zéro appelle-t-elle d'autres remarques de votre part ?

Pas de remarque supplémentaire, nous considérons cette hypothèse juste et cohérente avec la réalité des fournisseurs de cloud.

Dans ce cadre, il conviendra pour l'Arcep de s'assurer, dans le cadre de ses missions, qu'en retour les fournisseurs de cloud ne ralentissent pas artificiellement les qualités et temps des transferts de données, que cela soit pour dissuader leurs clients de quitter leurs services ou pour les pousser à avoir recours à des services supplémentaires leur permettant de transférer leurs données - et donc de changer de fournisseur - plus rapidement. De telles pratiques viendraient renforcer encore les barrières au changement de fournisseur, à l'opposé des objectifs de la loi SREN.

Q14 : Partagez-vous l'analyse selon laquelle les transferts de données induits par un usage multi-cloud présentent un caractère récurrent et un volume variable dans le temps et difficilement anticipable, qui pourraient impliquer une flexibilité moins grande pour réaliser ces transferts par rapport au cas d'un changement de fournisseur ? Si non, expliquez pourquoi.

Nous partageons l'analyse de l'Autorité selon laquelle les transferts de données induits par un usage multi-cloud présentent un caractère récurrent et un volume variable dans le temps et difficilement anticipable. En effet, dans un contexte multi-cloud, le trafic est continu, contrairement à une migration, qui reste un événement ponctuel.

Q15 : Parmi les éléments sur l'infrastructure d'un transfert de données présentés dans la section 2.1.2 et ceux que vous auriez évoqués en réponse à la question 2, identifiez-vous des équipements qu'un fournisseur doit spécifiquement déployer, ou des actions qu'il doit spécifiquement réaliser, pour permettre les transferts de données requis par ses clients dans le cadre de leur usage multi-cloud ? Le cas échéant, lesquels ?

Dans le contexte du multicloud, il est fréquent d'établir un lien physique entre les différents fournisseurs de services cloud impliqués afin de faciliter la communication directe et sécurisée entre ces derniers. Ce type de lien est souvent mis en place pour des raisons de performance de sécurité ou encore de latence réduite.

De la même manière, il est possible de mettre en place un routeur pour interconnecter les différents environnements cloud. Ces routeurs, souvent virtualisés, sont fournis par des acteurs tiers spécialisés dans les solutions de « Software Defined Cloud Interconnect » (SDCI), tels qu'Equinix Fabric, Megaport, Digital Realty Service Fabric ou Console Connect. L'utilisation de ces équipements engendre des frais, incluant à la fois le coût d'accès aux équipements et les charges liées au trafic transitant sur leurs réseaux.

Q16 : Quels postes de coûts seraient susceptibles selon-vous d'être affectés par un usage multi-cloud ? Quelle façon vous semble pertinente pour allouer, parmi l'ensemble des coûts, ceux qui seraient directement liés aux transferts de données dans le cadre de l'usage multi-cloud ? Quels éléments de référence ou indicateurs pourraient être pertinents pour ce faire ?

Se référer à la réponse précédente.

Q17 : Identifiez-vous certains types de clients présentant des besoins particuliers pour lesquels les coûts supportés par le fournisseur relatifs à ce type de transfert seraient différents ou pour lesquels des coûts supplémentaires seraient à envisager ?

Tout d'abord, il convient de noter que plus une migration est complexe, plus les coûts associés sont élevés. Plusieurs critères permettent d'évaluer la complexité, et donc le coût, d'une migration :

- La typologie de l'application : par exemple, VMware, Nutanix, Bare Metal, Kubernetes, etc.
- Le nombre de couches et de serveurs : applications multi-tiers, monolithiques, etc.
- L'utilisation de fonctionnalités spécifiques à un fournisseur : ces fonctionnalités étant parfois propriétaires, elles peuvent présenter des dépendances aux infrastructures du même fournisseur et donc des barrières à la portabilité et l'interopérabilité.
- La taille de l'application : exprimée en téraoctets (To) ou en nombre de serveurs.
- Sa criticité et sa période d'ouverture (24/7 vs Jours ouvrés, résilience géographique...)

- Ces facteurs, combinés au contexte de la migration, notamment sa criticité, influencent directement la complexité et le coût du projet.

Selon le projet, plusieurs types de coûts peuvent donc intervenir :

- Le coût humain, qui peut relever des trois parties concernées (fournisseur initial, client, fournisseur de destination). Cela correspond à la facturation des services de conseil spécialisé ou d'assistance technique.
- Le coût d'outillage (logiciels de migration, outils de sauvegardes ou de restauration, outils de lecture de données, les valises*) qui relève du fournisseur de destination et peut dans certains cas relever du fournisseur initial s'agissant des impératifs de destruction de matériel.
- Le coût lié au transfert de données, facturé pas le fournisseur initial (cf. sujet traité dans les réponses précédentes)
- Aussi, pendant la durée d'une migration, notamment pour des enjeux de continuité de service, le client peut être amené à payer le coût du service cloud chez son fournisseur initial et celui de son fournisseur de destination, jusqu'à ce que la migration soit effective (coûts dits de "double run").

* L'utilisation de valises de transfert de données correspond au recours à des équipements physiques employés pour déplacer des volumes massifs de données directement vers ou depuis un datacenter. Cela peut être nécessaire non seulement pour des raisons de capacité, mais également pour renforcer la sécurité des transferts en évitant de transiter par des réseaux publics. Ces valises permettent de répondre aux exigences les plus élevées en termes de fiabilité et de protection des données.

Q18 : En ce qui concerne le premier ensemble de prestations identifié en section 2.2.1 (i.e. les prestations directement liées au processus de changement de fournisseur et autres que le transfert de données) susceptible d'être couvert par les lignes directrices de l'Arcep, partagez- vous l'analyse de l'Autorité selon laquelle ces prestations relèveraient principalement de la mise à disposition de main d'œuvre pour des actions de soutien spécifique ? Le cas échéant, quelles sont selon vous les catégories de coûts sous-jacents à des prestations ? Pour chacune de ces catégories, identifiez-vous des manières de déterminer les coûts effectivement supportés par le fournisseur d'origine ?

Nous partageons l'analyse de l'Autorité selon laquelle ces prestations relèveraient principalement de la mise à disposition de main d'œuvre ou de conseil pour des actions de soutien spécifique. Il est utile de noter que, aujourd'hui, ces coûts de main de main d'œuvre de migration sont plutôt pris en charge par le fournisseur destinataire dans le cadre d'une proposition commerciale globale.

D'autres coûts peuvent intervenir et sont matériels. En effet, dans certains cas, notamment lorsque des données sensibles ont été hébergées, le fournisseur d'origine peut par exemple être tenu de détruire les disques lors de la migration.

Q19 : Identifiez-vous d'autres prestations que devrait réaliser le fournisseur d'origine dans le cadre du processus de changement de fournisseur pour respecter ses obligations de facilitation du changement de fournisseur prévues par le règlement sur les données, notamment au regard des différentes étapes d'extraction, de transformation et de téléversement des données ? Le cas échéant, quels seraient les coûts supportés par le fournisseur d'origine associés à ces prestations ?

De manière générale, il convient de préciser que le changement de fournisseur serait grandement facilité si les fournisseurs de cloud étaient dans l'obligation, lorsqu'un de leur client leur exprime une demande de migration, de proposer une fonctionnalité d'export des données de cet utilisateur dans des formats standards qui constitueraient le rôle de formats « pivots », ensuite exploitables et traduisibles par les autres fournisseurs si des besoins d'adaptation sont nécessaires. Cela permettrait de gommer les spécificités d'implantation des différents fournisseurs de services cloud, levant de fait les verrous techniques au changement de fournisseur.

Q20 : Avez-vous d'autres remarques concernant les frais de changement de fournisseur autres que ceux liés aux transferts de données ?

Les prestations des Entreprises de Services Numériques (ESN), offrant parfois un accompagnement à la migration d'un utilisateur vers les services d'un autre fournisseur, sont considérées comme des frais de changement de fournisseurs. Ces frais sont légitimes, mais ne doivent pas servir de manière détournée de moyen pour certains fournisseurs de continuer à facturer des frais de transfert de données si ces derniers venaient à être interdits. Il est important que les autorités compétentes assurent cette transparence des frais de changement de fournisseurs afin de s'assurer que ces derniers, y compris dans le cadre des prestations des ESN, ne puissent servir à refacturer des frais de transfert de données.

3. Réduire les difficultés techniques liées au changement de fournisseur et au recours simultané à plusieurs fournisseurs de services *cloud*

Q21 : Avez-vous des remarques sur la liste des services cloud utilisée pour illustrer les services IaaS, tels que définis dans l'article 29, I de la loi SREN ? Identifiez-vous d'autres services qui répondent à cette définition ?

Pas de remarque.

Q22 : Que pensez-vous de ces typologies et définitions relatives aux autres services cloud mentionnés à l'article 29, I de la loi SREN ?

Pas de remarque.

Q23 : Partagez-vous la compréhension de l'Arcep quant à la distinction entre services « standards » et « spécifiques » ?

Nous partageons la compréhension de l'Autorité.

Il est toutefois important de noter que certains services sont aujourd'hui considérés comme « standards » sur le marché mais peuvent être pilotés par des acteurs leaders du marché, ce qui octroie à ces derniers un avantage concurrentiel sur leurs concurrents.

En effet, ces derniers décident de manière unilatérale des modifications apportées au standard, selon un calendrier non prévisible, et selon des besoins ou enjeux qui leur sont propres. Ces modifications étant régulières et parfois conséquentes, elles obligent les autres fournisseurs qui y ont recours à s'adapter de manière réactive en permanence pour assurer une compatibilité avec la nouvelle version de ces standards. Les conséquences sont :

- Des coûts d'opération importants : les fournisseurs alternatifs sont contraints d'investir dans des développements (donc du temps de travail humain) pour assurer la réplication avec les nouveaux API du standard dès leur publication et donc permettre à minima la compatibilité et si possible l'interopérabilité et la transférabilité de leurs données.
- Un retard systématique des concurrents : étant maîtres de la temporalité et de la définition des modifications apportées au standard, ces acteurs sont en mesure d'adapter leurs propres outils et services en amont de l'annonce des modifications, et donc de proposer ces services adaptés sans délai, ce que ne sont pas en mesure de faire ses concurrents.
- Un déficit d'interopérabilité : la majorité des concurrents ne parviennent pas à se conformer à 100% au nouveau standard du fait des coûts d'opération mentionnés et

de la faible durée de temps disponible pour se mettre en conformité afin d'assurer l'interopérabilité. Il est important de noter que certains des standards du marché ne proposent pas de système de référentiel permettant d'assurer la conformité d'un service avec le standard référencé. Cela rend donc d'autant plus difficile d'atteindre l'interopérabilité entre services via le standard.

Pour remédier à cela, les pouvoirs publics devrait songer à imposer une gestion collégiale de ce type de standard, assurée par un organisme de standardisation tiers et indépendant, seule solution viable pour garantir une interopérabilité effective et équitable entre les services des fournisseurs.

Nous attirons l'attention de l'Autorité sur le fait que cette gouvernance collégiale est possible et existe sur d'autres services. Kubernetes – qui est au départ un développement fait par Google - présente par exemple une gouvernance collégiale, assurée par la Cloud Native Computing Foundation.

Q24 : Dans quelle mesure les outils « cloud-agnostiques » couvrent-ils les besoins des utilisateurs afin de s'adapter aux différences entre les offres de services cloud, notamment afin de développer des architectures multi-cloud ? Identifiez-vous des besoins dans le périmètre des fonctionnalités couvertes par ces outils ?

Les outils cloud-agnostiques fonctionnent principalement comme des facilitateurs. En automatisant les tâches de configuration des services cloud, ces outils contribuent à simplifier certaines opérations. Cependant, ils agissent davantage comme des leviers de productivité, en particulier pour les infrastructures importantes ou évolutives, mais ne suppriment pas les différences entre les fournisseurs de cloud.

Nous considérons que les seuls outils ou services pouvant être véritablement considérés comme cloud agnostiques sont ceux standards dans le marché, et donc uniformes peu importe le fournisseur de cloud (ex : Kubernetes), levant de fait les barrières à l'interopérabilité ou la portabilité. OpenTelemetry, cité en exemple par l'Autorité, pourrait être considéré comme tel puisqu'il constitue un standard de fait et joue ainsi un rôle d'outil cloud-agnostique en apportant une certaine uniformité dans l'observabilité et les métriques.

À l'inverse, d'autres outils présentés comme cloud-agnostique ne le sont pas au sens strict du terme. Ces outils ont par exemple pour fonction de faciliter les déploiements en traduisant un langage commun pour divers fournisseurs, toutefois le code généré reste spécifique à chaque fournisseur de cloud, et le rôle de l'outil s'apparente ainsi davantage à celui d'un registre des différentes spécificités des services de chaque fournisseur qu'à une solution uniformisatrice, et donc cloud-agnostique, permettant la mise en workload d'un fournisseur à un autre.

En conclusion, il est de notre compréhension que les seuls outils véritablement cloud-agnostiques sont les services reconnus comme des standards dans le marché et dont la

gouvernance est collégiale. Cela conduit à une harmonisation des services entre les différents fournisseurs et donc à gommer les barrières techniques à l'interopérabilité et la portabilité.

Les autres outils désignés comme cloud agnostiques peuvent parfois faciliter à gommer certaines différences entre les services de fournisseurs cloud, ou renforcer la transparence sur ces dernières, mais ne constituent pas des outils permettant d'en faire abstraction.

Q25 : Que pensez-vous de la liste des éléments identifiés par l'Arcep comme entrant dans le champ de la définition des actifs numériques ? En identifiez-vous d'autres ?

Les éléments identifiés comme entrant dans le champ de la définition des actifs numériques sont cohérents, bien qu'il existe une porosité entre un actif numérique et la notion de données exportables, par exemple : les machines virtuelles comportent également des données et le contenu d'une base de données est forcément lié à une technologie.

Q26 : Cette description vous semble-t-elle refléter le processus « standard » de migration ? Identifiez-vous d'autres opérations ou actifs numériques nécessaires à la mise en œuvre de cette migration d'une application sur un service IaaS ? Le cas échéant, pouvez-vous les décrire ?

La description reflète effectivement un processus « standard » de migration, mais elle se limite principalement à la migration des machines virtuelles. Voici des éléments supplémentaires et d'autres actifs numériques nécessaires pour compléter et améliorer le processus de migration d'une application vers un service IaaS :

- Problématiques de conversion du code : La migration directe du code source peut poser des défis importants, notamment lorsque celui-ci est compilé avec des bibliothèques et des outils spécifiques à un système d'exploitation particulier. Une recompilation sur un autre système peut être nécessaire, ce qui est complexe et sujet à erreurs. C'est pourquoi il est plus logique de migrer des applications déjà compilées (binaires).
- Migration des bases de données : Actuellement, il n'existe pas de format d'export standardisé entre les fournisseurs de bases de données. Chaque système a son propre format, obligeant à des conversions complexes lors de l'importation dans une nouvelle base. Développer et exiger des formats d'export standardisés pour simplifier la migration des données semble nécessaire pour garantir la compatibilité entre bases de données.
- Scripts d'automatisation : Les scripts sont utiles pour migrer les données et métadonnées de manière cohérente et automatisée. Cependant, ils nécessitent une phase de tests approfondis pour garantir leur fiabilité et prévenir les problèmes de compatibilité.
- Applications portables : Les applications portables, comme celles exécutées via des conteneurs Docker, sont idéales pour une migration sans modification ni

recompilation. Elles facilitent le processus en permettant une exécution uniforme sur différents systèmes d'exploitation.

Q27 : Partagez-vous le constat de l'Arcep quant à l'absence de difficultés techniques significatives rencontrées lors de la migration d'applications reposant exclusivement sur des services IaaS ? Dans le cas contraire, quelles difficultés identifiez-vous et que suggérez-vous pour les résoudre ?

Nous partageons le constat de l'Autorité quant à l'absence de difficulté technique significative lors de la migration d'applications reposant exclusivement sur des services IaaS.

En théorie, toute migration IaaS est réalisable, mais il est important de souligner que ces migrations peuvent s'avérer complexes. Ces complexités peuvent découler de plusieurs facteurs :

- Différences de fonctionnalités entre fournisseurs : tous les fournisseurs IaaS ne proposent pas les mêmes fonctionnalités, ce qui peut compliquer une migration lorsque certaines fonctions critiques ne sont pas disponibles chez un autre fournisseur. Cela constitue toutefois davantage une contrainte fonctionnelle qu'un véritable verrouillage.
- Volume et infrastructures critiques : les migrations impliquant de larges volumes de données ou des infrastructures critiques peuvent être techniquement exigeantes. Elles nécessitent des efforts importants pour planifier et assurer la continuité des services, ce qui est particulièrement crucial pour les solutions utilisées quotidiennement par un grand nombre d'utilisateurs.
- Technologies, capacité et SLA : la complexité de la migration peut également dépendre des technologies sous-jacentes, de la capacité des infrastructures à gérer la transition, et des niveaux de service (SLA) attendus. Ces éléments peuvent exiger des ajustements pour garantir le bon déroulement de la migration.

Ces difficultés, bien qu'existantes, sont inhérentes aux services IaaS et ne sont pas le résultat de mécanismes de verrouillage. A ce titre, nous estimons que davantage de normalisation dans ce domaine n'est pas nécessaire.

Nous attirons toutefois la vigilance de l'Autorité sur la nécessité de s'assurer que les fournisseurs ne dressent pas d'entrave à la réversibilité des données de leurs clients, et donc qu'ils veillent à garantir à ces derniers un accès continu et pérenne à leurs données, mobilisable s'ils décident de les transférer vers un autre fournisseur.

Q28 : Que pensez-vous du constat de l'Arcep quant à l'absence de freins techniques à la réalisation de l'équivalence fonctionnelle pour les services IaaS ? Le cas échéant, quels sont ces freins et quels sont les services IaaS concernés ?

Les freins techniques à la réalisation de l'équivalence fonctionnelle pour les services IaaS sont effectivement peu nombreux. Cela s'explique principalement par la forte standardisation des services IaaS (et la nature même de ces services), et des systèmes d'exploitation permettant l'exécution de ces services (Operating Systems ; ex: Linux), relativement bien adoptés par les acteurs du cloud.

Comme mentionné dans la réponse à la Q27, certaines migrations IaaS peuvent être complexifiées par des défis techniques spécifiques. Cependant, nous estimons que davantage de normalisation sur ces sujets n'est pas nécessaire.

Q29 : Cette description vous semble-t-elle refléter le processus standard de migration ? Identifiez-vous d'autres opérations nécessaires à la mise en œuvre de cette migration ou d'autres éléments susceptibles d'être nécessaires pour déployer une application construite à l'aide des services PaaS de même type ? Le cas échéant, pouvez-vous les décrire ?

La description reflète certaines des étapes essentielles du processus de migration d'une application construite à l'aide de services PaaS, mais elle ne couvre pas l'ensemble des opérations nécessaires.

Une évaluation approfondie de l'application et de ses dépendances est indispensable pour réussir la migration. Il faut notamment identifier les services standardisés et ceux spécifiques au fournisseur PaaS actuel, en privilégiant l'utilisation de technologies open source pour réduire les verrouillages technologiques. Par ailleurs, la compatibilité avec des standards de fait doit être prise en compte lors de la sélection de la nouvelle plateforme.

La migration implique également des efforts sur plusieurs fronts, notamment la migration des données de l'application et la mise en œuvre de stratégies de sauvegarde et de reprise après sinistre adaptées. Des tests rigoureux des fonctionnalités, des performances et de la scalabilité doivent être réalisés pour garantir le bon fonctionnement de l'application sur la nouvelle plateforme. En outre, il est crucial de réévaluer les besoins en matière de sécurité et de conformité pour adapter les politiques aux nouvelles exigences.

Enfin, la transition vers la nouvelle plateforme nécessite une planification minutieuse pour minimiser les interruptions de service. L'adoption de nouveaux outils pour la gestion des déploiements, la surveillance et la journalisation des applications est également importante, tout comme la formation des équipes aux nouvelles technologies et processus. Ces étapes garantiront une migration fluide et un déploiement réussi de l'application.

Q30 : Partagez-vous le constat de l'Autorité selon lequel les difficultés techniques de migration d'application reposant sur des services PaaS sont principalement liées à l'utilisation de services spécifiques au fournisseur d'origine ? Sinon, quelles sont les autres difficultés techniques de migration, selon vous ?

Les principales difficultés techniques de migration d'application reposant sur des services PaaS sont en effet principalement liées à l'utilisation de services spécifiques au fournisseur d'origine.

Nous souhaitons toutefois porter deux points d'attention à l'Autorité quant à cette analyse :

1. La très grande partie des services cloud d'hyperscalers sont propriétaires, non open source, présentant donc des dépendances avec leurs propres infrastructures et donc des limites à l'interopérabilité et à la portabilité. Cela devient une véritable problématique concurrentielle lorsque ce type de services PaaS deviennent très adoptés sur un segment de marché, puisque cela contribue à l'enfermement technique des utilisateurs dans l'écosystème du fournisseur.
2. Certains « standards » sont en réalité pilotés par des fournisseurs eux-mêmes, de manière individuelle : tel que développé dans notre réponse à la Q23, cela a des incidences importantes sur l'interopérabilité globale avec ces standards et octroi à ces acteurs un avantage concurrentiel non négligeable sur la concurrence.

Pour ces raisons, l'action des pouvoirs publics devrait favoriser :

- L'instauration de format « pivots » standards : à notre sens, l'interopérabilité et la portabilité ne peuvent être garanties qu'à condition que soient introduits des standards réellement ouverts, permettant aux données d'être présentées dans un format « pivot » garantissant l'interopérabilité et la portabilité des données. Cela ne signifie pas que le fournisseur de services cloud soit dans l'obligation d'exploiter les données dans ce format « pivot », il peut le faire sur son format propriétaire, mais qu'il soit en revanche dans l'obligation de rendre possible l'extraction et l'export des bases de données dans ce format ouvert permettant de garantir l'interopérabilité et la portabilité. Pour cela, il est donc nécessaire de définir, au niveau de l'industrie, ou de préférence des pouvoirs publics, des standards ouverts pour les différents types de bases de données existantes, qui représenteront donc ces formats « pivots ». La définition de ces standards « pivots » devra nécessairement être associée à une obligation pour les fournisseurs de services cloud de proposer une fonctionnalité d'export dans ce format, afin d'assurer la présentation des données dans un format interopérable. Les spécificités d'implantation des différents fournisseurs de services PaaS ne seraient ainsi plus une barrière à l'interopérabilité et à la portabilité des bases de données, levant de fait les verrous techniques au changement de fournisseur.
- L'établissement de gestion collégiale des standards : afin que les standards de fait ne soient pas pilotés seulement par un acteur du marché mais plutôt par une fondation (ex : le standard Kubernetes est gouverné de manière collégiale par la Cloud Native Computing Foundation) ou des tiers (ex : pouvoirs publics, instituts de normalisation).

Q31 : Quels sont les services spécifiques des fournisseurs de cloud dont l'utilisation dans les applications constituent les principaux freins à la migration vers d'autres fournisseurs de cloud ? Que recommanderiez-vous de mettre en œuvre pour limiter les

freins à la migration vers d'autres fournisseurs, associés à l'utilisation de ces services ? Selon quelles priorités ?

Tel que développé en détail dans notre réponse à la Q50, nous estimons que les services spécifiques, donc propriétaires, de workflows, de bases de données, de stockage, de conteneurs et d'orchestration et de déploiement, de par leur large adoption dans le marché et les fonctions qu'ils servent, représentent les principaux freins à la migration en termes de services PaaS.

Nous développons plus en détails lors de notre réponse à la Q50 les solutions qui pourraient être envisagées pour lever ces freins.

Q32 : Partagez-vous le constat de l'Autorité quant à l'existence de difficultés techniques de migration liées aux services auxiliaires ? Le cas échéant, quels services auxiliaires constituent les principaux freins à la migration vers d'autres fournisseurs de cloud ? Que recommanderiez-vous de mettre en œuvre pour limiter ces freins ? Selon quelles priorités ?

Nous partageons le constat de l'Autorité concernant les difficultés techniques de migration liées à certains services auxiliaires, en particulier dans les domaines où les standards sont insuffisants ou absents, et où les divergences entre fournisseurs créent des barrières significatives à la portabilité et l'interopérabilité des services.

Les services IAM (Identity and Access Management) constituent un des services aux barrières techniques les plus importantes. Cela s'explique par plusieurs éléments :

- L'absence de standardisation existante : si la gestion des identifiants de connexion bénéficie aujourd'hui de standards bien définis, les moteurs d'autorisation (2ème composante des services d'IAM) posent des défis beaucoup plus complexes et ne bénéficient pas de norme existante au niveau du marché ou des autorités de normalisation.
- L'hétérogénéité des services : en l'absence de consensus sur les syntaxes et les approches pour exprimer les autorisations, ces moteurs varient considérablement entre fournisseurs due aux différences fonctionnelles et au découpage de droits différent sur des services proches, rendant les traductions complexes, malgré des fonctionnalités finales similaires.
- L'imbrication des services IAM au sein d'autres services : la nature même des services IAM (qui gèrent les accès et autorisations à des services ou données d'un utilisateur) fait qu'ils s'imbriquent profondément dans l'architecture globale des utilisateurs et impliquent une grande quantité de services (notamment les services pour lesquels des gestions d'accès et d'autorisations sont définis).

Au-delà de la migration du service d'IAM en lui-même, la migration vers un autre fournisseur implique ainsi un retravail technique complet de l'architecture afin de réadapter l'ensemble des services au sein desquels l'IAM est imbriqué dans le fournisseur de destination.

De fait, les services IAM présentent des freins techniques majeurs à la migration et au multcloud.

Pour limiter ces freins, nous recommandons de prioriser d'engager des travaux pour faciliter l'harmonisation syntaxique des moteurs d'autorisation. Toutefois, une uniformisation complète des syntaxes nécessiterait des modifications profondes des systèmes existants, ce qui serait lourd pour les fournisseurs. Une solution plus pragmatique serait d'exiger que chaque fournisseur permette l'exportation de ses politiques IAM dans un format standardisé. Ce format, pouvant être traduit automatiquement dans différentes syntaxes, garantirait l'interopérabilité et la portabilité sans imposer des révisions massives des systèmes. Il serait aussi nécessaire d'harmoniser les niveaux de droits possibles sur des produits similaires de différents fournisseurs avec qu'au-delà de la syntaxe les politiques IAM puissent exprimer les mêmes droits.

De la même manière, l'Autorité doit être informée des difficultés similaires que peuvent rencontrer les utilisateurs sur un autre type de service auxiliaire : les services KMS (Key Management Systems). Lors de la migration de bases de données ou d'autres systèmes sécurisés, le transfert des clés de chiffrement est essentiel pour préserver la sécurité des données et garantir leur exploitabilité. Or, cette migration peut aujourd'hui s'avérer complexe en raison du manque d'harmonisation des solutions existantes. A contrario des IAM, un standard pertinent existe pourtant : le Key Management Interoperability Protocol (KMIP), sous la gouvernance d'OASIS, et pourrait répondre à ces besoins. Nous recommandons vivement l'adoption et la promotion de ce standard pour faciliter l'interopérabilité et la portabilité des services KMS.

Q33 : Cette description vous semble-t-elle refléter le processus standard de migration d'un logiciel SaaS ? Dans le cas contraire, quel serait le processus standard de migration d'un logiciel SaaS ?

Pas de remarque.

Q34 : Identifiez-vous des difficultés pour la récupération des données liées à l'utilisation d'un service SaaS ? Si oui, dans quel contexte ?

Pas de remarque.

Q35 : Confirmez-vous que la détermination du périmètre des données exportables constitue un enjeu particulier s'agissant des services SaaS pour les clients ? Identifiez-vous des difficultés de définition du périmètre des données exportables pour les autres services ? Le cas échéant, lesquelles et pour quels services ?

Pas de remarque.

Q36 : Comment définissez-vous, dans le cadre des contrats liants un clients à un fournisseur de services cloud, le périmètre des données exportables ?

Dans ses CGS en ligne, OVHcloud vise les "Contenus" de manière large comme désignant "toutes les informations, données, fichiers, systèmes, logiciels, applications, sites internet et autres éléments reproduits, hébergés, collectés, stockés, transmis, diffusés, publiés, et plus généralement utilisés ou exploités par le Client et/ou les Utilisateurs dans le cadre des Services" dont il est affirmé, à l'article 6 de nos CGS, qu'ils sont "la propriété du Client, des Utilisateurs ou des tiers qui lui ont concédé le droit de les utiliser" et sur lesquels par conséquent "OVHcloud n'exerce aucun contrôle a priori (ni) n'a (...) connaissance de ces (Contenus) (ni) n'intervient (...) dans (leur) gestion (ni) n'effectue aucune opération de validation ou de mise à jour de (ces) Contenus" puisque seul "le Client a la connaissance et le pouvoir de contrôle sur les Contenus (et) lui seul connaît le type de Contenus (sensible, public, confidentiel, etc.), si les Contenus contiennent des données à caractère personnel et de quel type, et la criticité du Contenu (importance vitale, données de test, données de production, etc.)". Cette définition de "Contenus" inclut donc la notion de "données exportables" au sens de de la loi SREN et du Data Act, voire la notion d'"actifs numériques".

Q37 : Pouvez-vous décrire de manière concrète les difficultés que rencontrent les clients et les fournisseurs de services cloud lorsqu'il doivent convenir du périmètre des données exportables liés à l'utilisation de services SaaS ?

Pas de remarque.

Q38 : Identifiez-vous d'autres difficultés techniques en cas de changement de fournisseur, que vous souhaitez porter à la connaissance de l'Arcep ?

Pas de remarque.

Q39 : Que pensez-vous de la description présentée par l'Autorité des différents modèles d'architectures multi-cloud et des besoins d'interopérabilité correspondants ?

La description présentée par l'Autorité reflète notre vision des différents modèles d'architectures multi-cloud et des besoins d'interopérabilité correspondants.

Q40 : Pour quels cas d'usage, présents ou futurs, une architecture «multi-cloudintégrée» vous semble-t-elle particulièrement souhaitable ? Identifiez-vous des freins à l'interopérabilité empêchant d'y parvenir ? Le cas échéant, quels sont ces freins, que recommanderiez-vous de mettre en œuvre pour les limiter ces freins et selon quelles priorités ?

Une architecture multi-cloud intégrée est particulièrement pertinente pour plusieurs cas d'usage, actuels et futurs. Elle permet d'optimiser la migration des workloads entre clouds afin de répondre aux besoins en coûts, performance ou disponibilité, et de tirer parti des services spécifiques proposés par différents fournisseurs. Elle renforce également la résilience et la haute disponibilité en répartissant les charges de travail et les données sur plusieurs plateformes pour limiter les risques de défaillance d'un fournisseur unique.

Cependant, plusieurs freins à l'interopérabilité peuvent entraver la mise en œuvre d'une telle architecture. Les incompatibilités technologiques entre fournisseurs compliquent la communication entre services. La gestion des environnements multi-cloud est complexe et peut entraîner des erreurs, tandis que les divergences en matière de sécurité et de conformité ajoutent des défis. Pour surmonter ces obstacles, il est crucial d'adopter des normes favorisant l'interopérabilité et de centraliser la gestion grâce à des outils adaptés.

Q41 : Partagez-vous la compréhension de l'Autorité selon laquelle l'interopérabilité des services cloud requiert des API disponibles, stables, documentées et accessibles depuis l'extérieur de l'écosystème de leur fournisseur ? Pourquoi ?

Nous partageons la compréhension de l'Autorité. Il convient toutefois de mentionner qu'une API est avant tout un contrat d'interface avec les clients, ce qui rend sa stabilité, sa documentation, sa disponibilité et son accessibilité essentielles, non seulement pour l'interopérabilité, mais premièrement pour sa consommation par l'utilisateur et son fonctionnement même.

Afin de faciliter l'interopérabilité des services cloud, nous attirons l'attention de l'Autorité sur le fait qu'au-delà de ces éléments, la cohérence des API est également essentielle. Cette cohérence est importante sous deux aspects principaux :

- Catégorie de l'API : les APIs peuvent être « synchrones » (renvoyant immédiatement une réponse à la requête) ou « asynchrones » (renvoyant une promesse ou un événement pour signaler que la réponse est disponible). L'interopérabilité entre deux services de fournisseurs différents sera nécessairement plus complexe et les services plus difficiles pour utilisation parallèle si la catégorie de l'API proposée est différente d'un fournisseur à un autre.
- Champs / Attributs : les API sont composées de nombreux "attributs" faisant référence à des composants de ces API notamment pour désigner des ensembles de données spécifiques (ex : information utilisateur, information produit, information commande). Or, si les API ont parfois des champs ou attributs aux fonctionnalités identiques, la façon dont ces derniers sont nommés ou configurés peut varier, entraînant des barrières techniques à l'interopérabilité avec d'autres services similaires.

La cohérence des API, qui suppose une cohérence entre les catégories, champs et attributs aux fonctions similaires, est donc essentielle pour l'interopérabilité des services cloud.

Q42 : Afin de favoriser l'interopérabilité des services de cloud, pouvez-vous détailler :

- **Quelles informations minimales devraient être renseignées à votre sens dans la documentation des API pour assurer une interopérabilité entre services cloud ?**
- **Selon quels critères estimez-vous qu'une API est suffisamment stable ? Quelles conditions les mises à jour de ces API devraient-elles respecter afin de permettre à l'utilisateur d'anticiper et d'adapter son usage de ces services ?**

Concernant les informations minimales devant être renseignées :

Il est impératif que la documentation des API inclue l'ensemble des éléments nécessaires pour permettre une utilisation correcte et optimale par les utilisateurs. Cela implique notamment : une description de chaque champ de l'API, le format attendu pour chacun d'entre eux, les cas d'erreurs, les outputs, préciser si le retour est synchrone ou asynchrone etc.

Pour préserver la stabilité des API et permettre aux utilisateurs de s'adapter aux évolutions, et donc de maintenir une interopérabilité, il est également essentiel de notifier à l'avance tout changement majeur dans cet API. Bien que les changements majeurs soient rares et déconseillés après la publication d'une version 1.0, leur gestion doit être rigoureuse. Lorsqu'un changement majeur est inévitable, une communication claire et un délai de préavis adapté sont nécessaires. Ce délai doit tenir compte du nombre de services concernées et de la capacité des organisations utilisant ces API à absorber les modifications sans interruption significative du service. Nous recommandons un préavis de 6 à 12 mois pour assurer une transition fluide et minimiser les impacts. Sans cela, certaines évolutions apportées à des API pourraient avoir des conséquences majeures sur la capacité des fournisseurs à permettre l'interopérabilité de leurs services, et entraîner des travaux importants pour se mettre en compatibilité.

Concernant la stabilité des API :

Comme expliqué plus haut, la prévenance vis-à-vis des changements et évolutions apportées aux API est un point clef, particulièrement pour les changements majeurs ("breaking changes"). Des normes existent pour permettre la gestion sémantique des différentes versions et ainsi offrir une méthode de communication des évolutions : par exemple la norme SemVer (Semantic Versioning). Cette méthode de numérotation des versions offre une clarté essentielle en indiquant explicitement les nouvelles fonctionnalités, les corrections de bugs et les modifications majeures susceptibles de rompre la compatibilité.

La stabilité des API pourrait être évaluée en fonction de leur cohérence avec les méthodes proposées par les normes de ce type. En effet cela permettrait aux utilisateurs et fournisseurs tiers de comprendre aisément la portée des évolutions et d'ajuster leur utilisation en conséquence, participant de fait à l'utilisation stable d'une API.

Q43 : Identifiez-vous d'autres modèles d'interopérabilité entre systèmes informatiques que les API ? Le cas échéant, lesquels ?

Il existe effectivement d'autres modèles d'interopérabilité entre systèmes informatiques en dehors des API. Cependant, ces alternatives se révèlent souvent moins efficaces et moins pratiques dans leur mise en œuvre. Les API restent, à ce jour, la norme de référence pour garantir une interopérabilité performante et flexible entre différents systèmes.

Q44 : Identifiez d'autres enjeux et difficultés techniques relatifs au changement de fournisseur et au développement du multi-cloud ?

Pas de remarque.

Q45 : Parmi les codes de conduite et recommandations d'application volontaire dont vous auriez connaissance, pouvez-vous indiquer les préconisations qui vous semblent pertinentes afin de préciser les règles et modalités de mise en œuvre des exigences essentielles prévues au II de l'article 28 de la loi SREN ?

Pas de remarque.

Q46 : Quelles sont les mesures actuellement mises en œuvre par les fournisseurs de services cloud afin de faciliter une équivalence fonctionnelle entre services IaaS qui couvrent le même type de fonctionnalités ? Quelles mesures supplémentaires permettraient de faciliter cette équivalence fonctionnelle ?

Comme indiqué à la réponse à la Q28, la bonne équivalence fonctionnelle entre services IaaS s'explique principalement par la forte standardisation des services IaaS (et la nature même de ces services), et des systèmes d'exploitation permettant l'exécution de ces services (Operating Systems ; ex: Linux), relativement bien adoptés par les acteurs du cloud.

Q47 : Quelles informations minimales devrait contenir, selon vous, l'offre de référence technique d'interopérabilité prévue par la loi SREN afin de permettre la bonne information des utilisateurs ?

L'offre de référence technique d'interopérabilité prévue par la loi SREN doit garantir une transparence optimale et fournir aux utilisateurs toutes les informations nécessaires à une utilisation efficace et informée des services.

Le prérequis de cette offre sera en effet d'indiquer si ces services sont des services spécifiques ou standards et, dans le cas de ces derniers, sur quels standards techniques ils reposent.

L'offre de référence devra nécessairement proposer une documentation complète. Cette dernière devra notamment détailler :

- Les moyens d'extraire les données du service dans un format documenté et à un coût raisonnable (ex : via un kit de développement permettant de lire la donnée).
- Les attributs disponibles.
- Les mécanismes de gestion des cas d'erreur.
- La description des outputs.
- La nature des retours (synchrone ou asynchrone).
- La gestion des évolutions ou de la fin de l'API.
- Les API de configuration (control plane) et d'utilisation (data plane) du service et – de préférence – leur éventuelle conformité avec des standards existants.

Cette documentation doit être cohérente dans sa syntaxe et son organisation, notamment en ce qui concerne les évolutions, pour assurer une utilisation intuitive et standardisée.

Il semble pertinent, pour favoriser l'interopérabilité et la facilité d'utilisation, que cette documentation soit fournie dans un format standardisé. La spécification OpenAPI, par exemple, apparaît comme une solution adaptée, car elle permet de décrire une API de manière structurée, sans exiger l'accès au code source ni à une documentation supplémentaire. Cette standardisation faciliterait l'adoption et l'intégration par les utilisateurs.

Q48 : Que pensez-vous de la proposition d'utiliser l'offre de référence technique d'interopérabilité pour informer les utilisateurs de la spécificité des services cloud, et d'en harmoniser la forme ?

L'utilisation de l'offre de référence technique d'interopérabilité semble pertinente afin d'informer les utilisateurs de la spécificité des services cloud.

Cela permettra aux consommateurs de mieux appréhender et anticiper leurs choix de services cloud, en prenant en compte leurs impacts à long terme, y compris dans des perspectives de migration ou de multicloud.

L'harmonisation est un point important puisqu'il garantira une transparence accrue et la comparaison des services sur une base comparable. En harmonisant la forme de la référence technique d'interopérabilité, le risque de voir des fournisseurs présenter leurs services comme interopérables alors qu'ils ne le sont pas véritablement sera amoindri, au bénéfice de l'information des utilisateurs.

Q49 : Partagez-vous le constat de l'Autorité quant au faible besoin de normalisation supplémentaire des services IaaS ? Dans le cas contraire, quels services et aspects de ces services devraient faire l'objet de travaux de normalisation, sous quelles formes et pour quelles raisons ?

Nous partageons l'analyse de l'Autorité, tout en attirant sa vigilance sur les points d'attention mentionnés dans notre réponse à la Q27.

Q50 : Partagez-vous l'analyse de l'Arcep concernant le besoin de normalisation des services PaaS ? Le cas échéant, quels services et aspects des services PaaS devraient faire l'objet de travaux de normalisation, sous quelles formes et pour quelles raisons ?

Il existe en effet des difficultés techniques d'interopérabilité et de portabilité liées aux services PaaS non standards, donc spécifiques. Il semble donc crucial d'engager certains travaux de normalisation.

Comme mentionné lors de notre réponse à la Q30 : l'interopérabilité et la portabilité seraient grandement favorisés par l'introduction des standards réellement ouverts, permettant aux données d'être présentées dans un format « pivot » garantissant l'interopérabilité et la portabilité des données. Cela ne signifie pas que le fournisseur de services cloud soit dans l'obligation d'exploiter les données dans ce format « pivot », il peut le faire sur son format propriétaire, mais qu'il soit en revanche dans l'obligation de rendre possible l'extraction et l'export des bases de données dans ce format ouvert permettant de garantir l'interopérabilité et la portabilité. Pour cela, il est donc nécessaire de définir, au niveau de l'industrie, ou des pouvoirs publics, des standards ouverts pour les différents types de bases de données existantes, qui représenteront donc ces formats « pivots ». La définition de ces standards « pivots » devra nécessairement être associée à une obligation pour les fournisseurs de services cloud de proposer une fonctionnalité d'export dans ce format, afin d'assurer la présentation des données dans un format interopérable. Les spécificités d'implantation des différents fournisseurs de services PaaS ne seraient ainsi plus une barrière à l'interopérabilité et à la portabilité des bases de données, levant de fait les verrous techniques au changement de fournisseur.

Parmi ces typologies de services, nous considérons comme prioritaire d'engager des travaux de normalisation sur les services suivants :

- Workflows : ces services sont aujourd'hui largement adoptés dans le marché en raison de leur rôle d'automatisation de tâches et donc des gains d'efficacité qu'ils permettent (par exemple dans les Ressources Humaines, le service workflow permet la gestion des demandes de congés automatiquement). L'absence de standardisation de ces outils entraîne des difficultés majeures en termes d'interopérabilité et de migration, d'autant plus que les métadonnées mobilisées sont souvent spécifiques à l'outil utilisé. Des travaux de standardisation, notamment autour des formats de définition de workflows (comme BPMN ou CWL) et des API, permettrait de rendre ces outils plus interopérables et adaptés à des environnements hybrides ou multicloud.
- Bases de données : les services PaaS de bases de données sont aujourd'hui largement adoptés dans le marché du cloud mais restent, pour beaucoup, proposés dans des formats propriétaires. En particulier : les fournisseurs PaaS proposent des APIs spécifiques pour gérer leurs bases de données (création, mise à jour, sauvegarde, restauration), limitant leur interopérabilité. Des travaux pour

harmoniser les APIs les bases de données relationnelles permettraient aux développeurs de travailler avec le même ensemble de commandes, quel que soit le fournisseur et favoriserait ainsi l'interopérabilité. De même, il n'existe pas de format commun pour l'extraction des données hébergées dans services propriétaires, rendant la migration de services PaaS de bases de données d'un fournisseur à un autre complexe. La migration serait ainsi facilitée si, sans standardiser le service lui-même, l'extraction de ces données lors de la migration se faisait dans un format d'export standard (par exemple basés sur des standards comme JSON ou Avro), reconnaissable et utilisable par les autres fournisseurs.

- Stockage : les services PaaS de stockage de données sont aujourd'hui indispensables sur le marché du cloud. Il n'existe toutefois pas de standard ouvert et à la gestion collégiale sur le marché. De fait les standards existants sont pilotés par des acteurs leaders du marché, selon des calendriers et intérêts qui leur sont propres, tel que décrit à la réponse à la Q30. De plus, ces standards n'incluent parfois pas des fonctionnalités avancées telles que le versioning ou la gestion des métadonnées, qui sont pourtant largement adoptées dans le marché. Des travaux pour permettre une gestion collégiale des standard liés au stockage de données seraient bénéfiques à l'interopérabilité et la migration dans le secteur du cloud.
- Conteneurs et d'orchestration : ces services sont aujourd'hui largement adoptés par les utilisateurs du cloud, en particulier grâce au développement du service Kubernetes. Si Kubernetes constitue de fait un standard open source dans le marché, avec une gestion collégiale assurée par la Cloud Native Computing Foundation, donc interopérable, les extensions propriétaires apportées à Kubernetes (par exemple pour la gestion de réseau et de stockage) ne sont pas interopérables. Combiné à la forte adoption des services de conteneurs et d'orchestration dans le marché, l'adoption de ces variantes propriétaires conduit à dresser de nouvelles barrières techniques au changement de fournisseur et à l'interopérabilité malgré la base ouverte que constitue Kubernetes. Des travaux seraient ainsi pertinents pour assurer l'interopérabilité des extensions à Kubernetes proposées par les fournisseurs de cloud.
- Déploiement d'applications : le déploiement d'applications dans le cloud nécessite des services nécessaires permettant la configuration générale de l'application, le choix de son infrastructure et de ses composants etc. Or, ces services sont aujourd'hui très différents d'un fournisseur à l'autre, conduisant l'utilisateur à devoir ré écrire en grande partie la configuration générale de son application lors du changement de fournisseur. La promotion de standards pour permettre le déploiement de ces applications dans le cloud faciliterait le déploiement d'application depuis n'importe quel service PaaS et donc, lèverait une barrière technique à l'interopérabilité ou au changement de fournisseur.

Une plus grande harmonisation de ces différents types de services permettrait ainsi de lever de nombreuses barrières pour permettre à l'utilisateur de quitter son fournisseur initial, et de porter ses applications et données pour les ré exécuter dans les services d'un autre fournisseur. Ils constituent ainsi la priorité sur laquelle devraient se pencher les pouvoirs publics dans le cadre de leurs travaux pour lever les freins techniques au changement de fournisseur sur les services PaaS.

Il existe également des mécanismes de verrouillage technique liés aux services PaaS apparaissant dans le cadre de l'émergence de l'Intelligence Artificielle, dont l'Autorité doit être informée.

L'entraînement d'un modèle IA suppose en effet l'accès à des infrastructures mais aussi des compétences techniques accrues et un investissement de temps important pour tester différentes hypothèses et obtenir un résultat performant. Pour répondre à cette problématique, les fournisseurs de cloud proposent des solutions automatisées dites de 'Machine Learning' (Auto-ML). Ces solutions PaaS permettent un certain degré d'automatisation et de simplification de cet entraînement, en permettant à l'utilisateur de simplement fournir ses données et préciser l'objectif qu'il souhaite atteindre afin que la solution effectue le travail d'entraînement elle-même et produise le modèle. Certains fournisseurs utilisent toutefois ces solutions AutoML à des fins de verrouillage en les rendant disponibles seulement dans des formats propriétaires et non transparent. Ces solutions produisent le modèle final, mais ne donnent pas à l'utilisateur l'accès au fichier source de ce modèle. Sans cela, et sans visibilité sur la façon dont son modèle a été entraîné, l'utilisateur n'a aucun contrôle sur son modèle et ne peut le déployer que sur les infrastructures du fournisseur ayant réalisé l'entraînement. L'utilisateur est ainsi verrouillé dans les infrastructures de ce fournisseur, puisque répliquer son modèle chez un autre fournisseur l'obligerait à réengager le processus d'entraînement depuis le début, entraînant de fait de nouvelles ressources financières et humaines importantes. Le même fonctionnement s'observe sur les solutions de « fine-tuning » (solutions permettant de spécialiser un modèle existant à partir de données spécifiques). L'opération de fine-tuning est effectuée par le fournisseur lui-même, sans transparence avec l'utilisateur, et le modèle est exploitable seulement à partir de ses infrastructures. Ce verrouillage technologique conduit les utilisateurs de solutions IA à se trouver enfermés dans les services de leur fournisseur d'entraînement, et de voir leurs modèles consommables exclusivement à partir des infrastructures cloud de ces derniers – le modèle final n'étant ni portable vers un autre fournisseur, ni interopérable avec d'autres infrastructures, par exemple pour l'inférence - conduisant à une captation du marché par ces acteurs. Alors que l'émergence de l'IA représente un potentiel massif pour les opérateurs du secteur du cloud, le manque de portabilité et d'interopérabilité des services PaaS de Machine Learning porte le risque de voir les utilisateurs de ces solutions se retrouver enfermés dans les infrastructures de ces fournisseurs.

Q51: Que pensez-vous d'initier des travaux de normalisation sur les services auxiliaires, notamment sur les services IAM ? Outre ce type de services, d'autres services auxiliaires devraient-ils faire l'objet de tels travaux et selon quelles priorités ?

Nous constatons un manque de solutions techniques et d'initiatives visant à standardiser les services auxiliaires, notamment dans le domaine des services IAM. Nous partageons donc l'avis qu'il s'agit d'un enjeu majeur, d'autant plus compte tenu du fait que les services

IAM impactent souvent l'architecture plus générale des utilisateurs, puisque s'imbriquant au sein des autres services.

Pour envisager cette normalisation, il est important de distinguer les différents composants d'un service IAM :

- La gestion des identifiants de connexion : pour laquelle il existe aujourd'hui des standards bien définis et relativement simples (OIDC, SAML...).
- Les moteurs d'autorisations : la situation devient beaucoup plus complexe. Ces moteurs présentent des structures granulaires et variées, avec des approches divergentes selon les fournisseurs, faute de consensus sur la manière d'exprimer les autorisations. De fait, la migration de tels services d'un fournisseur à un autre est très complexe et a des impacts sur l'ensemble des services considérés par ces autorisations (ex : un utilisateur ne migrera pas une base de données sensibles si cette dernière risque, après la migration, d'être accessible à un grand nombre de personnes). Cela crée un besoin urgent d'harmonisation syntaxique pour permettre une meilleure traduction des architectures.

L'enjeu principal se situe ainsi sur l'harmonisation des syntaxes des moteurs d'autorisation. Il s'agira toutefois de prendre en compte qu'une uniformisation de ces syntaxes en partant de zéro obligerait chaque fournisseur à réécrire intégralement son système, impliquant des travaux massifs pour chaque fournisseur de solutions IAM et impactant certainement les fournisseurs les plus petits que les grands fournisseurs bénéficiant de ressources techniques importantes.

La solution la plus pragmatique serait d'imposer non pas une uniformisation syntaxique, mais l'obligation pour chaque fournisseur d'exporter sa politique IAM dans un format standardisé. Ce format pourrait ensuite être traduit automatiquement dans différents langages selon les besoins, évitant ainsi des modifications profondes des systèmes existants de chaque fournisseur, tout en répondant aux impératifs d'interopérabilité et de portabilité.

Concernant les autres services auxiliaires : les services KMS (Key Management Systems), qui gèrent les clés de chiffrement, méritent également une attention particulière de l'autorité. Lorsqu'une base de données est déplacée, il est indispensable de pouvoir transférer les clés de chiffrement associées à ces services, sous peine de grandement mettre en danger la sécurité de certaines données des organisations ou de rendre ces données inexploitable. À cet effet, un standard existe déjà dans le marché : le Key Management Interoperability Protocol (KMIP), sous la gouvernance de l'organisation OASIS. L'adoption de ce standard serait, à notre avis, à même de favoriser l'interopérabilité des services KMS.

Q52 : Que pensez-vous du besoin de normaliser notamment les structures et les formats d'échanges de données entre des services SaaS du même type ? Le cas échéant, quels types de services SaaS devraient faire l'objet de tels travaux en priorité ? Pour quelle raison ?

Pas de commentaire.

Q53 : Avez-vous d'autres commentaires sur les enjeux soulevés dans cette consultation publique ?

Pas de commentaire.

Q54 : Au-delà de tous les sujets abordés dans les sections précédentes de cette consultation, quels autres enjeux relatifs à la régulation des services cloud mériteraient, selon vous, d'être portés à l'attention de l'Arcep ?

Nous attirons l'attention de l'Autorité sur le risque de voir l'émergence de l'Intelligence Artificielle, dont les services cloud constituent un intrant essentiel, renforcer certaines dynamiques et pratiques anticoncurrentielles au sein du marché du cloud.

Le vivier de croissance que représente ce segment incite certains acteurs à user de pratiques parfois déloyales pour attirer les utilisateurs d'IA dans leurs infrastructures et ensuite les verrouiller. Nous notons en particulier les dynamiques suivantes :

- Persistance des pratiques de verrouillage des utilisateurs
- Verrouillage financier : certains fournisseurs de cloud utilisent leurs moyens supérieurs pour offrir aux startups de l'IA des montants de crédits cloud que les fournisseurs alternatifs ne peuvent simplement pas égaler. Dans un secteur nécessitant des investissements massifs en capacité GPU pour l'entraînement des modèles, ces programmes disproportionnés de crédits cloud ont pour conséquence d'inciter les startups de l'IA à rejoindre les services de ces fournisseurs de cloud non pas car ils correspondent le mieux à leurs besoins spécifiques à moyen terme, mais en raison du montant de crédits cloud qui leur est proposé. L'Autorité de la concurrence française a ainsi souligné dans son récent avis sur l'IA générative que les crédits cloud pourraient ainsi avoir pour effet de verrouiller ces entreprises au sein des écosystèmes des hyperscalers, notamment en raison des freins techniques et tarifaires existants à la migration. Alors que les programmes de crédits cloud portaient précédemment jusqu'à 200 000€ par startup (montant déjà bien supérieur à celui proposé par les fournisseurs alternatifs), ces programmes qui visent désormais les start ups de l'IA ont récemment été augmentés à 300 000 ou 350 000€ par startup. Les fournisseurs alternatifs ne sont pas en capacité de proposer de tels montants. Cette situation conduit à une capture de l'écosystème IA dans les infrastructures de ces fournisseurs de cloud.
- Verrouillage technique : à travers l'enfermement des modèles dans les infrastructures du fournisseur de la solution d'entraînement (ainsi que présenté dans la réponse à la Q50)
- Renforcement des abus de position à partir de marchés adjacents :

- Ventes liées : Les fournisseurs de solutions IA également présents sur d'autres marchés adjacents, notamment le marché logiciel, peuvent utiliser leurs positions sur ces derniers pour s'approprier le marché de l'IA à travers des pratiques de vente liée ou de groupement de logiciels. Cela se traduit par l'intégration, par exemple dans des suites logicielles dominantes ou moteurs de recherche, de produits IA ainsi proposés à moindre prix et/ou directement intégrés dans les offres. La conséquence est que les utilisateurs de ces suites logicielles ou autres services deviennent de fait utilisateurs des solutions IA proposées par leur éditeur initial, permettant à ce dernier de s'approprier le marché.
- Auto-préférence : certains fournisseurs de cloud intégrés proposant également des solutions d'IA ne rendent disponible ces solutions que depuis leurs infrastructures cloud. Alors que certaines de ces solutions sont directement intégrés dans des produits numériques largement adoptés, le risque est important de voir les utilisateurs de ces produits – logiquement intéressés par les nouvelles fonctionnalités IA proposées - contraints de migrer vers les infrastructures cloud du fournisseur de la solution d'IA, alors même que la suite logicielle pouvait être précédemment déployée sur les infrastructures de fournisseurs de cloud tiers.

Alors que certains acteurs du numérique bénéficient déjà, initialement, d'un accès privilégié aux intrants essentiels à l'IA (données, talents, capacités de calcul), la persistance ou le renforcement de ces pratiques porte le risque sérieux de voir l'émergence de la technologie renforcer la concentration d'un marché du cloud déjà concentré à plus de 70% autour de 3 acteurs. La vigilance des autorités sur ces dynamiques est donc plus importante que jamais.