

| THEMATIQUE | NUMERO | PAGE | QUESTION | Proposition de réponse Hexatrust |
|--|--------|------|---|--|
| Frais de transfert Pratiques tarifaires | 1 | 12 | Avez-vous des observations sur les éléments de contexte liés aux pratiques tarifaires présentés ci-avant ? | Les pratiques tarifaires des fournisseurs de services cloud sont hétérogènes, avec des approches variées pour la facturation des transferts de données lors d'un changement de fournisseur. Certains offrent des transferts gratuits ou à coût marginal, tandis que d'autres facturent selon le volume transféré, avec des coûts variant par région et des options premium payantes. Depuis janvier 2024, le règlement européen impose que ces frais ne dépassent les coûts réels, et certains acteurs (Google, AWS, Azure) annoncent la gratuité, mais avec des démarches administratives dissuasives, partielles et qui ne constituent pas réellement la fin des frais de transfert. Ainsi ces pratiques, souvent non transparentes et parfois élevées malgré des coûts réels faibles, restent un obstacle pour les entreprises. Une harmonisation des conditions et une meilleure transparence sont nécessaires pour faciliter la portabilité et renforcer la compétitivité du marché. |
| | 2 | | 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 ? | Les coûts identifiés par l'ARCEP correspondent à ceux inhérents des activités habituelles d'un fournisseur cloud. Leur facturation n'est donc pas justifiée ni techniquement ni économiquement mais vise plutôt à enfermer l'utilisateur dans un service. Néanmoins, la mise en place de réseau spécifique (privés à la demande du client) entraîne des coûts. Il faudrait donc isoler les interconnexions spécifiques et les réseaux privés du reste, notamment en inscrivant la notion d'activités habituelles dans les CGV. |
| | 3 | | 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. | <p>En dehors d'activités spécifiques réglementées, le constat est partagé par les répondants auquel il faut ajouter : les coûts des adresses IP, les coûts des infrastructures de sécurité, les coûts opérationnels ainsi que la location d'espaces pour opérer le matériel dans les centres d'interconnexion. Parmi les autres coûts à prendre en compte, Hexatrust attire l'attention de l'ARCEP sur ceux-ci :</p> <ol style="list-style-type: none"> Coûts liés à la sécurité des transferts <ul style="list-style-type: none"> Chiffrement et protection des données en transit : <ul style="list-style-type: none"> >> Mise en œuvre de protocoles de chiffrement pour garantir la confidentialité et l'intégrité des données. >> Maintenance et gestion des clés de chiffrement. >> Clés de chiffrement fournies par le fournisseur du service ou fournies par le client > Surveillance et prévention des intrusions : >> Détection et mitigation des attaques potentielles lors des transferts (e.g., attaques DDoS). >> Ces coûts peuvent être importants en fonction des exigences spécifiques des clients (secteurs sensibles, données réglementées). >> Impact : Directement lié à la fiabilité du service et à la confiance des clients, avec possiblement des implications financières et juridiques importantes en cas de défaillance. Coûts liés au support technique et aux outils <ul style="list-style-type: none"> Assistance technique et support client : >> Aide pour la configuration des transferts ou la résolution de problèmes lors des migrations. Fourniture d'outils de migration : >> Développement ou mise à disposition de logiciels et d'API pour faciliter les transferts. >> Maintenance et mise à jour de ces outils pour les rendre interopérables avec des systèmes tiers. Coûts d'orchestration et de gestion des transferts <ul style="list-style-type: none"> Coordination des opérations : >> Planification et supervision des transferts pour minimiser les interruptions et optimiser les flux. Ressources humaines dédiées : >> Personnel mobilisé pour la gestion des transferts complexes, surtout dans les cas de volumes élevés ou d'architectures spécifiques. >> Déplacements peuvent être prévus. > Monitoring et reporting : >> Suivi en temps réel des transferts pour garantir leur succès et produire des rapports d'audit, souvent demandés par les clients. >> Impact : La complexité croît avec la taille et la structure des données, ainsi qu'avec les exigences spécifiques des clients en matière de performance ou de disponibilité. Coûts liés à la conformité réglementaire <ul style="list-style-type: none"> Adaptation aux normes et certifications : >> Respect des réglementations spécifiques d'une industrie. >> Audit, certification et maintien des processus de transfert. Contrats spécifiques pour certaines juridictions : >> Mise en place d'accords spécifiques en fonction des lois locales ou sectorielles. > Impact : Un non-respect pourrait entraîner des sanctions ou une perte de clients, en plus de coûts directs pour la mise en conformité. Coûts liés à la continuité de service <ul style="list-style-type: none"> Réduction de la latence et optimisation des flux : >> Mise en œuvre de mécanismes pour garantir des performances minimales durant les transferts. Dispositifs de basculement (failover) : >> Mise en place de solutions pour assurer la continuité en cas d'interruption. |
| | 4 | | 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. | Comme évoqué dans la réponse suivante, cela dépend du modèle proposé par l'opérateur. |

| | | | | |
|--|----|----|--|--|
| Frais de transfert Infrastructures de transfert et coûts associés | 15 | 5 | <p>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 réseau du fournisseur, stratégie propre aux accords d'interconnexion, etc.) a-t-elle une influence sur ses coûts de transfert de données ? Le cas échéant, pouvez-vous détailler votre réponse, en particulier les postes de coûts qui peuvent être concernés.</p> | <p>Dans une certaine mesure. Ainsi, même si tous ces coûts sont supportés par les fournisseurs, l'internalisation de certains services permet au dit fournisseur de limiter les frais supplémentaires liés à l'utilisation d'intermédiaires. Plus précisément :</p> <ol style="list-style-type: none"> 1. Degré d'internalisation des éléments de réseau Impacts sur les coûts : <ul style="list-style-type: none"> > Infrastructure propre (fibre noire, routeurs, centres de données) : >> Avantages : Réduction des coûts variables liés à la location de capacités réseau (ex : transit IP). >> Inconvénients : Coût initial élevé pour le déploiement et la maintenance de l'infrastructure, amorti sur le long terme. >> Influence : Les fournisseurs avec une forte internalisation réduisent leurs coûts opérationnels par Go transféré sur le long terme. > Réseaux loués (capacité partagée sur des infrastructures tierces) : >> Avantages : Flexibilité accrue pour ajuster la capacité en fonction de la demande. >> Inconvénients : Dépendance aux tarifs de tiers et limitation de la maîtrise des performances réseau. >> Influence : Les coûts peuvent augmenter si le trafic est élevé et/ou nécessite une disponibilité géographique étendue. > Postes de coûts concernés : >> Investissement initial (CAPEX) pour la construction d'infrastructures réseaux. >> Coûts récurrents (OPEX) pour la location de réseaux ou la maintenance des équipements. 2. Stratégie propre aux accords d'interconnexion Impacts sur les coûts : <ul style="list-style-type: none"> > Peering (gratuit ou payant) : >> Le peering gratuit entre réseaux partenaires peut réduire ou éliminer les coûts d'interconnexion, mais dépend de négociations bilatérales. >> Le peering payant (pouvant être moins coûteux que le transit IP) représente une charge supplémentaire. > Transit IP : >> Les fournisseurs utilisant le transit IP pour les interconnexions payent un tarif par unité de bande passante transférée, influençant directement les coûts de transfert. >> Une stratégie reposant fortement sur le transit IP peut rendre les coûts variables plus élevés. > Points de présence stratégiques (PoPs) : >> Une infrastructure de peering bien positionnée réduit les distances et les coûts liés au transit des données. > Postes de coûts concernés : >> Frais de transit ou de peering. >> Développement ou maintenance des PoPs. 3. Positionnement géographique et couverture réseau Impacts sur les coûts : <ul style="list-style-type: none"> > Les fournisseurs opérant dans plusieurs régions peuvent rationaliser les coûts en utilisant des PoPs stratégiques et des routes directes. > Les transferts intercontinentaux peuvent nécessiter des interconnexions plus coûteuses et des capacités accrues. Postes de coûts concernés : > Déploiement de fibre et d'équipements dans des régions spécifiques. > Coûts liés à l'interconnexion dans les hubs internationaux 4. Optimisation des investissements à long terme Impacts sur les coûts : <ul style="list-style-type: none"> > Économies d'échelle : Un fournisseur ayant des volumes de données élevés peut réduire ses coûts unitaires grâce à des accords négociés ou en internalisant davantage son réseau. > Flexibilité financière : Les fournisseurs ayant investi massivement dans leurs infrastructures propres peuvent mieux contrôler leurs coûts dans des environnements concurrentiels. Postes de coûts concernés : > Frais d'amortissement d'infrastructures propriétaires. > Coût d'ajustement pour gérer les pics de demande. 5. Stratégies spécifiques pour des cas d'usage particuliers Impacts sur les coûts : <ul style="list-style-type: none"> > Clients nécessitant des garanties spécifiques (latence, sécurité) : exigences peuvent nécessiter des investissements supplémentaires en infrastructures dédiées (ex : lien direct client vers centre de données du fournisseur). > Accords spécifiques pour réseaux privés ou gouvernementaux (e.g., RIE en France) : configurations imposent des frais spécifiques non généralisables à l'ensemble du trafic. Postes de coûts concernés : > Coûts de configuration et de gestion d'infrastructures dédiées. > Tarifs spécifiques négociés avec des partenaires. |
| | | 6 | <p>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 ?</p> | <p>Nous sommes d'accord avec l'idée que la capacité d'utilisation de bande passante est un déterminant majeur des coûts, car elle constitue la base sur laquelle les infrastructures sont construites et dimensionnées. Cela injustifie d'autant plus la facturation en fonction du volume de données transférées car les coûts imputés aux fournisseurs ne varient pas en fonction du volume mais en fonction de la capacité d'utilisation de la bande passante. La capacité d'utilisation garantie de la bande passante pourrait être comparé à la taille d'un tuyau et non pas au débit réel. Les hyperscalers tendent à limiter la taille du tuyau sans jouer sur le débit de celui-ci.</p> <p>Toutefois, il est important de reconnaître que cette approche ne capture pas l'ensemble des facteurs contextuels et des coûts marginaux associés à des cas spécifiques. Une tarification équitable devrait tenir compte à la fois des coûts fixes liés à la capacité et des coûts supplémentaires engendrés par des contraintes particulières, comme la localisation, la sécurité, ou la conformité.</p> <p>Coûts spécifiques pour des cas particuliers :</p> <ul style="list-style-type: none"> > Certains transferts nécessitent des infrastructures ou des garanties spécifiques (e.g., bande passante réservée pour des applications critiques, sécurisation avancée). <p>> Dans ces cas, la bande passante peut ne pas être partagée ou optimisée, entraînant des coûts proportionnellement plus élevés.</p> <p>Transferts ponctuels et imprévus :</p> <p>> Un transfert massif ou non planifié peut temporairement saturer une partie du réseau, nécessitant une allocation dynamique de ressources ou des investissements imprévus.</p> <p>Interconnexion avec des tiers :</p> <ul style="list-style-type: none"> > Les coûts d'interconnexion à des réseaux spécifiques sont à considérer. Ces coûts ne sont pas strictement liés à la capacité globale du réseau. <p>Conformité et sécurité :</p> <p>> Dans des secteurs réglementés ou sensibles, les exigences de conformité (ex : chiffrement spécifique) peuvent représenter des coûts additionnels non directement liés à la capacité de bande passante.</p> |
| | | 16 | <p>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 ?</p> | <p>Il s'agit effectivement de la raison expliquant que les fournisseurs prévoient et dimensionnent en conséquence leur infrastructure pour supporter ce type d'évènement sur le réseau.</p> <p>Mais il faut rappeler que la contrainte des pics peut être gérée par des stratégies d'optimisation, comme la planification des transferts, l'utilisation de technologies avancées, et la priorisation des services selon les contrats des clients :</p> <ul style="list-style-type: none"> > Flexibilité offerte par la programmation des transferts : Certains types de transferts (e.g., migrations de données planifiées) peuvent être répartis dans le temps pour éviter les périodes de pointe, réduisant ainsi l'impact des pics sur le dimensionnement. > Différences entre pics locaux et globaux : Les pics de demande ne sont pas uniformes dans le réseau. Une zone géographique ou un PoP peut connaître un pic, tandis que d'autres restent sous-utilisés. Les fournisseurs peuvent donc optimiser localement sans nécessairement surdimensionner l'ensemble du réseau. > Impact des modèles d'abonnement des clients : Les clients disposant de SLA garantissant des niveaux de performance élevés forcent les fournisseurs à prévoir de la capacité pour ces besoins spécifiques. Les clients ayant des exigences plus flexibles ont moins d'impact sur le dimensionnement. > Effets des optimisations technologiques : Les innovations, comme la virtualisation des réseaux (SDN) et l'intelligence artificielle (IA) pour la gestion des flux, permettent de mieux répartir la charge sans augmenter indéfiniment la capacité. |

| | | | |
|--|----|--|--|
| | 8 | 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 ? | L'analyse de l'ARCEP est juste, le fournisseur initial ne peut identifier que le point de départ. Sa capacité à identifier la finalité et la route exacte d'un transfert de données est limitée. |
| Frais de transfert Dans le cas d'un changement de fournisseur | 9 | 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. | Il est effectivement fréquent que la migration de données soit lissée sur plusieurs mois. Un transfert de données lié à un changement de fournisseur est généralement non récurrent, avec une flexibilité d'exécution. Cependant, il existe des nuances et des exceptions qui pourraient limiter cette analyse dans certains contextes : 1. Taille exceptionnelle des données : Pour certains clients (e.g., plateformes de streaming, banques), le volume des données à migrer peut être exceptionnellement élevé, nécessitant des transferts intensifs sur une période prolongée. Ces transferts massifs peuvent avoir un impact localisé sur certaines parties du réseau, surtout si les ressources disponibles sont déjà sous pression. 2. Contraintes liées à la latence ou à la sécurité : Certains transferts critiques nécessitent une bande passante dédiée pour respecter des exigences de latence ou de sécurité spécifiques (e.g., cryptage en temps réel). Cela peut limiter la possibilité de lisser les transferts et augmenter temporairement la charge réseau. 3. Transferts sur des routes spécifiques : Si la migration implique des interconnexions spécifiques où la capacité réseau est limitée, cela pourrait nécessiter des ajustements ou des allocations spécifiques/supplémentaires. |
| | 10 | 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. | Analyse partagée. Néanmoins, cela est le cas lorsque des prestations complémentaires sont réalisés à l'initiative du client, hors du cadre initial du contrat souscrit. Mais il existe des exceptions importantes où des coûts spécifiques peuvent survenir : 1. Volume exceptionnel de données : Lorsque le transfert concerne des volumes massifs et inhabituels, comme pour des plateformes de streaming ou des services financiers, cela peut créer une charge imprévue sur certaines parties du réseau, nécessitant des ajustements temporaires ou permanents. 2. Contraintes spécifiques au client : Certains clients imposent des exigences particulières (e.g., haute disponibilité, faible latence, sécurité avancée) qui peuvent nécessiter : o La mise en œuvre de solutions spécifiques, comme des circuits sécurisés ou des liens à haut débit. 3. Dépendance aux réseaux tiers : Si une part importante du transfert passe par des réseaux tiers (transit IP, peering), les coûts liés à l'utilisation de ces infrastructures peuvent augmenter. Cela ne nécessite pas de déployer des équipements au sein du réseau propriétaire, mais peut engendrer des coûts spécifiques facturés par les opérateurs tiers. 4. Scénarios multi-client ou multi-transferts : Si plusieurs clients effectuent des migrations importantes simultanément, la charge combinée pourrait exiger des ajustements temporaires, voire des investissements ponctuels. |
| | 11 | 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. | L'analyse est globalement partagée, les frais de transfert sont très souvent artificiels. Bien que liés au fonctionnement habituel d'un provider de cloud, ils sont décorrélés des coûts du changement de fournisseur en lui-même (capacité réseau préexistante, frais fixes dominants liés au transfert de données, comme les investissements dans la fibre optique, les équipements réseau, ou les contrats de transit IP, et absence de nécessité de redimensionnement). Ils sont avant tout facturés pour dissuader le changement de fournisseurs. |
| | 12 | 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 ? | Certaines situations spécifiques peuvent justifier la facturation d'un transfert de données dans le cadre d'un changement de fournisseur, notamment lorsque le transfert génère des coûts additionnels significatifs et directement liés aux besoins particuliers des clients : 1. Volumes de données exceptionnellement élevés : Les entreprises ou institutions manipulant des volumes massifs de données (ex : plateformes de streaming, services financiers, administrations) peuvent nécessiter une bande passante importante et des ressources dédiées pour effectuer leur transfert. > Postes de coûts spécifiques : >> Bande passante dédiée : Coûts liés à l'allocation temporaire ou à la location de capacité supplémentaire. >> Renforcement régional : Si une région ou un point d'interconnexion spécifique devient un goulot d'étranglement. >> Infrastructure temporaire : Déploiement temporaire pour gérer le trafic additionnel. 2. Exigences spécifiques en matière de sécurité : Certains clients, comme les banques, les entreprises manipulant des données hautement sensibles, peuvent demander des garanties de sécurité élevées (ex : chiffrement en transit, prévention d'intrusion). > Postes de coûts spécifiques : >> Chiffrement avancé : Coûts liés aux protocoles de chiffrement et à la gestion des clés. >> Surveillance réseau en temps réel : Détection et prévention des attaques potentielles pendant le transfert. >> Tests de conformité et audit : Validation des mesures de sécurité avant et après le transfert. 3. Urgence ou délais contraints : Les clients demandant des délais très courts pour leur transfert (comme en cas de cessation rapide d'un contrat ou de migration d'urgence) peuvent nécessiter une priorisation et une allocation de ressources exceptionnelles. > Postes de coûts spécifiques : >> Mobilisation accélérée : Coûts associés à l'allocation rapide de ressources réseau et humaines. >> Perturbation d'autres opérations : Si le transfert affecte la gestion normale du réseau. 4. Besoins spécifiques d'assistance technique : Les clients sans expertise technique interne ou ayant des configurations complexes peuvent demander un accompagnement personnalisé. > Postes de coûts spécifiques : >> Support technique dédié : Assistance pour configurer et superviser le transfert. >> Développement d'outils sur mesure : Création de connecteurs ou scripts spécifiques pour faciliter la migration. >> Validation et tests : Vérification des données transférées pour garantir leur intégrité et leur conformité. |
| | 13 | 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 ? | Un plafond des frais de transfert fixé à zéro peut renforcer la concurrence. Pour assurer l'efficacité de ce dispositif, il serait pertinent de : > Assurer une transparence totale sur les conditions d'application de la gratuité. > Favoriser des mécanismes d'incitation à une utilisation efficace et planifiée des transferts. En effet, il existe plusieurs menaces ou risques que le dispositif soit contourné via : > L'incitation à des usages inefficients comme les transferts inutiles (ou mal planifiés), ou consommation accrue de bande passante (sans considération pour l'impact environnemental ou les ressources réseau). > Le report des coûts sur d'autres services : Les fournisseurs pourraient compenser l'absence de frais de transfert en augmentant les prix d'autres services, comme le stockage. |
| | 14 | 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 selon laquelle les transferts de données induits par un usage multi-cloud présentent des caractéristiques récurrentes, des volumes variables difficiles à anticiper, et une flexibilité moindre pour leur réalisation par rapport aux transferts ponctuels liés à un changement de fournisseur. |

| | | | |
|--|----|---|---|
| Frais de transfert Dans le cas d'un usage multi-cloud | 15 | 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 ? | <p>Pour permettre les transferts de données dans un usage multi-cloud, aucun équipement spécifique n'est généralement déployé par le fournisseur cloud. Les coûts ne relèvent donc pas des frais de transfert mais de l'architecture multi-cloud mise en place par le client, incluant :</p> <ul style="list-style-type: none"> > Liaisons physiques : Connexions inter-cloud (e.g., interconnexions directes entre fournisseurs via des réseaux privés ou publics). > Infrastructure du client : Équipements réseau (e.g., routeurs, pare-feu) et solutions logicielles pour gérer les flux entre clouds. > Ces coûts sont inhérents à l'architecture multi-cloud et non à des frais directs de transfert de données. |
| | 16 | 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 ? | <p>Comme indiqué précédemment, les postes de coûts affectés par un usage multi-cloud relèvent principalement de la mise en place d'une infrastructure spécifique (e.g., interconnexions réseau, équipements de gestion), qui constitue un préalable au multi-cloud. Ces coûts sont structurels et liés à l'architecture.</p> <p>Allocation des coûts :</p> <p>Aucun coût supplémentaire ne doit être imputé directement au multi-cloud, hormis ceux liés à l'architecture initiale.</p> <p>Indicateurs pertinents :</p> <p>Investissements dans les interconnexions réseau.</p> <p>Coûts de maintenance et gestion des équipements nécessaires au fonctionnement multi-cloud.</p> <p>Le multi-cloud ne devrait pas engendrer de facturation supplémentaire en dehors des coûts d'architecture.</p> |
| | 19 | | <p>Certains types de clients présentent des besoins particuliers qui peuvent entraîner des coûts spécifiques ou supplémentaires pour les transferts multi-cloud :</p> <ul style="list-style-type: none"> > Bande passante et infrastructure réseau renforcées pour gérer des volumes massifs ou des exigences de latence. > Sécurisation des transferts, avec chiffrement et surveillance renforcés. > Support technique avancé pour les cas complexes, comme les migrations fréquentes ou les architectures multi-cloud distribuées. <p>Concrètement :</p> <p>1. Clients manipulant des volumes massifs de données (plateformes de streaming, services cloud de stockage massif, entreprises de traitement d'images/vidéos)</p> <ul style="list-style-type: none"> > Besoins spécifiques : <ul style="list-style-type: none"> >> Transfert de données volumineux, souvent en continu. >> Exigences élevées de bande passante pour éviter les ralentissements. > Coûts spécifiques : <ul style="list-style-type: none"> >> Bande passante dédiée : Augmentation des capacités réseau pour gérer les transferts. >> Infrastructure renforcée : Mise à niveau des routeurs, commutateurs, et PoPs pour gérer le volume élevé. >> Transit IP : Frais supplémentaires si le trafic passe par des réseaux tiers. <p>2. Clients ayant des exigences critiques en matière de latence (entreprises de jeux vidéo en ligne, trading haute fréquence, applications en temps réel -IoT, télémédecine-).</p> <ul style="list-style-type: none"> > Besoins spécifiques : <ul style="list-style-type: none"> >> Transferts rapides et fiables avec une latence minimale. >> Routes optimisées pour garantir la performance. > Coûts spécifiques : <ul style="list-style-type: none"> >> Optimisation des routes : Utilisation de réseaux définis par logiciel (SDN) ou de circuits dédiés. >> Proximité des PoPs : Déploiement de points de présence régionaux pour réduire la latence. >> Surveillance en temps réel : Monitoring avancé pour détecter et résoudre rapidement les congestions. <p>3. Clients soumis à des réglementations strictes (secteurs bancaire, santé, administration publique).</p> <ul style="list-style-type: none"> > Besoins spécifiques : <ul style="list-style-type: none"> >> Conformité aux réglementations du secteur >> Transferts sécurisés garantissant la confidentialité et l'intégrité des données. > Coûts spécifiques : <ul style="list-style-type: none"> >> Chiffrement des données : Mise en œuvre de protocoles avancés >> Audits de conformité : Validation régulière des processus de transfert. >> Stockage temporaire sécurisé : Tampons pour garantir que les données sensibles restent protégées pendant les transferts. <p>4. Clients utilisant des applications hautement distribuées (architectures multi-cloud avec déploiements globaux, et les entreprises utilisant des services spécifiques dans plusieurs clouds).</p> <ul style="list-style-type: none"> > Besoins spécifiques : <ul style="list-style-type: none"> >> Transferts réguliers entre plusieurs fournisseurs, souvent dans des régions géographiquement éloignées. > Coûts spécifiques : <ul style="list-style-type: none"> >> Interconnexions multi-cloud : Renforcement des accords de peering et du transit entre clouds. >> Maintenance réseau : Ajustements fréquents pour garantir la compatibilité et la performance. <p>5. Clients demandant des garanties de sécurité accrues (Défense, renseignement, grandes entreprises critiques).</p> <ul style="list-style-type: none"> > Besoins spécifiques : <ul style="list-style-type: none"> >> Protection renforcée contre les cyberattaques pendant les transferts. >> Mesures avancées de prévention d'intrusion et de surveillance. > Coûts spécifiques : <ul style="list-style-type: none"> >> Pare-feu et IDS/IPS : Déploiement de systèmes de sécurité pour chaque transfert. >> Équipe dédiée : Supervision par des experts en cybersécurité. >> Circuits privés : Isolation physique ou logique pour certains transferts sensibles. <p>6. Clients à forte variabilité de trafic (E-commerce avec pics saisonniers, événements en ligne).</p> <ul style="list-style-type: none"> > Besoins spécifiques : <ul style="list-style-type: none"> >> Gestion de transferts massifs lors de pics imprévus. >> Besoin d'une capacité réseau flexible et évolutive. > Coûts spécifiques : <ul style="list-style-type: none"> >> Allocation temporaire de ressources : Location de capacité réseau pour gérer les pics. >> « Surdimensionnement » : Coûts d'investissement pour anticiper les fluctuations. <p>Les coûts varient en fonction du projet mais ils sont humains, techniques (fournisseur de destination), liés au transfert (fournisseur initial). Plus la migration est complexe, plus les coûts seront élevés : typologie d'application, complexité des serveurs, fonctionnalités spécifiques, taille de l'application, etc.</p> |
| | 17 | 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 ? | |

| | | | | |
|---|----|----|---|---|
| Frais de transfert Frais et prestations liés ou non au changement de fournisseur | 18 | | 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 ? | <p>Nous partageons globalement l'analyse de l'Autorité selon laquelle les prestations liées au processus de changement de fournisseur, hors transfert de données, relèvent principalement de la mise à disposition de main d'œuvre pour des actions spécifiques (e.g., migration, extraction, transformation des données).</p> <p>Toutefois, ce constat doit être précisé dans le cadre du SaaS : pour ceux-ci les prestations la mise à disposition de main d'œuvre pour des actions spécifiques devrait relever des "autres prestations supplémentaires d'accompagnement à la migration" décrites par ailleurs. En effet, si les prestations "qui rentrent dans le périmètre de ses obligations de facilitation du changement de fournisseur" (voir ci-après) sont correctement accomplies par le fournisseur SaaS, le client ne doit pas avoir, sauf cas spécifiques, besoin d'assistance supplémentaire. En outre, il faudrait plutôt faire référence aux obligations contractuelles des fournisseurs plutôt qu'à leurs obligations respectives.</p> <p>Parmi les obligations de facilitations, Hexatrust identifie :</p> <ol style="list-style-type: none"> 1. Utilisation de standards ouverts : Réduction des coûts par alignement avec des normes de l'industrie. 2. Automatisation via API : Limitation de l'intervention humaine et évaluation des coûts techniques associés. 3. Documentation publique : Transparence sur les étapes et outils disponibles pour minimiser les besoins en assistance. |
| | 19 | | 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 tétéversement des données ? Le cas échéant, quels seraient les coûts supportés par le fournisseur d'origine associés à ces prestations ? | <p>Nous n'identifions pas d'autres prestations que devrait réaliser le fournisseur d'origine dans le cadre du processus de changement de fournisseur, au-delà de celles déjà mentionnées en réponse à la question 18. Il est important de noter que ce sont les éléments contractuels qui définissent finalement les prestations incluses et non incluses dans l'abonnement.</p> <p>Il nous semble important de préciser que les différents types de services Cloud englobent des réalités technologiques très différentes.</p> <p>Sur le SaaS, il est important de contribuer à une bonne compréhension par le marché de ces différences, de responsabiliser clients et fournisseurs, sur ce qui est de la compétence du fournisseur d'origine (assurer la portabilité et extraire les données) et ce qui est de la compétence du fournisseur de sortie (adapter ces données au nouveaux services)</p> |
| | 20 | 22 | Avez-vous d'autres remarques concernant les frais de changement de fournisseur autres que ceux liés aux transferts de données ? | <p>Nous souhaitons partager des remarques à l'Autorité concernant les frais de changement de fournisseur autres que ceux liés aux transferts de données. Si ces frais sont légitimes, ils ne doivent pas être des frais de transfert de données déguisés si ces derniers venaient à être interdits. Il est essentiel de responsabiliser les clients en assurant une transparence complète sur les pertes de données potentielles lors du changement de prestataire et sur les données récupérables d'un prestataire à l'autre. Les prestations de service doivent être autorisées, mais elles doivent être transparentes en ce qui concerne les coûts.</p> <p>1. Frais pour services IaaS/PaaS : un fournisseur IaaS/PaaS ne devrait pas facturer de frais pour les transferts de données dans le cadre d'un changement de fournisseur, sauf en cas de migration complexe nécessitant un service d'accompagnement spécifique.</p> <p>Points à souligner :</p> <ul style="list-style-type: none"> > Alignement avec le Data Act : Cette approche est en phase avec l'esprit de l'article 30, paragraphe 6, du Data Act, qui cherche à minimiser les barrières au changement de fournisseur. > Facturation justifiée pour des prestations supplémentaires : >> Si le client demande un accompagnement spécifique ou des développements sur mesure, une facturation proportionnée aux efforts requis semble raisonnable. >> Les coûts spécifiques pourraient inclure : <ul style="list-style-type: none"> - Analyse des besoins clients. - Configuration d'environnements temporaires pour la transition. - Développement d'automatisations pour faciliter la migration. <p>Notre recommandation :</p> <p>Il serait utile de définir des seuils clairs pour distinguer une migration standard (gratuite) d'une migration complexe (facturable), avec des critères basés sur :</p> <ul style="list-style-type: none"> >> Le volume des données. >> La complexité des architectures à migrer. >> Les ressources supplémentaires demandées par le client. <p>2. Frais pour services SaaS : la consultation ne reflète pas pleinement la complexité des migrations industrielles dans des secteurs comme l'automobile ou l'aéronautique, où les défis principaux résident dans l'ingénierie métier et l'interopérabilité entre systèmes.</p> <p>Points à souligner :</p> <ul style="list-style-type: none"> > Nature des défis pour les SaaS complexes : >> Les migrations dans ces secteurs impliquent souvent une phase prolongée de coexistence des systèmes et une intégration progressive avec des processus métiers spécifiques. >> Ces projets nécessitent des solutions sur mesure, des développements spécifiques et une coordination étroite avec les équipes clients. > Coûts majeurs identifiés : <ul style="list-style-type: none"> >> Ingénierie métier : Analyse approfondie des besoins industriels et développement de solutions personnalisées. >> Interopérabilité : Développement et déploiement de connecteurs ou interfaces API spécifiques pour garantir la coexistence des systèmes. >> Phase de transition étendue : Maintien des systèmes en double pendant une période prolongée, augmentant les coûts opérationnels. > Divergence avec l'article 30 du Data Act : >> Bien que cet article n'impose pas aux fournisseurs de développer de nouvelles technologies ou services, la réalité industrielle dans les secteurs complexes rend ces adaptations indispensables pour réussir une migration. <p>Notre recommandation :</p> <ul style="list-style-type: none"> > L'ARCEP pourrait prendre en compte les spécificités des projets SaaS dans des environnements industriels complexes en : >> Permettant une facturation des services d'ingénierie métier et de développement sur mesure, sous réserve de transparence sur les coûts. >> Encourageant les fournisseurs à documenter les coûts de ces prestations pour les différencier clairement des frais liés à l'infrastructure. <p>Enfin, nous tenons à souligner que les prestations des Entreprises de Services Numériques (ESN), qui incluent parfois l'accompagnement à la migration d'un utilisateur vers les services d'un autre fournisseur, peuvent être perçues comme des manières détournées d'intégrer des frais de changement de fournisseurs.</p> |
| | 21 | 24 | 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 ? | <p>La définition d'un service cloud selon la loi SREN met en lumière plusieurs caractéristiques fondamentales des services cloud et s'aligne avec celles généralement acceptées, comme celles de l'ISO ou du NIST, tout en soulignant des aspects spécifiques à la modularité, la distribution, et l'interaction réduite avec le fournisseur.</p> <p>Cela mériterait quelques Nuances importantes à relever dans la définition :</p> <ol style="list-style-type: none"> a. Nature des ressources <ul style="list-style-type: none"> > Des modèles émergents : <ul style="list-style-type: none"> >> Bare Metal : Services qui fournissent un accès direct à des serveurs physiques, souvent dans des environnements spécifiques nécessitant des performances maximales ou des configurations sur mesure. >> Accélérateur matériels spécialisés : Services fournissant un accès à des unités de calcul spécifiques comme les GPU ou les FPGA. > Des modèles d'architecture cloud centralisée, distribuée ou fortement distribuée : >> Cette distinction est essentielle pour différencier les modèles d'architecture cloud : <ul style="list-style-type: none"> - Centralisée : avec des data centers regroupés (ex : AWS, OUTSCALE, OVHcloud...). - Distribuée : Une extension pour minimiser la latence ou respecter des contraintes de localisation des données (e.g., Google Cloud régionales). - Fortement distribuée : Modèle émergent comme l'edge computing, où les ressources sont proches, voire localisées, de l'utilisateur final (ex : AWS Outposts , OUTSCALE Dedicated Cloud). <ol style="list-style-type: none"> b. Mobilisation et libération rapides <ul style="list-style-type: none"> > Cela met en avant : <ul style="list-style-type: none"> >> L'élasticité du cloud : Capacité à ajuster les ressources automatiquement ou sur demande pour répondre à des variations de charge. >> La simplicité d'utilisation : Réduction de la complexité pour l'utilisateur grâce à des interfaces de self-service (portails ou APIs). c. Interaction minimale avec le fournisseur > La réduction des efforts de gestion reflète la philosophie as-a-Service. Elle limite la dépendance opérationnelle des utilisateurs envers le fournisseur. <p>Enfin, une explication des responsabilités des acteurs de la chaîne de valeur participerait à une meilleure distinction des parties prenantes :</p> <ul style="list-style-type: none"> > Client : Responsable de la gestion des ressources consommées (configuration des machines virtuelles, gestion des données...). > Partenaires tiers (le cas échéant) : Intègrent ou personnalisent les services Cloud pour des cas d'usage spécifiques. |

| | | | | |
|--|----|----|--|---|
| Interopérabilité Spécificités et standardisation des services cloud | 22 | | <p>Que pensez-vous de ces typologies et définitions relatives aux autres services cloud mentionnés à l'article 29, I de la loi SREN ?</p> | <p>Nous souhaitons apporter quelques remarques sur les typologies et définitions des services cloud mentionnés à l'article 29, I de la loi SREN, notamment concernant le PaaS.</p> <p>La nature du PaaS est une plateforme fournissant les outils et frameworks nécessaires au développement, déploiement, et gestion des applications. Cette couche est centrée sur l'environnement d'exploitation, et non directement sur les données des clients.</p> <p>La définition pourrait clarifier que le PaaS est destiné aux développeurs ou intégrateurs et inclut des services comme :</p> <ul style="list-style-type: none"> > Hébergement d'applications > Intégration continue (CI/CD) > Outils de test, surveillance, et analyse... <p>Nous considérons le SaaS comme des services élémentaires managés (e.g., bases de données managées, services de messagerie) devraient être classés comme des SaaS lorsqu'ils sont directement consommés par l'utilisateur final. Lorsqu'un service est prêt à l'emploi pour l'utilisateur final, il est logique de le considérer comme un SaaS, même si, techniquement, il repose sur des principes d'infrastructure ou de plateforme.</p> <p>Exemples typiques :</p> <ul style="list-style-type: none"> > Une base de données managée accessible directement par une API pourrait être considérée comme un PaaS pour les développeurs qui l'utilisent pour construire des applications. > En revanche, si cette base de données est présentée comme une application prête à l'emploi pour des utilisateurs finaux (e.g., une solution CRM), elle relèverait plutôt du SaaS. <p>Nous recommandons d'introduire des critères dans la définition pour distinguer les services PaaS (orientés développeurs) des SaaS (orientés utilisateurs finaux), tels que :</p> <ul style="list-style-type: none"> > Le niveau d'abstraction fourni > Le public cible (développeurs vs utilisateurs métiers) > L'accès aux fonctionnalités avancées (exploitation directe vs utilisation prédéfinie) <p>Une meilleure différenciation entre ces typologies permet de :</p> <ul style="list-style-type: none"> > Clarifier les responsabilités des fournisseurs : Par exemple, un fournisseur PaaS doit garantir la disponibilité des outils et environnements, mais pas nécessairement le contenu. > Éviter des malentendus dans la portabilité des services : Les défis liés au transfert de services PaaS (comme les frameworks) diffèrent de ceux d'un SaaS (où les données et configurations sont plus critiques). |
| | 23 | 25 | <p>Partagez-vous la compréhension de l'Arcep quant à la distinction entre services « standards » et « spécifiques » ?</p> | <p>Ni la loi SREN ni le Data Act ne clarifient ou n'exploitent explicitement la distinction entre services « standards » et « spécifiques », compliquant son interprétation et son application, notamment pour définir les responsabilités des fournisseurs ainsi que les obligations de portabilité et d'interopérabilité.</p> <p>Cette distinction manque de fondement légal et pratique clair, et son applicabilité est limitée, même pour les services IaaS, et encore davantage pour les SaaS. Si elle doit être maintenue, elle nécessiterait des critères objectifs tels que l'interopérabilité, la standardisation ou la complexité.</p> <p>Bien que les services IaaS soient souvent perçus comme des « blocs de construction » relativement génériques (machines virtuelles, stockage objet, etc.), les orientations technologiques varient largement entre fournisseurs (ex : Une machine virtuelle sur AWS (EC2) peut inclure des configurations spécifiques à l'environnement AWS (e.g., Elastic Load Balancer, autoscaling), qui diffèrent fondamentalement de celles offertes par OUTSCALE ou OVHcloud). Cette diversité technologique rend difficile l'identification de ce qui constitue un service « standard », même dans le cas des IaaS, qui sont pourtant les plus proches d'un dénominateur commun.</p> <p>Les services SaaS sont intrinsèquement conçus pour répondre à des besoins métier spécifiques. Ils diffèrent souvent par leurs fonctionnalités, interfaces, intégrations, et configurations (exemple : Un logiciel de gestion de la relation client (CRM) comme Salesforce est hautement configurable en fonction des besoins de l'utilisateur final. Il est donc difficile de définir un « standard » qui s'appliquerait à tous les services CRM SaaS). Cette variabilité accentue l'ambiguïté de la distinction pour les SaaS.</p> <p>Les risques d'une catégorisation arbitraire des services en « standards » et « spécifiques » pourrait engendrer :</p> <ul style="list-style-type: none"> • Des litiges entre fournisseurs et utilisateurs sur la nature des services. • Une incertitude quant aux obligations de portabilité ou d'interopérabilité, particulièrement pour les services classés comme « spécifiques ». • Une inhibition de l'innovation car les fournisseurs pourraient être réticents à développer des fonctionnalités différenciées ou avancées si elles risquent d'être exclues des catégories « standards » et soumises à des réglementations plus strictes. |
| | 24 | | <p>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 ?</p> | <p>Les outils cloud-agnostiques répondent aux besoins fondamentaux des architectures multi-cloud (portabilité, orchestration, gestion des coûts), mais ils ne suppriment pas les différences et fonctionnalités avancées propres aux fournisseurs de cloud. Les seuls outils ou services pouvant être véritablement considérés comme cloud-agnostiques sont ceux qui sont standard dans le marché levant de fait les barrières à l'interopérabilité ou la portabilité. Ces outils créent une abstraction, mais les utilisateurs doivent encore gérer :</p> <p>Besoins identifiés :</p> <ul style="list-style-type: none"> > Interopérabilité renforcée : Adoption de standards ouverts par les fournisseurs. > Support pour les fonctionnalités avancées : Intégration progressive des services propriétaires dans les outils agnostiques. > Formation et documentation : Sensibiliser les utilisateurs à exploiter au mieux l'hétérogénéité des offres. <p>Les outils cloud-agnostiques restent un levier, mais ne peuvent totalement éliminer les spécificités des fournisseurs, ce qui exige une responsabilité partagée entre utilisateurs et fournisseurs.</p> |

| | | | | |
|---|----|----|---|---|
| Interopérabilité é Portabilité des données et des applications | 25 | 26 | 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 ? | <p>Nous souhaitons donc apporter des observations concernant la définition et le périmètre des actifs numériques, ainsi que leur portabilité, notamment dans le contexte des obligations fixées par la loi SREN et le Data Act :</p> <p>1. Définition et périmètre des actifs numériques > Problèmes identifiés : 1. Flou autour de la notion d'actifs numériques : >> La définition de l'ARCEP, bien que précisée, reste ambiguë, notamment pour les notions d'« applications » ou de « technologies de virtualisation ».</p> <p>>> Le considérant 83 du Data Act ajoute à cette confusion en évoquant les actifs « dont le client a le droit d'utilisation », sans spécifier les types d'actifs ou leurs conditions de portabilité.</p> <p>2. Propriétés hybrides des actifs numériques : >> Certains actifs, tels que les applications ou configurations, peuvent mêler la propriété intellectuelle du fournisseur (e.g., frameworks ou outils fournis) et les contributions du client (e.g., code développé). >> Ces actifs posent des questions complexes en matière de propriété intellectuelle et de droits d'utilisation.</p> <p>3. Distinction entre données et applications : >> Une clarification est nécessaire pour différencier : - Les applications utilisées par le client (propriété du fournisseur, non transférables). - Les applications développées par le client à l'aide de l'infrastructure du fournisseur (exportables en tant que données).</p> <p>Propositions de clarification : 1. Applications : >> Différencier explicitement : - Applications du fournisseur : Logiciels ou outils fournis dans le cadre du service (non portables). - Applications développées par le client : Code, configurations ou frameworks déployés par le client (portables en tant que données).</p> <p>2. Technologies de virtualisation : >> Exclure clairement les outils et infrastructures sous-jacents utilisés pour offrir les services, car ils relèvent de la propriété intellectuelle du fournisseur.</p> <p>3. Actifs numériques exportables : >> Limiter la portabilité aux éléments créés ou configurés par le client, notamment : - Les configurations spécifiques (e.g., paramètres réseau, scripts d'automatisation).</p> <p>- Les environnements développés (e.g., conteneurs, code source).</p> <p>4. Encadrement des droits d'utilisation : >> Introduire des lignes directrices claires pour distinguer : - Les actifs numériques que le client a le droit d'utiliser dans un cadre donné (non transférables). - Les actifs numériques que le client a le droit d'exporter et de réutiliser (transférables).</p> <p>2. Portabilité des actifs numériques : limites et protection des fournisseurs Problèmes identifiés : 1. Risque de dilution des droits de propriété intellectuelle et des secrets d'affaires : >> La portabilité pourrait être interprétée comme une obligation de transférer des actifs protégés par la propriété intellectuelle ou des secrets d'affaires du fournisseur, ce qui est incompatible avec l'article 30(6) du Data Act.</p> <p>2. Manque de précision sur les actifs hybrides : >> Certains actifs numériques incluent des contributions du fournisseur et du client, rendant leur portabilité complexe.</p> <p>Propositions pour limiter la portabilité : 1. Exclusion explicite des actifs protégés : >> Exclure les actifs numériques relevant de la propriété intellectuelle du fournisseur ou contenant des secrets d'affaires.</p> <p>2. Clarification des actifs hybrides : >> Définir un cadre pour gérer les actifs co-développés ou configurés à partir de ressources du fournisseur, par exemple : - Conserver le droit d'utilisation chez le client sans permettre leur transfert. - Permettre la portabilité des configurations ou résultats finaux, mais pas des outils sous-jacents.</p> <p>3. Exclusion des obligations de développement : >> Réaffirmer que les fournisseurs ne sont pas tenus de développer de nouvelles technologies ou d'adapter leurs outils pour répondre aux demandes spécifiques de portabilité.</p> <p>3. Application aux services SaaS Problèmes spécifiques aux SaaS : 1. Hétérogénéité des modèles SaaS : >> Les SaaS intègrent souvent des fonctionnalités non standardisées ou spécifiques au fournisseur, ce qui complique leur portabilité.</p> <p>2. Liens étroits avec l'infrastructure : >> De nombreux SaaS utilisent des outils et frameworks intégrés, rendant leur extraction ou portabilité souvent irréaliste.</p> <p>Propositions pour les SaaS : 1. Limiter la portabilité : >> Se concentrer sur la portabilité des données clients générées ou manipulées par le SaaS, plutôt que sur les fonctionnalités ou l'infrastructure du service.</p> <p>2. Encourager l'interopérabilité : >> Prévoir des standards ouverts pour permettre aux clients de migrer leurs données ou configurations entre services SaaS similaires.</p> <p>4. Points supplémentaires à rappeler à l'ARCEP 1. Clarification urgente de la définition des actifs numériques : >> Une définition claire et précise est essentielle pour éviter des litiges entre fournisseurs et clients.</p> <p>2. Protection des droits des fournisseurs : >> Garantir que la mise en œuvre de la loi SREN respecte pleinement l'article 30(6) du Data Act pour protéger la propriété intellectuelle et les secrets d'affaires des fournisseurs.</p> <p>3. Distinction entre données et actifs numériques : >> Séparer les obligations liées aux données exportables (facilement identifiables) et celles liées aux actifs numériques (souvent complexes et hybrides).</p> <p>La liste des actifs numériques proposée par l'ARCEP nécessite des clarifications majeures, notamment sur les notions d'applications, de technologies de virtualisation, et d'actifs hybrides. La portabilité doit être limitée aux éléments créés ou configurés par le client et ne pas inclure les outils ou technologies relevant de la propriété intellectuelle du fournisseur.</p> <p>Pour les SaaS, il serait pertinent de concentrer les efforts sur la portabilité des données et sur l'interopérabilité, tout en excluant les obligations de transfert des fonctionnalités ou infrastructures sous-jacentes.</p> |
| | 26 | 27 | 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 ? | <p>La description d'un processus "standard" de migration pour les services IaaS est pertinente. Elle peut toutefois être enrichie pour refléter les complexités supplémentaires et les actifs numériques impliqués dans certaines configurations spécifiques.</p> <p>> Utilisation d'outils cloud-agnostiques : Adopter des solutions comme Terraform pour simplifier la gestion des infrastructures dans plusieurs clouds et utiliser des orchestrateurs comme Kubernetes pour maximiser la portabilité des applications.</p> <p>> Documentation complète : Maintenir une documentation des configurations, scripts, et dépendances pour garantir un transfert fluide.</p> <p>Il faudrait également y intégrer les problématiques de conversion des scripts qui rendent la migration difficile.</p> |

| | | | | |
|--|----|----|--|--|
| Interopérabilité é Portabilité des données - IaaS | 27 | 28 | 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 ? | <p>Nous partageons le constat de l'Autorité quant à l'absence de difficultés techniques significatives 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.</p> <p>Ces complexités peuvent découler de plusieurs facteurs :</p> <ul style="list-style-type: none"> > 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. <p>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.</p> <p>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.</p> |
| | 28 | | 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 ? | Nous partageons le constat de l'Autorité. Comme mentionné précédemment, 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. |
| Interopérabilité é Portabilité des données - PaaS | 29 | 29 | 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 ? | Cette description est fidèle mais elle ne couvre pas l'ensemble des opérations nécessaires. Une évaluation approfondie de l'application et de ses dépendances est indispensable. Il est également 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. |
| | 30 | | 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 ? | <p>Constat partagé. Nous attirons toutefois l'attention de l'Autorité sur deux points :</p> <ul style="list-style-type: none"> > La majorité des services cloud des hyperscalers sont propriétaires et non open source, ce qui limite l'interopérabilité et la portabilité, renforçant ainsi le verrouillage technique des utilisateurs lorsque ces services PaaS dominent un segment de marché. > Certains standards, tels que S3, sont contrôlés par des hyperscalers. <p>Nous recommandons que l'action publique favorise l'instauration de formats pivots standards (facilitant l'extraction et l'export des données dans un format ouvert) et une gouvernance collégiale des standards.</p> |
| | 31 | | 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 ? | L'interopérabilité et la portabilité dépendent de l'introduction de standards ouverts, permettant un format "pivot" garantissant ces propriétés. Il est essentiel de définir de tels standards pour les différents types de bases de données existantes. |
| Interopérabilité é Portabilité des données - services auxiliaires | 32 | | 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 ? | Pas de commentaire à date. |
| Interopérabilité é Portabilité des données - SaaS | 33 | 30 | 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 ? | <p>Il est important de préciser qu'il n'y a pas de migration de "logiciel SaaS", tel que proposé dans la question de l'ARCEP. Les données sont exportées mais le service/logiciel reste propriété du fournisseur qui travaille à la restitution des données apportées ou produites via la solution SaaS.</p> <p>De plus, la rédaction actuelle de la partie d) est ambiguë. Elle risquerait de pousser à la mise en place d'une fonctionnalité qui permettrait une extraction totale des données en permanence, ce qui entraînerait des coûts importants pour les fournisseurs, en raison du maintien en condition opérationnelle, sans que l'usage le justifie. La restitution intégrale des données ne doit être possible qu'en sortie et non en run. En outre, certains services sont optionnels.</p> <p>Enfin, il appartient au propriétaire de données et non au prestataire SaaS d'adapter les données vers le système cible.</p> |
| | 34 | | Identifiez-vous des difficultés pour la récupération des données liées à l'utilisation d'un service SaaS ? Si oui, dans quel contexte ? | <p>En raison des difficultés techniques à anticiper les évolutions technologiques, il est primordial de ne pas imposer une technologie de restitution dans les contrats.</p> <p>Ces difficultés s'expriment lors de la formalisation du contrat et à l'occasion de sa révision.</p> |
| | 35 | 31 | 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 ? | Rien à signaler. |
| | 36 | | Comment définissez-vous, dans le cadre des contrats liants un client à un fournisseur de services cloud, le périmètre des données exportables ? | Les données exportables sont composées de tout ou parties des documents électroniques et/ou données structurées ayant été déposées/uploadées par le client et/ou co-construites par le client dans le cadre du service SaaS. |
| | 37 | | Pouvez-vous décrire de manière concrète les difficultés que rencontrent les clients et les fournisseurs de services cloud lorsqu'ils doivent convenir du périmètre des données exportables liés à l'utilisation de services SaaS ? | L'export de données ne pose pas de difficulté. C'est après la migration que les difficultés ont tendance à survenir, beaucoup de clients ayant tendance à se tourner vers le fournisseur initial pour obtenir un accompagnement afin d'implémenter les données dans la nouvelle solution cloud. |
| Interopérabilité é Autres techniques | 38 | | Identifiez-vous d'autres difficultés techniques en cas de changement de fournisseur, que vous souhaitez porter à la connaissance de l'Arcep ? | Nous n'avons pas de remarque. Néanmoins, le schéma n°2 lié à cette question ne permet pas en l'état de comprendre les responsabilités respectives du fournisseur de sortie et du nouveau fournisseur sur les actions réalisées. |
| | 39 | | 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. |

| | | | | |
|---|----|----|--|---|
| Interopérabilité Architecture multi-cloud | 40 | 33 | Pour quels cas d'usage, présents ou futurs, une architecture « multi-cloud intégré » 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 ? | Le multi-cloud optimise la migration des workloads entre cloud en répondant aux besoins de coûts, en performance, en disponibilité, afin de tirer parti des services proposés par les différents fournisseurs. Cela renforce la résilience et la disponibilité. L'interopérabilité rencontre néanmoins plusieurs freins : incompatibilités technologiques entre fournisseurs, divergences en matière de sécurité ou de conformité. |
| Interopérabilité Interopérabilité et API | 41 | 34 | 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 ? | La vision est partagée uniquement dans le cadre du multi-cloud, entendu qu'il se limite au IaaS sans concerner le SaaS. Dans le cadre du SaaS, une telle interopérabilité sémantique conduirait d'une part à dévoiler des savoirs-faires relevant de la propriété industrielle et d'autre à limiter l'innovation des acteurs du marché. Sur le IaaS, il est nécessaire de mentionner qu'il s'agit de pré-requis pour rendre consommable et faire fonctionner les API. Nous attirons également l'attention de l'ARCEP sur la nécessité d'imposer une cohérence entre les API (i.e. : une cohérence entre les champs et attributs aux fonctions similaires, mais parfois nommés ou configurés différemment) |
| | 42 | | 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 ? | Comme pour la Q41, notre réponse ne vaut que dans un contexte IaaS. Une documentation complète des API est essentielle, incluant la description des champs, les formats attendus, les cas d'erreurs, les outputs et le type de retour (synchrone ou asynchrone). Il est également crucial de notifier à l'avance les changements majeurs (6-12 mois de préavis). L'utilisation de la norme SemVer garantit une clarté sur les nouvelles fonctionnalités, les corrections de bugs et les modifications rompant la compatibilité. |
| | 43 | | Identifiez-vous d'autres modèles d'interopérabilité entre systèmes informatiques que les API ? Le cas échéant, lesquels ? | Des alternatives existent mais sont souvent moins efficaces et pratiques dans leur mise en œuvre. Les API restent la norme de référence pour garantir une interopérabilité performante et flexible entre différents systèmes. |
| Interopérabilité Difficultés techniques du multi-cloud | 44 | | Identifiez d'autres enjeux et difficultés techniques relatifs au changement de fournisseur et au développement du multi-cloud ? | Pas de commentaire |
| Interopérabilité Normalisation ciblée | 45 | 35 | 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 commentaire |
| Interopérabilité Equivalence fonctionnelle | 46 | 36 | 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 ? | En lien avec la réponse à la Q28, la bonne équivalence fonctionnelle entre services IaaS s'explique surtout par le haut niveau de standardisation des services IaaS et des systèmes d'exploitation qui exécutent ces services (OS) et qui sont bien adoptés par les acteurs du Cloud. |
| Interopérabilité Information des utilisateurs | 47 | 37 | 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 devrait garantir une transparence optimale et fournir aux utilisateurs toutes les informations nécessaires à une utilisation efficace et informée des services. Elle doit tout d'abord indiquer si ces services sont des services spécifiques ou standards. L'offre devra détailler : les moyens d'extraire les données du service dans un format documenté et à un coût raisonnable, les attributs disponibles, les mécanismes de gestion des cas d'erreur, la description des outputs, la nature des retours, la gestion des évolutions ou de la fin de l'API. Cette documentation doit être cohérente dans sa syntaxe et son organisation. Il semble pertinent que cette documentation soit fournie dans un format standardisé. La spécification OpenAPI apparaît par exemple comme une solution adaptée. |
| | 48 | | 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 ? | Cette proposition est bonne et permettrait aux consommateurs de mieux appréhender et anticiper leurs choix. L'harmonisation garantira une transparence accrue et la comparaison des services sur une base établie. |
| Interopérabilité Harmonisation des services | 49 | 38 | 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 ? | L'analyse de l'ARCEP est partagée. Néanmoins, nous attirons sa vigilance sur les points d'attention mentionnés en réponse à la Q27. |
| | 50 | | 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 ? | Le constat est partagé. Comme mentionné dans la réponse à la Q30, l'interopérabilité et la portabilité ne peuvent être garanties qu'avec des standards ouverts, permettant un format « pivot » pour les données. Nous jugeons prioritaire de normaliser les services suivants : workflows, bases de données, stockage, conteneurs et orchestration, ainsi que le déploiement d'applications. Nous alertons l'Autorité sur les verrouillages techniques liés aux services PaaS, notamment dans le domaine de l'IA, où des solutions AutoML sont proposées sous des formats propriétaires et non transparents. |
| | 51 | | 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 ? | Il y a un constat d'un manque de solutions techniques et d'initiatives visant à standardiser les services auxiliaires, notamment dans le domaine des services IAM. Il serait nécessaire de normaliser les moteurs d'autorisation, au-delà de la gestion des accès, du fait des approches divergentes selon les fournisseurs. Chaque fournisseur devrait exporter sa politique IAM dans un format standardisé. Ce format pourrait ensuite être traduit automatiquement dans différents langages. |
| | 52 | | 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 ? | La standardisation des structures et de formats d'échanges de données, sous la forme d'ontologie ou de "standard d'échange" existe (par exemple : NF ISO 20614 Protocole d'échange de données pour l'interopérabilité et la préservation ou encore ISAD(G) : Norme générale et internationale de description archivistique). Ces travaux démontrent que cette standardisation n'est possible/pertinente que dans des verticales/secteurs d'activités bien définies. Ce type de travaux de standardisation devraient être strictement limités à la volonté des commissions de normalisation (Fr ou UE ou ISO) et être réalisés de manière verticale pour chaque secteur et sous-secteur concernés. |
| Avis sur la consultation | 53 | 39 | Avez-vous d'autres commentaires sur les enjeux soulevés dans cette consultation publique ? | Pas de commentaire |
| Enjeux cloud à porter à la connaissance de l'ARCEP | 54 | | 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 ? | Il est nécessaire d'alerter l'ARCEP sur les risques autour de l'IA - dont le cloud est un intrant essentiel - et qui pourraient venir renforcer certaines dynamiques et pratiques anticoncurrentielles au sein du marché du cloud, telles que le verrouillage technique et financier des utilisateurs, ou le renforcement des abus de position à partir de marchés adjacents (i.e. : ventes liées, auto-préférence). |