



Consultation publique de l'Arcep

29 octobre 2024 – 16 décembre 2024

Régulation des services d'informatiques en nuage
(*cloud*) : faciliter le changement de fournisseurs de
services *cloud* et la mise en œuvre d'architectures
multi-cloud grâce à
un nouvel encadrement tarifaire et technique

Réponse d'Orange

Version confidentielle

Contact : affaires.reglementaires@orange.com

Lien vers les documents en consultation :

[Régulation des services d'informatique en nuage \(*cloud*\) : Faciliter le changement de fournisseurs de services *cloud* et la mise en œuvre d'architectures multi-*cloud* grâce à un nouvel encadrement tarifaire et technique \(14 octobre 2024\) | Arcep](#)

Synthèse générale

Cette consultation publique s'inscrit dans le cadre de la mise en œuvre de la loi SREN, qui anticipe certaines dispositions du règlement européen sur les données (*Data Act*), et vise à définir les modalités d'encadrement des frais de transfert de données et de changement de fournisseur de services *cloud*, ainsi que les exigences techniques d'interopérabilité et de portabilité.

Ces nouvelles dispositions réglementaires répondent à un double objectif : faciliter le changement de fournisseur de services *cloud* et encourager le développement d'architectures multi-*cloud*. Elles s'inscrivent dans un contexte de marché caractérisé par une forte concentration autour de trois acteurs majeurs américains, qui représentent plus de 70% du marché européen.

Concernant le changement de fournisseur de services *cloud*, Orange met en évidence les limites d'une approche unitaire par niveau (IaaS vers IaaS, PaaS vers PaaS, SaaS vers SaaS). Les architectures Cloud Native combinent différents types de services interconnectés, créant des dépendances complexes qui rendent la migration plus délicate qu'une simple portabilité niveau par niveau, ce qui doit être prise en compte dans l'élaboration des lignes directrices.

Concernant les prestations d'accompagnement, Orange souligne l'importance de distinguer les prestations directement liées au processus de changement de fournisseur de celles relevant de l'accompagnement à la migration. Conformément à l'article 27 de la loi SREN, seules les prestations que seul le fournisseur d'origine peut réaliser doivent être encadrées en termes de tarification. Les prestations d'accompagnement plus larges, qui peuvent être réalisées par des intégrateurs ou le client lui-même, ne devraient pas être soumises à cet encadrement. Cette distinction est d'autant plus importante que la migration d'un système d'information complet implique une complexité bien supérieure au simple transfert de données.

Concernant l'encadrement tarifaire des frais de transfert, Orange défend une approche différenciée qui tient compte non seulement du type de transfert de données, changement de fournisseur ou échanges de données au sein d'une architecture *multi-cloud*, mais aussi de la diversité des services de connectivité *cloud*. Si l'encadrement des frais de transfert via *peering* public peut être pertinent, les frais associés aux offres de connectivité privée devraient être exclues du périmètre de régulation. Cette position s'appuie sur l'article 31 de la loi SREN qui prévoit des exclusions pour les solutions sur-mesure répondant à des besoins spécifiques en termes de performance et de sécurité.

Concernant l'interopérabilité des services *cloud*, Orange préconise une approche différenciée selon les types de services. Pour les services IaaS, déjà largement standardisés, une normalisation supplémentaire apparaît peu pertinente. En revanche, pour les services auxiliaires comme l'IAM (Identity and Access Management) ou l'observabilité, des travaux de normalisation pourraient significativement améliorer la sécurité et la résilience des environnements *cloud*.

Concernant la documentation technique, Orange soutient l'établissement de normes impliquant l'ensemble des parties prenantes, plutôt que de laisser les standards des *hyperscalers* s'imposer par défaut.

Enfin, Orange souligne l'importance d'une approche pragmatique dans la mise en œuvre des obligations réglementaires. Les futures lignes directrices de l'ARCEP devraient établir un cadre, qui facilite la portabilité et l'interopérabilité tout en tenant compte des contraintes techniques et en préservant la capacité d'innovation du marché.

*** **

Observations d'Orange sur l'encadrement des frais de transfert de données et de changement de fournisseur de services *cloud*

Question 1. Avez-vous des observations sur les éléments de contexte liés aux pratiques tarifaires présentées ci-avant ?

Dans le cadre de la mise en œuvre des nouvelles dispositions de la loi SREN relatives à l'encadrement des frais de transfert de données et de changement de fournisseur de services *cloud*, nos observations sur le contexte des pratiques tarifaires portent sur plusieurs aspects essentiels qui méritent d'être soulignés :

- Tout d'abord, il est important de noter une limitation technique fondamentale : en tant que fournisseur de services *cloud*, il n'est techniquement pas possible de distinguer si un transfert de données est lié à un usage quotidien des applications ou à un fonctionnement réparti entre les services *cloud* de différents fournisseurs dans le cadre d'une architecture *multi-cloud* mise en place par l'entreprise cliente. Cette réalité technique doit être prise en compte dans la mise en œuvre de l'article 27 de la loi SREN qui prévoit un encadrement des frais de transfert.
- D'autre part, l'émergence du *cloud* public a profondément modifié les pratiques de facturation du secteur. Les trois principaux *hyperscalers* (AWS, Microsoft Azure et Google Cloud) proposent un modèle de facturation au volume en gigaoctets qui est devenu le standard de fait du marché. Orange, en tant qu'acteur européen du *cloud*, propose une approche différenciée avec son offre Flexible Engine qui maintient un modèle de facturation à la bande passante (en Mbits) sans limite d'usage en volume. Cette approche alternative, qui coexiste avec le modèle dominant de facturation au volume, répond aux besoins spécifiques de certains clients, notamment ceux ayant des usages intensifs en transfert de données ou nécessitant une prévisibilité accrue de leurs coûts.

Quelque soit le modèle de facturation retenu, l'analyse de l'impact financier des frais de transfert de données sortants lors d'un changement de fournisseur, désormais encadrés par l'article 27 II de la loi SREN, révèle qu'il est généralement limité comparé au coût global du service *cloud*, même si le montant augmente très fortement si les contenus stockés sont des fichiers de taille importante, notamment les contenus multimédias.

Prenons deux exemples de cas d'usage principaux pour illustrer cette situation :

- pour un hébergement de système d'information classique (20 machines virtuelles et 5 To de données), les frais de transfert ponctuels représentent environ 8% du prix de l'abonnement mensuel.
- pour un site web avec 20 To de données (images, vidéos), les frais de transfert représentent de l'ordre du double du prix de l'abonnement mensuel.

Ces observations s'inscrivent dans le contexte plus large du règlement européen sur les données (*Data Act*) dont la loi SREN anticipe certaines dispositions. Le règlement prévoit notamment la suppression progressive des frais de changement de fournisseur d'ici 2027, ce qui souligne l'importance d'une approche équilibrée dans la définition du cadre tarifaire transitoire. Les récentes annonces des *hyperscalers* concernant la gratuité des transferts de données pour les changements de fournisseur démontrent que le marché évolue déjà dans cette direction.

Orange soutient cette évolution vers plus de transparence et de flexibilité pour les clients, tout en soulignant l'importance de préserver la diversité des modèles de facturation qui répondent à des besoins différents. Pour autant, la diversité des modèles de facturation (volume vs bande passante, différents types de connectivité apportant différentes qualités de service) ainsi que la difficulté à distinguer la nature des flux de données soulève un enjeu important pour l'application de l'article 27 de la loi SREN ce qui impose de définir précisément le périmètre des frais de transfert soumis à l'encadrement tarifaire. En particulier, il convient de clarifier comment s'applique cet encadrement aux frais de transport des données entre différents environnements *cloud*, que ce soit dans le cadre d'un changement de fournisseur (article 27 II) ou d'une utilisation *multi-cloud* (article 27 IV). Cette clarification est d'autant plus nécessaire que les modèles techniques et commerciaux d'interconnexion entre *clouds* peuvent varier significativement en fonction des choix des entreprises.

Ces éléments de contexte nous semblent essentiels pour éclairer la réflexion dans la définition des modalités d'encadrement tarifaire prévues, en particulier pour la fixation du montant maximal de tarification des frais de transfert de données dans le cadre d'un changement de fournisseur (article 27 V) et l'élaboration des lignes directrices relatives aux frais de transfert dans le cadre du *multi-cloud* (article 27 VI).

Sur l'infrastructure mobilisée pour transférer des données et les catégories de coûts associés

Question 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 ?

La description des transferts de données et des éléments d'infrastructure présentée dans la consultation mérite d'être précisée et complétée pour refléter la réalité complexe du marché des services *cloud*, particulièrement dans le contexte de la mise en œuvre du *Data Act* et de la loi SREN.

En effet, dans le document de consultation, sont identifiés les composants fondamentaux de l'infrastructure supportant les transferts de données : serveurs, équipements de routage et câbles en fibre optique. Toutefois, cette description doit être enrichie pour prendre en compte deux aspects essentiels qui structurent aujourd'hui le marché : l'infrastructure de sécurité et la dualité des modes de connectivité.

L'infrastructure de sécurité constitue un élément indissociable des transferts de données, particulièrement dans le contexte des exigences de l'article 28 de la loi SREN qui impose que la portabilité des données s'effectue "dans des conditions sécurisées". Cette infrastructure comprend notamment des équipements de chiffrement, des pare-feux et des systèmes de détection d'intrusion qui garantissent l'intégrité et la confidentialité des données transférées.

Par ailleurs, il est crucial de distinguer deux modes de connectivité qui répondent à des besoins différents des entreprises. Le premier mode, basé sur le *peering* public, correspond à l'infrastructure décrite dans la consultation. Cependant, il existe également un second mode de connectivité privée, particulièrement important pour les entreprises ayant des exigences spécifiques en matière de sécurité et de performance.

Cette connectivité privée s'appuie pour les offres proposées par Orange sur des réseaux MPLS dédiés, qui offrent des garanties de service (SLA) et une isolation complète d'Internet. Elle permet notamment de répondre aux besoins des entreprises gérant des applications critiques, pour lesquelles la qualité et la sécurité des transferts de données sont primordiales.

Les offres de connectivité privée, qui sont d'ailleurs souvent co-marketées entre les fournisseurs de *cloud* et les opérateurs télécoms, constituent un modèle distinct qui mérite d'être clairement exclus des lignes directrices tarifaires concernant les frais de transfert.

Ces offres se caractérisent par :

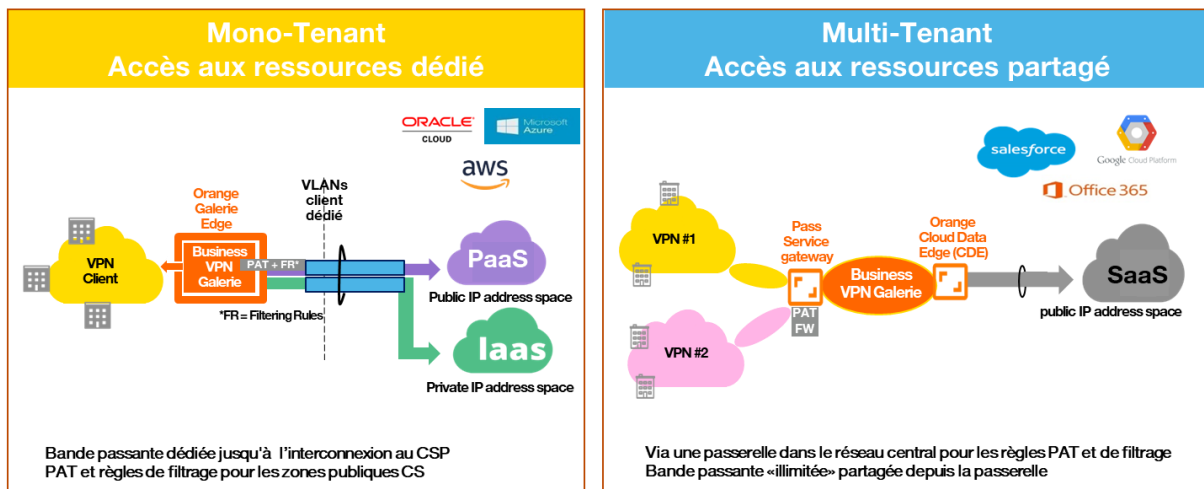
- Une infrastructure entièrement privée et sécurisée
- Des garanties de performance et de disponibilité
- Une supervision continue
- Une flexibilité permettant l'adaptation aux besoins des entreprises

En effet, l'application indifférenciée des mêmes règles aux deux types de connectivité pourrait avoir des effets négatifs sur la capacité des entreprises à choisir le niveau de service adapté à leurs besoins, particulièrement pour les applications critiques nécessitant des garanties renforcées.

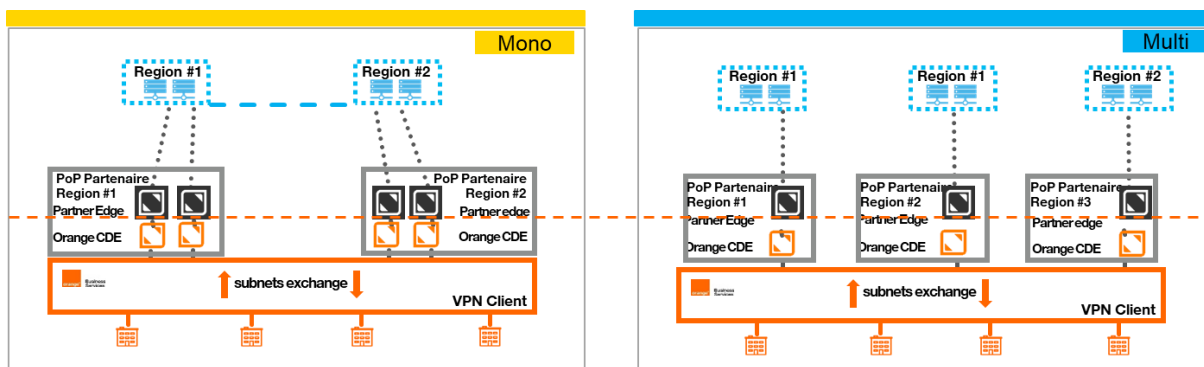
Cette distinction est d'autant plus importante que les offres de connectivité privée sont généralement indépendantes des services *cloud* eux-mêmes et peuvent être utilisées avec l'ensemble des principaux fournisseurs de services *cloud* du marché. Elles constituent ainsi un élément facilitateur du multi-*cloud*, s'inscrivant pleinement dans les objectifs de la loi SREN visant à faciliter le changement de fournisseur et le recours simultané à plusieurs fournisseurs.

En conclusion, il est important de préserver la spécificité des offres de connectivité privée, garantissant ainsi aux entreprises la possibilité de choisir le niveau de service adapté à leurs besoins.

Pour illustrer notre propos, les architectures d'interconnexion physique selon que le service *cloud* interconnecté en mode privé est un IaaS/PaaS mono-tenant ou bien un SaaS multi-tenant sont décrites ci-après :



si l'on focalise sur les équipements et les connexions au sein du colocation center :



Note : CDE signifie *Cloud Data Edge* et désigne des routeurs dédiés connectés aux routeurs du fournisseur de services *cloud*.

Pour les architectures techniques détaillées précédemment, la limite de responsabilité (cf. trait en pointillé) de l'opérateur de *cloud* connectivité privée se situe à l'interface entre les cross-connect privés (liens fibrés) et les ports des « partner edges ».

Question 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.

Les principaux déterminants des coûts liés aux transferts de données méritent d'être approfondie pour refléter la complexité des infrastructures et des modèles de connectivité existants sur le marché des services *cloud*.

Si nous partageons le constat que le transport des données et l'interconnexion constituent des déterminants majeurs des coûts, il est essentiel de distinguer les structures de coûts spécifiques associées aux différents types de connectivité, conformément à l'esprit de l'article 27 de la loi SREN qui vise à encadrer les frais de transfert de données.

- Pour la connectivité via *peering* public, les coûts sont principalement liés à l'infrastructure Internet publique et comprennent plusieurs composantes essentielles. Les fournisseurs doivent investir dans la mise en place et la maintenance de points de présence (POPs), ainsi que dans les équipements d'interconnexion nécessaires pour assurer la connectivité avec d'autres opérateurs. S'ajoutent à cela les frais récurrents de transit et de *peering*, qui varient selon les accords conclus avec les autres acteurs du marché.
- En revanche, la structure de coûts pour la connectivité privée présente des caractéristiques distinctes. Cette connectivité privée, dont les coûts sont supportés directement par l'entreprise, s'appuie sur des infrastructures MPLS dédiées, qui nécessitent des investissements spécifiques et génèrent des coûts d'exploitation associés.

Les coûts associés à la connectivité privée incluent notamment :

- les équipements dédiés pour les cross-connect, essentiels pour assurer l'interconnexion physique sécurisée
- l'hébergement des *Cloud Data Edge* routers, qui permettent le routage optimal des flux de donnée
- le développement et la maintenance du réseau backbone en national et à l'international
- la mise en place et le fonctionnement d'une supervision de bout en bout jusqu'à l'interconnexion avec le fournisseur de services *cloud* (ou partner EDGE).

Ces investissements sont nécessaires pour garantir les niveaux de service (SLA) attendus par les entreprises pour leurs applications critiques, conformément aux exigences des transferts de données dans des conditions sécurisées.

Dans le cas d'une connectivité privée, les coûts ne sont pas uniquement liés au volume de données transférées, mais également aux exigences de qualité de service, de sécurité et de disponibilité.

Par ailleurs, la structure de coûts de la connectivité privée reflète des investissements significatifs dans des infrastructures dédiées qui permettent d'offrir des garanties supérieures en termes de performance et de sécurité. Ces investissements sont distincts de ceux réalisés pour les services *cloud* eux-mêmes et contribuent à la qualité globale du service fourni aux entreprises.

En conclusion, nous recommandons que l'analyse des coûts liés aux transferts de données prenne en compte cette dualité des modèles de connectivité et ne s'applique qu'au service de connectivité via *peering* public.

Question 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.

L'estimation et la quantification des postes de coûts liés aux transferts de données dans le *cloud* soulèvent des enjeux méthodologiques complexes qu'il convient d'analyser dans le contexte des objectifs de la loi SREN et du *Data Act* visant à encadrer les frais de transfert de données.

L'établissement d'une méthodologie uniforme d'estimation des coûts apparaît particulièrement délicat en raison de la multiplicité des facteurs qui influencent la structure des coûts. Cette complexité est d'autant plus importante qu'elle doit s'inscrire dans le cadre de l'article 27 de la loi SREN, qui impose que les frais de transfert de données ne soient pas supérieurs aux coûts supportés par le fournisseur.

En effet, la structure des coûts dépend de nombreux paramètres interdépendants qui varient significativement selon les cas d'usage et les choix technologiques :

- Premièrement, les aspects de dimensionnement jouent un rôle crucial. Le nombre de connexions simultanées, le dimensionnement de la capacité et le niveau d'overbooking influencent directement les investissements nécessaires en infrastructure. Ces éléments sont par nature dynamiques et évoluent en fonction des besoins des clients.
- Deuxièmement, la typologie de connectivité choisie impacte fortement la structure des coûts. Qu'il s'agisse de connexions via *peering* public ou de connectivité privée MPLS, les technologies employées et les niveaux de service associés génèrent des coûts différents. La localisation géographique des infrastructures et des points d'interconnexion constitue également un facteur de variation significatif.
- Troisièmement, les services associés et les garanties de service représentent une composante importante des coûts. La supervision, le niveau de redondance, les garanties de temps de rétablissement et les engagements de performance nécessitent des investissements spécifiques qui doivent être pris en compte dans l'analyse des coûts.

Dans ce contexte, l'utilisation de données de référence standardisées, comme le coût moyen de la bande passante sur le marché européen ou le coût moyen de déploiement d'une interface d'interconnexion, ne permettrait pas de refléter fidèlement la réalité économique des services fournis. Ces indicateurs, bien que pertinents dans une approche macro-économique, ne capturent pas la diversité des situations et des niveaux de service proposés.

Par ailleurs, conformément au considérant 94 du *Data Act* qui souligne l'importance de maintenir "un niveau élevé de sécurité", les coûts liés aux mesures de sécurité et de protection des données doivent

également être considérés. Ces coûts varient selon les exigences spécifiques des clients et les niveaux de protection requis.

Enfin, les outils de monitoring et de reporting permettent certes de suivre la consommation de bande passante et le taux de charge des connexions *cloud*. Cependant, ces données techniques ne permettent pas d'isoler les coûts spécifiquement liés aux transferts de données dans le cadre d'un changement de fournisseur ou d'une utilisation *multi-cloud*, comme le requiert l'article 27 de la loi SREN.

En conclusion, plutôt qu'une approche uniforme basée sur des données de référence standardisées, il nous semble utile d'intégrer les différents facteurs qui influencent la structure des coûts. Cette approche permettrait de mieux refléter la diversité des services proposés et des besoins des entreprises, tout en garantissant la transparence nécessaire sur les frais de transfert de données.

Question 5. 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-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.

La stratégie d'investissements et de dépenses d'exploitation a une influence significative sur les coûts de transfert de données.

En support des offres de connectivité privée d'Orange, nous investissons dans l'extension et la maintenance de notre infrastructure MPLS pour offrir des services de connectivité au *cloud* sécurisés et performants. Le degré d'internalisation des éléments de réseaux du fournisseur, la stratégie propre aux accords d'interconnexion, et les choix technologiques (par exemple, l'utilisation de technologies SDN pour l'automatisation et la flexibilité) influencent directement les coûts de transfert de données.

Les postes de coûts concernés incluent les frais de déploiement et de maintenance des équipements réseau, les frais de transit et de *peering*, et les coûts opérationnels liés à la gestion et à la supervision des connexions *cloud*.

Question 6. 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 ?

L'analyse proposée par l'Autorité concernant la correspondance entre les coûts afférents au transfert de données et la détention d'une capacité d'utilisation de bande passante mérite d'être nuancée et précisée pour refléter la complexité des infrastructures et services de connectivité *cloud*.

En effet, si la capacité d'utilisation de bande passante constitue un élément fondamental dans la structure des coûts, conformément à l'esprit de l'article 27 de la loi SREN qui encadre les frais de transfert de données, cette approche doit être enrichie pour prendre en compte l'ensemble des paramètres qui déterminent la qualité et la sécurité du service.

La capacité de bande passante ne peut être considérée isolément, car elle s'inscrit dans un écosystème technique plus large qui comprend plusieurs dimensions essentielles. Tout d'abord, le dimensionnement de cette capacité doit être adapté aux usages spécifiques des clients, qu'il s'agisse d'utilisations courantes ou de transferts liés à un changement de fournisseur. Ce dimensionnement influence directement les investissements en infrastructure et les coûts d'exploitation associés.

Par ailleurs, conformément au considérant 94 du *Data Act* qui souligne l'importance de maintenir "*un niveau élevé de sécurité*", la mise à disposition de cette capacité nécessite l'implémentation de mesures de sécurité appropriées. Ces mesures, qui génèrent des coûts spécifiques, sont particulièrement importantes dans le contexte de la connectivité privée, où les exigences de sécurité sont généralement plus élevées.

La nature même de la connectivité influence significativement la structure des coûts.

- Dans le cas d'une connectivité via *peering* public, les coûts sont principalement liés à la gestion des interconnexions avec d'autres opérateurs et à la maintenance des points de présence.
- En revanche, pour la connectivité privée, les coûts incluent la maintenance d'une infrastructure dédiée, la gestion d'équipements spécifiques pour garantir la performance et la sécurité, ainsi que la supervision continue du service.

Cette dualité des modèles de connectivité se reflète dans les offres proposées sur le marché.

En conclusion, bien que nous partagions l'analyse de l'Autorité sur l'importance de la capacité d'utilisation de bande passante dans la structure des coûts, nous recommandons une approche plus globale prenant en compte l'ensemble des paramètres qui contribuent à la fourniture d'un service de qualité. Cette approche permettrait de mieux refléter la réalité économique du marché et de garantir que les futures lignes directrices de l'ARCEP préservent la capacité des acteurs à investir dans des infrastructures performantes et sécurisées.

Question 7. 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 ?

La gestion des pics de demande en trafic de ses clients constitue une contrainte fondamentale pour le fournisseur dans le dimensionnement de son réseau.

Ainsi, pour notre offre de connectivité privée, nous dimensionnons notre infrastructure MPLS pour supporter les pics de trafic anticipés, en tenant compte des besoins spécifiques de chaque client. Cela inclut la mise en place de capacités de bande passante suffisantes et la gestion proactive des ressources réseau pour garantir une performance optimale et une disponibilité de 100%.

Question 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 ?

Nous partageons l'analyse de l'Autorité concernant l'impossibilité technique pour les fournisseurs de services *cloud* d'identifier la finalité précise des transferts de données ou de déterminer avec certitude le routage exact du trafic. Cette réalité technique a des implications importantes pour la mise en œuvre des dispositions de l'article 27 de la loi SREN relatives à l'encadrement des frais de transfert de données.

En tant que fournisseur de services *cloud*, nous constatons qu'il est techniquement impossible de distinguer si un transfert de données particulier est lié à un changement de fournisseur, à un usage *multi-cloud* ou à l'utilisation quotidienne des services. Cette limitation s'explique par la grande diversité des architectures applicatives et des cas d'usage mis en œuvre par nos clients. Chaque service fourni à

l'utilisateur final peut présenter des caractéristiques uniques en termes de flux de données et d'interactions réseau.

Cette situation est inhérente à la nature même des services *cloud* et des réseaux sur lesquels ils s'appuient. En effet, seul le propriétaire du service peut connaître la finalité précise de ses transferts de données, car elle est directement liée à ses choix d'architecture et à ses objectifs métier. Le fournisseur de services *cloud*, même s'il peut observer les flux de données, n'a pas la visibilité nécessaire sur l'intention sous-jacente de ces transferts.

Par ailleurs, concernant le routage exact du trafic, la nature distribuée d'Internet et la complexité des interconnexions entre les différents réseaux rendent impossible la prédiction précise du chemin qu'emprunteront les données. Cette incertitude existe même dans le cas de la connectivité privée, bien que dans une moindre mesure grâce à l'utilisation d'infrastructures dédiées.

Même si nous disposons d'outils sophistiqués de monitoring et de reporting permettant de suivre la consommation de bande passante et le taux de charge sur les connexions *cloud* de nos clients, ces outils ne peuvent pas déterminer la finalité spécifique de chaque transfert de données. Ils fournissent des informations techniques précieuses sur les volumes et les performances, mais ne peuvent pas identifier l'intention ou l'usage sous-jacent des transferts.

Cette réalité technique doit être prise en compte dans l'élaboration des lignes directrices de l'ARCEP concernant l'encadrement des frais de transfert de données. En effet, la mise en œuvre effective des dispositions de la loi SREN nécessiterait la mise en place de mécanismes permettant aux clients de déclarer explicitement la finalité de leurs transferts de données lorsque ceux-ci s'inscrivent dans le cadre d'un changement de fournisseur ou d'une architecture *multi-cloud*.

Cette approche déclarative permettrait de concilier les objectifs de la réglementation avec les contraintes techniques inhérentes aux services *cloud*, tout en garantissant la transparence nécessaire sur les frais de transfert de données

Sur le coût incrémental pour réaliser un transfert de données dans le cadre d'un changement de fournisseur d'un client

Question 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.

L'analyse proposée par l'Autorité concernant la nature non récurrente des transferts de données lors d'un changement de fournisseur et la flexibilité supposée de leur mise en œuvre mérite d'être nuancée au regard des réalités opérationnelles des migrations *cloud*.

S'il est exact qu'un changement de fournisseur constitue un événement non récurrent impliquant une quantité définie de données, conformément au cadre établi par l'article 27 de la loi SREN, la notion de flexibilité dans la réalisation de ces transferts doit être examinée plus précisément.

En effet, la flexibilité du processus de migration est contrainte par plusieurs facteurs critiques :

- Premièrement, l'enjeu principal d'une migration *cloud* réside dans la minimisation du temps d'interruption de service (*downtime*). Cette exigence est particulièrement critique pour les applications métier sensibles où chaque minute d'interruption peut avoir des impacts significatifs

sur l'activité des entreprises. Cette contrainte limite considérablement la flexibilité théorique du processus de transfert.

- Deuxièmement, pour minimiser l'impact sur les utilisateurs finaux, les opérations de migration sont souvent planifiées en dehors des heures ouvrées, typiquement la nuit ou le week-end. Cette contrainte temporelle, bien que nécessaire pour l'activité du client, génère des coûts supplémentaires liés à la mobilisation d'équipes techniques en horaires décalés. Cette réalité opérationnelle doit être prise en compte dans l'analyse des coûts, conformément à l'esprit du *Data Act* qui vise à encadrer les frais de changement de fournisseur tout en maintenant la qualité de service.
- Troisièmement, la nécessité de réaliser la migration dans les délais les plus courts possible conduit généralement à utiliser la bande passante maximale disponible. Cette approche, qui vise à minimiser la durée totale de la migration, peut générer des pics de trafic inhabituels. Le fournisseur de services *cloud* doit s'assurer que ces pics de trafic n'impactent pas la qualité de service des autres clients, conformément au considérant 94 du *Data Act* qui souligne l'importance de maintenir "un niveau élevé de sécurité".

Par ailleurs, la complexité des architectures applicatives peut nécessiter des séquences de migration précises et coordonnées, limitant encore davantage la flexibilité théorique du processus. Cette contrainte est particulièrement importante pour les applications critiques où l'ordre de migration des différents composants doit être strictement respecté.

En conclusion, bien que nous partagions le constat du caractère non récurrent des transferts de données lors d'un changement de fournisseur, nous ne pouvons souscrire à l'hypothèse d'une flexibilité significative dans leur réalisation. Les contraintes opérationnelles, techniques et métier imposent souvent des conditions strictes de mise en œuvre qui limitent considérablement la flexibilité du processus.

Cette réalité opérationnelle devrait être prise en compte dans l'élaboration des lignes directrices de l'ARCEP concernant l'encadrement des frais de transfert de données.

Question 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.

L'analyse de l'impact d'un transfert de données dans le cadre d'un changement de fournisseur sur le déploiement d'équipements supplémentaires mérite d'être approfondie en tenant compte des spécificités techniques et opérationnelles des infrastructures *cloud*.

Dans le contexte de l'article 27 de la loi SREN, qui encadre les frais de transfert de données, il est important de comprendre que le dimensionnement des infrastructures *cloud* repose sur une approche statistique sophistiquée qui permet d'optimiser l'utilisation des ressources tout en garantissant la qualité de service.

En effet, le rôle fondamental du fournisseur de services *cloud* est d'assurer un dimensionnement suffisant de son infrastructure pour absorber les variations de charge, y compris les pics de trafic, sans impact sur la qualité de service fournie à l'ensemble de ses clients. Cette capacité à gérer les pics de charge s'inscrit dans une logique d'optimisation continue des ressources, conformément aux principes d'efficacité économique et technique du *cloud computing*.

Dans ce contexte, un transfert de données lié à un changement de fournisseur, bien qu'il puisse générer un pic de trafic significatif pour le client concerné, peut généralement être absorbé par la capacité réseau non utilisée du fournisseur. Cette capacité d'absorption repose sur deux facteurs clés :

- Premièrement, les infrastructures *cloud* sont dimensionnées selon des modèles statistiques, qui prennent en compte la probabilité de pics de trafic simultanés entre différents clients. Cette approche est particulièrement efficace pour les fournisseurs disposant d'une base installée importante de clients, car la loi des grands nombres permet une meilleure prévisibilité et une optimisation plus fine des ressources.
- Deuxièmement, conformément au considérant 94 du *Data Act* qui souligne l'importance de maintenir "un niveau élevé de sécurité", les fournisseurs maintiennent généralement une marge de capacité suffisante pour garantir la stabilité et la résilience de leurs services, même en cas de pics de charge imprévus.

Cette approche permet d'éviter le déploiement d'équipements supplémentaires spécifiquement dédiés aux transferts de données liés aux changements de fournisseur. Les infrastructures existantes, notamment les interconnexions via *peering* public, sont conçues pour absorber ces variations de charge dans le cadre de leur dimensionnement normal.

Cependant, il est important de noter que cette capacité d'absorption des pics de trafic est directement liée à la taille et à la maturité du fournisseur de services *cloud*. Les grands fournisseurs de services *cloud*, bénéficiant d'une base clients importante et diversifiée, sont généralement mieux positionnés pour gérer ces variations de charge sans nécessiter d'investissements supplémentaires spécifiques.

En conclusion, nous confirmons que les transferts de données liés aux changements de fournisseur n'impliquent généralement pas le déploiement d'équipements supplémentaires, grâce à une approche de dimensionnement statistique des infrastructures et à l'optimisation continue des ressources.

Question 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.

Au-delà de la structure de coût mise en place pour assurer le transfert de données « classique » avec le bon niveau de qualité, et en l'absence de demande particulière d'un client sur le niveau de qualité de service (QoS) d'un transfert de données spécifique, il n'est pas identifié de coût incrémental spécifique pour un transfert de données dans le cadre d'un changement de fournisseur.

Lorsqu'un client décide de changer de fournisseur, le transfert de données peut être réalisé en utilisant cette infrastructure existante, sans nécessiter de déploiement d'équipements supplémentaires ou de ressources spécifiques. En l'absence de demande particulière d'un client sur le niveau de QoS d'un transfert de données spécifique, le transfert peut être effectué en utilisant les capacités de bande passante et les ressources réseau déjà disponibles.

Question 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 ?

Dans le cadre de l'article 27 de la loi SREN qui encadre les frais de transfert de données, il convient d'identifier certains cas spécifiques où la facturation du transfert de données lors d'un changement de fournisseur pourrait être justifiée par des exigences particulières des clients générant des coûts additionnels directement imputables.

Ces situations particulières concernent principalement les cas où les clients expriment des besoins spécifiques en termes de garanties de service pour le transfert de leurs données, allant au-delà des conditions standards de migration. Ces exigences peuvent être justifiées par la nature critique de leurs activités ou par des contraintes réglementaires spécifiques à leur secteur.

Plusieurs cas de figure peuvent être identifiés :

1. Garanties de performance spécifiques

Lorsqu'un client requiert des garanties de bande passante dédiée pour sa migration, nécessitant une réservation de capacité qui sort du cadre du dimensionnement statistique habituel, des coûts spécifiques peuvent être encourus.

2. Contraintes temporelles strictes

Dans les cas où le client exige des créneaux de migration très précis avec des garanties de temps de transfert, nécessitant une mobilisation dédiée de ressources techniques et une supervision renforcée, des coûts supplémentaires peuvent être justifiés.

3. Exigences de sécurité renforcée

Certains clients, notamment dans les secteurs régulés, peuvent nécessiter des mesures de sécurité additionnelles pour leurs transferts de données, comme le chiffrement renforcé ou des tunnels dédiés, générant des coûts spécifiques.

4. Besoins spécifique de reporting et de traçabilité

Les clients soumis à des obligations réglementaires strictes peuvent avoir besoin de rapports détaillés et d'une traçabilité complète du processus de migration, nécessitant la mise en place d'outils et de procédures spécifiques.

Dans ces situations, les coûts additionnels peuvent être directement liés à :

- la mise en place d'infrastructures dédiées temporaires
- la mobilisation d'équipes techniques spécialisées
- l'implémentation de mesures de sécurité supplémentaires
- le développement d'outils de supervision et de reporting spécifiques

Ces cas particuliers devraient être clairement identifiés et documentés dans les contrats, conformément à l'article 27 de la loi SREN qui impose aux fournisseurs de communiquer de façon claire et compréhensible les informations sur les frais de transfert de données.

Cependant, il est important de souligner que ces situations doivent rester exceptionnelles et être justifiées par des besoins objectifs et mesurables. La facturation associée devrait être strictement limitée aux coûts supplémentaires directement imputables à ces exigences spécifiques, conformément au principe de proportionnalité.

En conclusion, il est important d'identifier et de traiter ces cas particuliers, tout en maintenant des garde-fous stricts pour éviter toute dérive dans la facturation des transferts de données.

Question 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 ?

L'hypothèse d'un plafond des frais de transfert de données fixé à zéro dans le cadre d'un changement de fournisseur mérite d'être précisée pour tenir compte des différentes situations de transfert et des modèles de connectivité existants sur le marché.

Si le principe d'un plafond à zéro s'inscrit dans l'esprit de l'article 27 de la loi SREN visant à faciliter le changement de fournisseur, il convient de délimiter précisément son périmètre d'application pour préserver la capacité des acteurs à répondre aux besoins spécifiques de certains clients.

Nous proposons que ce plafond à zéro s'applique aux transferts de données standards réalisés dans le cadre d'un changement de fournisseur, c'est-à-dire aux situations où :

- le transfert utilise l'infrastructure existante sans exigence particulière
- aucune garantie de service spécifique n'est requise
- les conditions de sécurité standard sont suffisantes
- aucun besoin de reporting particulier n'est exprimé

En effet, dans ces situations standards, les coûts de transfert peuvent être absorbés par l'infrastructure existante, qu'il s'agisse de connexions via *peering* public ou d'infrastructures spécifiques pour une connectivité privée, sans générer de coûts additionnels significatifs.

Cependant, conformément à l'analyse développée en réponse à la question 12 et au considérant 94 du *Data Act* qui souligne l'importance de maintenir "un niveau élevé de sécurité", certaines situations particulières devraient pouvoir faire l'objet d'une tarification spécifique lorsque :

- des garanties de performance dédiées sont requises
- des contraintes temporelles strictes sont imposées
- des exigences de sécurité renforcées sont nécessaires
- des besoins de reporting et de traçabilité particuliers sont exprimés

Dans ces cas spécifiques, les coûts additionnels directement liés à ces exigences particulières devraient pouvoir être facturés, sous réserve qu'ils soient :

- clairement identifiés et documentés
- directement liés aux exigences spécifiques du client
- proportionnés aux services additionnels fournis
- communiqués de manière transparente, conformément à l'article 27 (VII) de la loi SREN

En conclusion, nous recommandons que le plafond à zéro soit appliqué aux transferts de données standards via *peering* public tout en prévoyant un cadre spécifique pour les situations nécessitant des garanties ou des services additionnels.

Sur les coûts directement imputables aux transferts de données réalisés dans le cadre d'un usage *multi-cloud*

Question 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.

L'analyse des caractéristiques des transferts de données dans le cadre d'un usage *multi-cloud* nécessite une approche nuancée qui prenne en compte la diversité des architectures et des cas d'usage.

Dans le contexte de l'article 27 de la loi SREN, qui distingue les frais de transfert de données selon leur finalité, il est essentiel de comprendre que les transferts liés au *multi-cloud* présentent des caractéristiques fondamentalement différentes de ceux associés à un changement de fournisseur.

En effet, le profil de trafic généré par une architecture *multi-cloud* est intrinsèquement lié au design de la solution mise en place par le client. Cette architecture détermine non seulement la fréquence et le volume des transferts, mais également leur variabilité dans le temps. Les transferts de données dans ce contexte peuvent présenter des caractéristiques similaires à celles d'un trafic classique orienté vers l'utilisateur final, avec :

1° une récurrence qui dépend directement des choix d'architecture faits par l'entreprise cliente tels que la réplication de données entre *clouds*, la synchronisation d'applications distribuées ou les échanges entre services complémentaires

2° une variabilité qui reflète par conséquence les pics d'activité des applications, les cycles métier de l'entreprise et les besoins de synchronisation des données.

Cette nature récurrente et variable du trafic *multi-cloud*, conforme au considérant 99 du *Data Act* qui reconnaît que "*le processus de sortie des données d'un fournisseur [...] vers un autre dans le but de faciliter l'utilisation simultanée de services peut constituer une activité continue*", implique des contraintes spécifiques en termes de dimensionnement et de gestion des infrastructures.

Contrairement à un changement de fournisseur qui représente un événement ponctuel et planifiable, le trafic *multi-cloud* nécessite une infrastructure capable de supporter des variations de charge importantes, mais aussi de garantir une disponibilité continue, de maintenir des performances constantes et d'assurer une sécurité permanente.

Cette réalité technique a des implications importantes pour :

- le dimensionnement des infrastructures
- la gestion de la qualité de service
- la tarification des services
- la planification des capacités

En conclusion, nous confirmons que les transferts de données dans le cadre d'un usage *multi-cloud* présentent effectivement un caractère récurrent et variable, directement lié à l'architecture technique choisie par le client. Cette caractéristique fondamentale doit être prise en compte dans l'élaboration des lignes directrices de l'ARCEP concernant l'encadrement des frais de transfert de données, afin

d'assurer un cadre réglementaire adapté à la réalité opérationnelle des architectures *multi-cloud* tout en préservant la capacité des acteurs du marché à fournir des services adaptés aux besoins des entreprises.

Question 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 ?

L'article 28 de la loi SREN impose aux fournisseurs de services *cloud* d'assurer l'interopérabilité et la portabilité des données "*dans des conditions sécurisées*". Pour répondre à cette exigence dans le contexte du *multi-cloud*, des équipements spécifiques peuvent être déployés pour permettre une connectivité directe et sécurisée vers les différents fournisseurs de services *cloud*.

La mise en œuvre d'une stratégie de *cloud* connectivité efficace nécessite en effet le déploiement et la gestion d'une infrastructure réseau sophistiquée. Cette infrastructure s'appuie principalement sur des réseaux existants, complétés par des interconnexions physiques mutualisées multi-clients qui permettent d'optimiser les coûts tout en garantissant la qualité de service requise.

Ces infrastructures doivent être spécifiquement dimensionnées et configurées pour supporter les transferts de données *multi-cloud*, avec une attention particulière portée à la capacité de bande passante et à la gestion proactive des ressources réseau. Cette approche vise à garantir une performance optimale et une disponibilité maximale, conformément aux exigences du considérant 94 du *Data Act* qui souligne l'importance de maintenir "*un niveau élevé de sécurité*" dans les échanges de données.

Dans le cadre des offres de connectivité privée basées sur le réseau MPLS, la spécificité de ces équipements réside notamment dans leur capacité à assurer une connectivité directe vers les différents fournisseurs de services *cloud*, évitant ainsi le transit par Internet public et garantissant des performances prévisibles et sécurisées. Cette connectivité directe nécessite des investissements significatifs en termes d'infrastructure, mais permet d'offrir des garanties de service essentielles pour les utilisations professionnelles du *multi-cloud*.

Dans une architecture comme dans l'autre, la gestion de ces équipements requiert également une expertise particulière pour assurer leur configuration optimale et leur maintenance continue. Cette expertise est nécessaire pour garantir non seulement la performance des transferts de données, mais aussi leur sécurité et leur fiabilité, conformément aux attentes des clients professionnels et des entreprises.

En conclusion, si l'infrastructure existante constitue la base des services de connectivité *multi-cloud*, des équipements et des configurations spécifiques sont nécessaires pour garantir la qualité et la sécurité des transferts de données dans ce contexte particulier.

Question 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 ?

Les postes de coûts susceptibles d'être affectés par un usage *multi-cloud* incluent les frais de bande passante, les frais de transit et de *peering*, et les coûts opérationnels liés à la gestion et à la supervision des connexions *cloud*.

Même si nous utilisons des outils de monitoring et de reporting pour suivre la consommation de bande passante et le taux de charge sur les connexions *cloud* de nos clients, cela ne nous permet pas d'allouer les coûts de manière précise et transparente sans connaître l'usage de ces données et donc sans pouvoir distinguer ce qui relève d'une utilisation nominale des applications ou d'un transfert de données.

Question 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 ?

Nous avons identifié des situations particulières où certains clients présentent des besoins spécifiques qui peuvent justifier des coûts supplémentaires pour les transferts de données dans le cadre d'un usage *multi-cloud*, notamment les grandes entreprises ou les organisations soumises à des réglementations sectorielles strictes, qui expriment des attentes particulières en termes de qualité de service et de sécurité pour leur connectivité *cloud*.

Ces besoins spécifiques se manifestent principalement à travers des exigences de niveau de service élevé pour la connectivité vers le *cloud*, nécessitant la mise en place d'interconnexions spécifiques. Ces exigences peuvent être justifiées par la nature critique des applications hébergées, les obligations réglementaires auxquelles sont soumis ces clients, ou encore leurs besoins spécifiques en termes de performance et de disponibilité.

Ces situations particulières font généralement l'objet de solutions techniques dédiées et d'une contractualisation spécifique qui définit précisément : les niveaux de service garantis, les outils de supervision et de reporting, des mécanismes de sécurité et des modalités de support dédiés.

Il est par ailleurs important de souligner que le *Data Act* et la loi SREN prévoient explicitement des exclusions pour les solutions sur mesure. En effet, l'article 31 de la loi SREN énonce que les obligations définies ne s'appliquent pas "*aux services d'informatique en nuage dont la majorité des caractéristiques principales ont été conçues sur mesure pour répondre aux besoins spécifiques d'un client particulier ou dont tous les composants ont été développés pour les besoins d'un client spécifique et qui ne sont pas offerts à grande échelle sur le plan commercial par l'intermédiaire du catalogue de services du fournisseur de services d'informatique en nuage*".

Cette approche du législateur reconnaît ainsi la spécificité de certains besoins clients qui ne peuvent être satisfaits par des offres standards et nécessitent des développements particuliers. Elle permet également de préserver la capacité d'innovation des fournisseurs pour répondre aux besoins les plus exigeants de leurs clients, tout en maintenant un cadre clair pour les services standards.

En conclusion, les solutions sur mesure, développées spécifiquement pour répondre aux besoins particuliers de certains clients en matière de qualité de service, de sécurité ou de performance, y compris les solutions de connectivité, peuvent légitimement être considérées comme relevant de cette exclusion, dès lors qu'elles répondent aux critères définis.

Sur les frais de changement de fournisseur autres que ceux liés au transfert de données

Question 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 ?

Considérant que l'article 27 de la loi SREN interdit aux fournisseurs de facturer des frais de changement de fournisseur supérieurs aux coûts supportés par le fournisseur et directement liés à ce changement, il convient de distinguer les prestations directement liées au processus de changement de fournisseur des prestations supplémentaires d'accompagnement à la migration. Les prestations directement liées au processus de changement de fournisseur sont celles qui ne peuvent être réalisées que par le fournisseur de services *cloud* d'origine et qui rentrent dans le périmètre de ses obligations de facilitation du changement de fournisseur, telles que définies par le règlement sur les données (*Data Act*) et la loi SREN.

Le règlement sur les données précise que les frais de changement de fournisseur incluent, outre les frais liés au transfert de données, les frais encourus pour des actions de soutien spécifiques pendant le processus de changement de fournisseur (article 29 du *Data Act*). Ces actions de soutien comprennent notamment l'extraction des données dans un format lisible par machine, la fourniture des capacités, des informations, de la documentation, de l'assistance technique adéquate et, le cas échéant, des outils nécessaires pour faciliter le processus de changement de fournisseur (considérant 92 du *Data Act*).

En tant que fournisseur de services *cloud*, Orange a une expérience significative dans l'accompagnement de ses clients entreprise lors de changements de fournisseur. Notre position nous permet de constater que le changement de fournisseur est souvent assimilé à un simple transfert de données au sens de fichiers à plat type S3, ce qui est restrictif. En réalité, la plupart du temps, le changement de fournisseur est beaucoup plus complexe car l'extraction de données permettant une réutilisation est très compliquée pour plusieurs raisons :

- Premièrement, l'automatisation est difficile en raison de l'absence de formats universels. Cela nécessite des interventions manuelles complexes au niveau technique, avec l'utilisation de logiciels spécifiques pour migrer les données, mais aussi au niveau organisationnel, avec une connaissance approfondie des deux environnements et une phase de migration proprement dite.
- Deuxièmement, les ressources nécessaires pour réaliser ces migrations sont de type Professional Services, c'est-à-dire des ressources qualifiées pour effectuer des évaluations, mener des projets de transition et gérer une période de double run.

L'analyse menée à date par l'Autorité indique que la nature des prestations directement liées au processus de changement de fournisseur est intimement liée au degré d'adhérence qu'aura développé le client avec l'environnement *cloud* de son fournisseur. Plus les services proposés au client sont personnalisés, plus il lui sera coûteux de migrer le service en question dans un autre environnement.

Il est également important de souligner que la vision développée dans le texte de la consultation semble souvent unitaire, partant de la machine virtuelle ou de la base de données stockée dans le *cloud*. Cependant, en tant que fournisseur de services *cloud*, nous constatons que la migration de systèmes d'information complets est bien plus complexe. Ces systèmes s'appuient sur différentes applications, chacune supportée par sa propre infrastructure matérielle et logicielle. La migration d'un système d'information complet implique donc une complexité bien plus grande que le simple transfert de machines virtuelles ou de bases de données. Elle nécessite une coordination étroite entre les différentes couches de l'infrastructure et des applications, ainsi qu'une gestion rigoureuse des dépendances et des interconnexions entre les composants du système.

Pour respecter ses obligations de facilitation du changement de fournisseur, le fournisseur d'origine doit réaliser plusieurs prestations spécifiques :

- l'extraction des données : Le fournisseur d'origine doit extraire les données du client dans un format lisible par machine. Cette prestation inclut la préparation des données pour le transfert, en s'assurant qu'elles sont complètes et intègres. Les coûts associés incluent les heures de travail des techniciens et des ingénieurs de données, ainsi que les frais liés à l'utilisation de logiciels spécifiques d'extraction.
- la fourniture des capacités nécessaires : Le fournisseur d'origine doit fournir les capacités techniques nécessaires pour permettre le transfert des données. Cela peut inclure la mise à disposition de bande passante suffisante, de ressources de stockage temporaires et d'autres infrastructures nécessaires pour faciliter le transfert. Les coûts associés incluent les frais d'infrastructure et les coûts opérationnels liés à l'utilisation de ces ressources.
- la documentation et l'assistance technique : Le fournisseur d'origine doit fournir une documentation détaillée sur les données et les systèmes du client, ainsi qu'une assistance technique pour répondre aux questions et résoudre les problèmes éventuels pendant le processus de migration. Les coûts associés incluent les heures de travail des experts techniques et des consultants en migration.
- la mise à disposition d'outils spécifiques : Le fournisseur d'origine doit mettre à disposition les outils nécessaires pour faciliter le transfert des données. Cela peut inclure des logiciels de transfert de données, des outils de conversion de formats et d'autres solutions techniques adaptées aux besoins spécifiques du client. Les coûts associés incluent les frais de licence des outils et les coûts de développement ou de personnalisation des solutions.

En conclusion, les prestations directement liées au processus de changement de fournisseur, telles que définies par le règlement sur les données et la loi SREN, relèvent principalement de la mise à disposition de main-d'œuvre pour des actions de soutien spécifiques. Il est important que ces prestations soient facturées de manière transparente et proportionnée, en reflétant les coûts complets de personnel effectivement supportés par le fournisseur. Les lignes directrices de l'Arcep devront préciser les modalités de détermination de ces coûts sur la base des coûts complets de personnel du fournisseur de services *cloud* et ce quel que soit le niveau de qualification et le pays de l'expert concerné, afin de garantir une tarification juste et équitable pour les clients.

Question 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 téléversement des données ? Le cas échéant, quels seraient les coûts supportés par le fournisseur d'origine associés à ces prestations ?

En complément des prestations directement liées au processus de changement de fournisseur, il est essentiel de distinguer les prestations supplémentaires d'accompagnement à la migration, qui peuvent être réalisées par l'entreprise elle-même ou par un intégrateur tiers. Ces prestations vont au-delà des obligations de facilitation du changement de fournisseur et incluent des services spécifiques demandés par le client pour assurer une migration réussie.

Les prestations supplémentaires d'accompagnement à la migration comprennent :

- L'évaluation initiale des systèmes et des données : Cette étape consiste à réaliser un audit complet des systèmes d'information et des données du client pour identifier les dépendances, les interconnexions et les éventuelles incompatibilités avec l'environnement du nouveau fournisseur. Les coûts associés à cette prestation incluent les heures de travail des experts techniques et des consultants en migration.
- La planification et la gestion de projet : La migration d'un système d'information complet nécessite une planification rigoureuse et une gestion de projet pour coordonner les différentes étapes de la migration, minimiser les interruptions de service et garantir une transition en douceur. Les coûts associés incluent les frais de gestion de projet, les réunions de coordination et les outils de gestion de projet.
- La transformation des données : Une fois les données extraites, elles doivent souvent être transformées pour correspondre au schéma et aux formats du nouvel environnement. Cette étape peut inclure la conversion de bases de données, la modification de scripts et la réécriture de certaines parties du code. Les coûts associés incluent les heures de travail des développeurs et des ingénieurs de données.
- Le téléversement des données : Après transformation, les données doivent être téléversées dans l'environnement du nouveau fournisseur. Cette étape peut nécessiter des outils spécifiques pour assurer la sécurité et l'intégrité des données pendant le transfert. Les coûts associés incluent les frais de licence des outils de transfert de données et les heures de travail des techniciens.
- Les tests et la validation : Avant de mettre en production le nouveau système, il est essentiel de réaliser des tests pour s'assurer que toutes les applications fonctionnent correctement dans le nouvel environnement. Les coûts associés incluent les heures de travail des testeurs et des ingénieurs qualité, ainsi que les éventuels frais de correction des problèmes identifiés.
- La formation et le support post-migration : Une fois la migration terminée, il est souvent nécessaire de former les utilisateurs finaux et les administrateurs système à l'utilisation du nouvel environnement. De plus, un support post-migration peut être nécessaire pour résoudre les problèmes éventuels et assurer une transition en douceur. Les coûts associés incluent les frais de formation, les supports pédagogiques et les heures de travail des équipes de support.

Ces prestations supplémentaires d'accompagnement à la migration sont souvent réalisées par des intégrateurs spécialisés ou par l'entreprise elle-même, avec le soutien du fournisseur de services *cloud*. Elles sont essentielles pour garantir une migration réussie et minimiser les risques d'interruption de service. Il est important que ces prestations soient clairement distinguées des prestations directement liées au processus de changement de fournisseur de services *cloud*.

Question 20. Avez-vous d'autres remarques concernant les frais de changement de fournisseur autres que ceux liés aux transferts de données ?

Dans le contexte de l'article 27 de la loi SREN, les frais de changement de fournisseur ne peuvent pas être supérieurs aux coûts supportés par le fournisseur et directement liés à cette migration, ce qui souligne le besoin de définir un standard d'automatisation et de processus pour l'opérationnalisation de la réglementation relative au changement de fournisseur.

Cette nécessité se justifie par le fait que les trois acteurs majeurs du marché, ainsi que les opérateurs de data centers tels qu'Equinix, proposent tous des formats standards, des outils et des processus pour la migration des données et des applications. Cependant, ces formats et processus sont tous différents les uns des autres, ce qui complique la migration pour les clients et entraîne des coûts supplémentaires. Par exemple, Amazon Web Services propose AWS DataSync et AWS Snowball, Google Cloud propose Transfer Appliance et Storage Transfer Service, et Microsoft Azure propose Azure Migrate et Data Box. De même, Equinix propose des solutions spécifiques pour l'interconnexion et le transfert de données entre différents environnements *cloud*. Bien que ces outils et processus soient conçus pour faciliter la migration, leur diversité crée une fragmentation qui complique la tâche des entreprises souhaitant changer de fournisseur.

En outre, au-delà des différences de formats et de processus, nous constatons un manque d'équivalence fonctionnelle entre les services proposés par ces différents fournisseurs. Chaque fournisseur propose des services spécifiques avec des fonctionnalités uniques, ce qui rend difficile la migration sans adaptation ou transformation des données et des applications. Cette situation entraîne des coûts supplémentaires pour les entreprises, qui doivent souvent recourir à des services professionnels pour adapter leurs systèmes aux nouveaux environnements.

Pour répondre à ces défis, un standard d'automatisation et/ou de processus permettrait de réduire les coûts et les complexités associés à la migration en harmonisant les formats et les processus de transfert de données et d'applications. Il faciliterait également l'interopérabilité entre les différents environnements *cloud*, en permettant aux entreprises de migrer plus facilement leurs systèmes sans avoir à adapter ou transformer leurs données et applications de manière significative.

La mise en place d'un standard d'automatisation et/ou de processus pourrait inclure les éléments suivants :

1. Formats de données standardisés : Définir des formats de données standards pour les principaux types de données (par exemple, bases de données, fichiers, objets) afin de faciliter leur transfert entre différents environnements *cloud*.
2. API et outils de migration standardisés : Développer des API et des outils de migration standardisés qui peuvent être utilisés par tous les fournisseurs de services *cloud* et opérateurs de data centers. Ces outils devraient être compatibles avec les principaux environnements *cloud* et permettre une migration transparente des données et des applications.
3. Processus de migration harmonisés : Établir des processus de migration harmonisés qui définissent les étapes clés de la migration, les rôles et responsabilités des parties impliquées, et les meilleures pratiques pour minimiser les interruptions de service et garantir l'intégrité des données.

4. Équivalence fonctionnelle : Promouvoir l'équivalence fonctionnelle entre les services proposés par les différents fournisseurs de services *cloud*, en encourageant l'adoption de standards communs pour les fonctionnalités de base (par exemple, stockage, calcul, réseau) et en facilitant l'interopérabilité des services spécifiques.

En conclusion, la définition d'un standard d'automatisation et/ou de processus en collaboration avec les principaux acteurs du marché et les organismes de normalisation pourrait réduire les coûts et les complexités associés à la migration.

Observations d'Orange sur la réduction des difficultés techniques liées au changement de fournisseur et au recours simultané à plusieurs fournisseurs de services *cloud*

sur l'interopérabilité et la portabilité des services *cloud*

Question 21. 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 ?

L'article 29, I de la loi SREN mentionne l'importance de définir clairement les services IaaS (*Infrastructure as a Service*) pour faciliter le changement de fournisseur et le recours simultané à plusieurs fournisseurs de services *cloud* (*multi-cloud*).

Dans ce contexte, nous recommandons de limiter les services IaaS aux services de base tels que les capacités de calcul et de stockage permettant l'exécution de machines virtuelles (VM), ce qui permet la définition d'une base de services standards et potentiellement standardisés, et facilite la portabilité et l'interopérabilité entre les différents environnements *cloud* pour les services de base.

Les services IaaS managés incluent des fonctionnalités supplémentaires telles que la gestion automatisée, les mises à jour de sécurité, les sauvegardes, et les optimisations de performance. Ces services introduisent des spécificités et des dépendances qui compliquent la migration et l'interopérabilité.

Question 22. Que pensez-vous de ces typologies et définitions relatives aux autres services *cloud* mentionnés à l'article 29, I de la loi SREN ?

L'article 29, I de la loi SREN mentionne différentes typologies de services *cloud*, notamment les services IaaS (Infrastructure as a Service) et PaaS (Platform as a Service). Cependant, les définitions actuelles de ces services ne reflètent pas pleinement la réalité de leur utilisation par les clients.

Les définitions de IaaS et de PaaS ne font pas état du fait que les fonctionnalités IaaS et PaaS sont très imbriquées. En pratique, sous un même contrat, le client va consommer à la fois des services IaaS et des services PaaS. Cette imbrication des services est une caractéristique essentielle des environnements *cloud* actuels et doit être prise en compte dans les définitions suivantes et les typologies utilisées pour réguler le marché :

- Les services IaaS fournissent des ressources informatiques de base telles que la puissance de calcul, le stockage et les réseaux. Ils permettent aux clients de déployer et de gérer des machines virtuelles d'autres infrastructures de base.
- Les services PaaS, quant à eux, offrent des environnements de développement et de déploiement d'applications, en fournissant des outils et des services supplémentaires tels que les bases de données gérées, les environnements de développement intégrés, les services de messagerie et les plateformes d'intelligence artificielle.

En effet, dans la réalité des contrats de services *cloud*, les clients ne consomment pas ces services de manière isolée. Au contraire, ils utilisent souvent une combinaison de services IaaS et PaaS pour répondre à leurs besoins spécifiques.

Par exemple, un client peut utiliser des machines virtuelles (IaaS) pour héberger des applications, tout en utilisant des bases de données gérées (PaaS) pour stocker et gérer les données de ces applications. De même, un client peut utiliser des conteneurs (IaaS) pour déployer des micro-services, tout en utilisant des services de messagerie (PaaS) pour assurer la communication entre ces micro-services.

Cette imbrication des services IaaS et PaaS présente plusieurs avantages pour les clients. Elle leur permet de bénéficier de la flexibilité et de la scalabilité des services IaaS, tout en profitant des fonctionnalités avancées et des outils de développement offerts par les services PaaS. Elle permet également une meilleure intégration et une gestion plus efficace des applications et des infrastructures.

Pour refléter cette réalité, il serait utile de proposer des définitions plus flexibles, qui reconnaissent que les clients consomment souvent des services IaaS et PaaS de manière combinée et intégrée.

En conclusion, les définitions actuelles de IaaS et de PaaS ne reflètent pas pleinement la réalité de leur utilisation par les clients, qui consomment souvent ces services de manière imbriquée et intégrée.

Question 23. Partagez-vous la compréhension de l'Arcep quant à la distinction entre services « standards » et « spécifiques » ?

L'article 29, I de la loi SREN mentionne différentes typologies de services *cloud*, notamment les services « standards » et « spécifiques ». Cependant, cette distinction pourrait être affinée pour mieux refléter la réalité des offres de services *cloud*.

En effet, plutôt que de parler de services « standards » et « spécifiques », il serait pertinent de distinguer entre les « socles de services » et les « services différenciants pour les fournisseurs » :

- Les « socles de services » sont des services fournis par tous les fournisseurs de services *cloud*, sans toutefois obéir à un standard strict en termes de formats, d'applications, etc... Ces services incluent des fonctionnalités de base telles que la puissance de calcul, le stockage, les réseaux, les bases de données, et les environnements de développement. Bien que ces services soient disponibles chez tous les fournisseurs, ils peuvent varier en termes de performance, de prix, et de modalités de mise en œuvre.

Par exemple, tous les fournisseurs proposent des machines virtuelles et des services de stockage d'objets, mais les spécificités techniques et les interfaces utilisateur peuvent différer.

- Les « services différenciants pour les fournisseurs » sont des services qui permettent aux fournisseurs de se distinguer les uns des autres. Ces services sont souvent en perpétuelle évolution et incluent des fonctionnalités avancées et innovantes qui répondent à des besoins spécifiques des clients.

Par exemple, certains fournisseurs peuvent offrir des services d'intelligence artificielle, des plateformes d'Internet des objets (IoT), des outils de gestion de la sécurité, ou des services de blockchain. Ces services différenciants sont souvent développés pour répondre à des besoins émergents et peuvent offrir des avantages compétitifs significatifs aux clients qui les utilisent.

Chaque fournisseur de services *cloud* dispose de sa propre interface utilisateur, ce qui ajoute une couche supplémentaire de différenciation. Les interfaces utilisateur peuvent varier en termes de convivialité, de fonctionnalités, et de capacités de personnalisation. Cette diversité permet aux clients de choisir le fournisseur qui offre l'interface la mieux adaptée à leurs besoins et à leurs préférences.

En conclusion, la distinction entre services « standards » et « spécifiques » pourrait être affinée en parlant de « socles de services » et de « services différenciants pour les fournisseurs ». Cette approche permettrait de mieux refléter la réalité des offres de services *cloud* et de reconnaître la diversité et l'innovation qui caractérisent ce marché.

Question 24. 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 ?

Dans le contexte de l'article 29, I de la loi SREN, qui mentionne l'importance de faciliter le changement de fournisseur et le recours simultané à plusieurs fournisseurs de services *cloud* (*multi-cloud*), il est important d'examiner dans quelle mesure les outils « *cloud-agnostiques* » couvrent les besoins des utilisateurs afin de s'adapter aux différences entre les offres de services *cloud*.

Terraform est un exemple d'outil dit « *cloud-agnostique* » qui permet de paramétrer des infrastructures *cloud* chez différents fournisseurs de *cloud*. Terraform facilite l'utilisation de ces différents fournisseurs en offrant une interface commune pour la gestion des infrastructures, ce qui permet aux utilisateurs de déployer et de gérer des ressources sur plusieurs plateformes *cloud* à partir d'un même ensemble de configurations.

Cependant, il est important de noter que Terraform ne permet pas de s'affranchir complètement de la compétence relative à chaque environnement. En effet, chaque fournisseur de services *cloud* a ses propres spécificités et particularités, et les utilisateurs doivent avoir une connaissance approfondie de ces spécificités pour utiliser efficacement Terraform.

Par exemple, les configurations réseau, les options de sécurité, et les services spécifiques peuvent varier d'un fournisseur à l'autre, et ces différences doivent être prises en compte lors de la création des configurations Terraform.

En outre, l'utilisation de Terraform dans un contexte *multi-cloud* s'avère rapidement très complexe. La gestion de plusieurs environnements *cloud* simultanément nécessite une coordination étroite et une compréhension approfondie des interactions entre les différentes plateformes. Les utilisateurs doivent être capables de gérer les dépendances entre les ressources déployées sur différents *clouds*, de synchroniser les configurations, et de résoudre les conflits potentiels. Cette complexité peut entraîner des défis supplémentaires en termes de gestion et de maintenance des infrastructures.

Il n'existe pas de langage universel pour toutes les configurations *cloud*, car chaque provider nécessite une connaissance des spécificités de son environnement. Ainsi, bien que Terraform facilite l'utilisation de ces différents fournisseurs, chaque interaction reste liée à la plateforme de services cible. Les utilisateurs doivent adapter leurs configurations en fonction des particularités de chaque fournisseur, ce qui peut nécessiter des ajustements et des personnalisations spécifiques.

En conclusion, bien que les outils « *cloud-agnostiques* » comme Terraform offrent des avantages significatifs en termes de gestion des infrastructures *multi-cloud*, ils ne permettent pas de s'affranchir complètement des compétences spécifiques à chaque environnement. L'utilisation de Terraform dans

un contexte *multi-cloud* peut s'avérer complexe et nécessite une compréhension approfondie des spécificités de chaque fournisseur de services *cloud*.

Question 25. 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 ?

L'article 28 de la loi SREN définit les actifs numériques comme « *tous les éléments au format numérique, y compris les applications, sur lesquels le client d'un service d'informatique en nuage a un droit d'utilisation, indépendamment de la relation contractuelle que le client a avec le service d'informatique en nuage qu'il a l'intention de quitter* ».

Il nous semble utile de compléter cette définition en ajoutant aux applications les configurations et toutes les dépendances, qu'elles soient verticales (connecteurs) ou horizontales (dépendances entre les applications). La complexité de ces configurations ne dépend pas du fournisseur de *cloud*, mais de la complexité du système d'information (SI) hébergé sur le *cloud*. Pour autant, cette complexité a un fort impact sur la lourdeur de la migration sortante.

Les configurations incluent les paramètres de déploiement, les règles de sécurité, les configurations réseau, les scripts d'automatisation, et d'autres éléments nécessaires au bon fonctionnement des applications dans l'environnement *cloud*. Les dépendances verticales, telles que les connecteurs, permettent aux applications de communiquer avec d'autres services ou bases de données, tandis que les dépendances horizontales concernent les interactions entre différentes applications au sein du même environnement.

La prise en compte de ces configurations et dépendances est essentielle pour garantir une migration réussie et minimiser les interruptions de service. Lorsqu'un client décide de changer de fournisseur de services *cloud*, il doit non seulement migrer les applications elles-mêmes, mais aussi toutes les configurations et dépendances associées. Cette tâche peut s'avérer particulièrement complexe et nécessite une planification rigoureuse et une expertise technique approfondie.

La complexité des configurations et des dépendances a un fort impact sur la lourdeur de la migration sortante. Plus le système d'information est complexe, plus la migration sera difficile et coûteuse. Les clients doivent souvent recourir à des services professionnels pour gérer cette complexité et s'assurer que toutes les configurations et dépendances sont correctement migrées vers le nouvel environnement *cloud*.

En conclusion, la définition des actifs numériques pourrait être complétée en ajoutant aux applications les configurations et toutes les dépendances, verticales et horizontales. La complexité de ces configurations ne dépend pas du fournisseur de *cloud*, mais de la complexité du système d'information hébergé sur le *cloud*. Cette complexité a un fort impact sur la lourdeur de la migration sortante et doit être prise en compte pour garantir une migration réussie et minimiser les interruptions de service.

Question 26. 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 ?

Dans son article 29, la loi SREN mentionne l'importance de faciliter le changement de fournisseur et le recours simultané à plusieurs fournisseurs de services *cloud* (*multi-cloud*). Dans ce contexte, il est pertinent d'examiner le processus standard de migration d'une application sur un service IaaS.

Le processus de migration décrit dans la consultation publique de l'Arcep semble être conçu pour des clients qui ont modernisé leur infrastructure avec une approche Infrastructure as Code (IaC). Cette approche permet de gérer et de provisionner des ressources informatiques à l'aide de fichiers de configuration automatisables, ce qui facilite la migration des applications et des infrastructures.

Cependant, la situation des entreprises que nous rencontrons est souvent différente, notamment les clients en infogérance qui n'ont pas encore modernisé leurs infrastructures. Ces clients rencontrent plusieurs défis spécifiques :

1. Inventaire non fiable : Les clients en infogérance ont souvent des difficultés à maintenir un inventaire fiable de leurs actifs informatiques. Cela complique la planification et l'exécution des migrations, car il est difficile de savoir exactement quelles ressources doivent être migrées et comment elles sont interconnectées.
2. Systèmes obsolètes : Les systèmes d'exploitation (OS) et les middlewares utilisés par ces clients sont souvent obsolètes. Cela pose des défis supplémentaires en termes de compatibilité et de sécurité lors de la migration vers un nouvel environnement *cloud*.
3. Absence d'automatisation : Ces clients n'ont pas automatisé leur infrastructure, ce qui signifie que les processus de gestion et de déploiement des ressources sont manuels et sujets à des erreurs. L'absence d'automatisation rend la migration plus laborieuse et augmente le risque d'interruptions de service.

Pour ces raisons, la méthodologie de migration que nous utilisons commence par un audit approfondi de l'infrastructure client. Cet audit a pour objectif de déterminer des stratégies de migration par application ou par machine virtuelle (VM) et d'identifier les éléments qui ne peuvent pas être reconstruits dans le nouvel environnement *cloud*. L'audit permet de dresser un inventaire précis des ressources et de leurs dépendances, d'évaluer l'état des systèmes et de planifier les étapes de la migration de manière méthodique.

La majorité des cas clients que nous rencontrons ne permettent pas d'avoir une approche industrielle des migrations. Chaque migration doit être adaptée aux spécificités de l'infrastructure et des applications du client, ce qui nécessite une planification sur mesure et une expertise technique approfondie. Les migrations doivent être réalisées de manière progressive, en minimisant les interruptions de service et en assurant la continuité des opérations.

En conclusion, le processus standard de migration décrit dans la consultation publique de l'Arcep est applicable aux clients qui ont modernisé leur infrastructure avec une approche IaC. Cependant, la réalité des clients en infogérance que nous rencontrons chez Orange est différente.

Ces clients ont des infrastructures non modernisées, des systèmes obsolètes et des processus souvent manuels, ce qui rend la migration plus complexe. La méthodologie de migration doit commencer par un audit approfondi de l'infrastructure client et être adaptée aux spécificités de chaque cas client.

Question 27. 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 ?

Dans le contexte d'un changement de fournisseur ou du recours simultané à plusieurs fournisseurs de services *cloud*, il est important d'examiner les difficultés techniques rencontrées lors de la migration d'applications reposant exclusivement sur des services IaaS.

Notre expérience diffère des constats présentés dans la consultation publique. Une des difficultés majeures est que, pour les machines virtuelles (VM), il est possible d'exporter le contenu de la VM, mais pas l'ensemble des informations associées à la VM, telles que le dimensionnement ou certains paramètres de fonctionnement de la machine virtuelle. Même en se limitant au socle des fonctionnalités IaaS, il est incorrect de considérer qu'une application reconstruite « à l'identique » se comportera de façon identique, en particulier en termes de performance.

Les *hyperscaler* fournissent des outils permettant de migrer au niveau de la VM, souvent à froid. Cependant, les clients attendent une migration à chaud avec des délais d'interruption de service limités, ce qui conduit à des migrations application par application. Si le client a plusieurs centaines de VM, il attend un lotissement et une migration globale étalée sur plusieurs mois. Cela nécessite d'une part d'avoir cartographié les dépendances entre applications et d'utiliser des logiciels du commerce permettant l'équivalent d'un Plan de Reprise d'Activité (PRA).

Il n'est pas possible d'affirmer de généralités sur les *hyperscalers*, car les outils et la méthodologie de migration diffèrent entre eux. Cependant, on constate que les *hyperscalers* fournissent des outils pour faciliter la migration entrante, mais pas la migration sortante.

En conclusion, les difficultés techniques rencontrées lors de la migration d'applications reposant exclusivement sur des services IaaS sont significatives et varient en fonction des fournisseurs de services *cloud*. Les outils fournis par les *hyperscalers* facilitent principalement la migration entrante, tandis que la migration sortante reste complexe et nécessite une planification rigoureuse et une expertise technique approfondie.

Question 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 ?

Dans le contexte d'un changement de fournisseur ou du recours simultané à plusieurs fournisseurs de services *cloud*, il est aussi important d'examiner les freins techniques à la réalisation de l'équivalence fonctionnelle pour les services IaaS.

Si on raisonne au niveau d'une machine virtuelle (VM), les services de IaaS purs sont sensiblement équivalents entre les principaux *hyperscalers* tels qu'AWS, Azure et Google Cloud Platform. En revanche, les concepts sont différents avec ceux d'un IaaS VMware/Broadcom, et la migration ne pourra pas être automatisée. Les différences de concepts et d'architectures entre les fournisseurs de services *cloud* rendent la migration complexe et nécessitent souvent des ajustements manuels.

Lorsque le client dispose d'une infrastructure plus complexe, la modélisation au niveau du groupement des ressources et des services réseau (par exemple, les Load Balancers) est différente pour chaque *hyperscaler*. Ces différences font partie de l'identité de chaque *hyperscaler* et influencent le choix d'un fournisseur plutôt qu'un autre. Il paraît peu envisageable de résorber ces différences, et ce n'est pas forcément souhaitable non plus, car cette hétérogénéité permet à des clients ayant des besoins, contraintes ou préférences différentes de trouver la solution qui leur est particulièrement adaptée.

À titre d'exemple, l'offre Cloud Avenue d'Orange Business s'appuie sur vCloud Director. Elle repose sur des concepts de pools de ressources et de quotas partagés que l'on ne retrouve pas chez les

hyperscalers ou les *clouds* basés sur OpenStack. Cloud Avenue utilise également le service NSX qui introduit des notions de Edge Gateways, qui n'existent pas chez les *hyperscalers*.

Un autre exemple est la notion de Virtual Private Cloud (VPC), dont la portée est plus large sur Google Cloud Platform que sur AWS ou Azure. Les services de firewall et de load balancers sont également typiquement différents tant dans leurs fonctionnalités que dans leurs modèles de facturation. Cela peut nécessiter de revoir l'urbanisation de son système d'information (SI) en cas de migration.

En conclusion, bien que les services IaaS purs puissent sembler équivalents entre les principaux *hyperscalers* du marché, les différences de concepts et d'architectures entre les fournisseurs de services *cloud* créent des freins techniques à la réalisation de l'équivalence fonctionnelle.

Ces différences sont inhérentes à l'identité de chaque fournisseur et permettent aux clients de choisir des solutions adaptées à leurs besoins spécifiques.

Question 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 ?

Dans le contexte de l'article 29 de la loi SREN, qui souligne l'importance de faciliter le changement de fournisseur et le recours simultané à plusieurs fournisseurs de services *cloud*, la description du processus standard de migration d'une application construite à l'aide de services PaaS nécessite une analyse nuancée qui tienne compte de la grande diversité et de l'hétérogénéité des services concernés.

Cette analyse doit s'inscrire dans le cadre plus large du *Data Act* qui établit une distinction importante entre les services d'infrastructure (IaaS) et les autres services de traitement de données (PaaS et SaaS) en termes d'obligations. En effet, l'article 30 du *Data Act* opère une différenciation claire : alors que les services IaaS sont soumis à une obligation d'équivalence fonctionnelle, les services PaaS bénéficient d'obligations allégées, centrées sur la mise à disposition d'interfaces ouvertes et la compatibilité avec les spécifications communes ou les normes harmonisées d'interopérabilité.

En effet, contrairement aux services IaaS qui présentent un niveau relativement élevé de standardisation, les services PaaS se caractérisent par une variété considérable d'offres et de fonctionnalités. Cette diversification croissante à mesure que l'on monte dans les couches d'abstraction (IaaS/PaaS/SaaS) rend particulièrement complexe l'établissement d'un processus de migration standardisé.

Le paysage des services PaaS englobe aujourd'hui un spectre très large de solutions, allant des plateformes d'orchestration de conteneurs comme Kubernetes aux bases de données managées, en passant par les solutions serverless, les services de Big Data, les API Gateways ou encore les modules d'intelligence artificielle générative. Chacun de ces services présente des caractéristiques techniques spécifiques qui influencent directement les modalités de leur migration.

Cette diversité technique se traduit par des défis de migration particuliers pour chaque type de service.

Par exemple, la migration d'une application utilisant des services Kubernetes managés nécessite une attention particulière aux configurations des clusters et aux orchestrations de conteneurs, tandis que la migration de bases de données managées soulève des enjeux de compatibilité des schémas et de performance des requêtes.

Le cas des services *Serverless* illustre particulièrement bien cette complexité. La migration de fonctions Lambda d'AWS vers les Cloud Functions de Google Cloud, par exemple, implique souvent une réécriture significative du code pour s'adapter aux spécificités de l'environnement d'exécution du fournisseur de destination. Cette réalité technique est d'ailleurs prise en compte dans l'article 30(2) du *Data Act* qui, plutôt que d'imposer une équivalence fonctionnelle stricte, requiert la mise à disposition gratuite d'interfaces ouvertes pour faciliter la portabilité.

Les services de Big Data ajoutent une couche supplémentaire de complexité avec des enjeux spécifiques liés aux volumes de données à transférer et à la compatibilité des formats. De même, les API Gateways et les services d'IA générative présentent des défis particuliers en raison de leurs intégrations multiples et de leurs dépendances avec des modèles spécifiques.

En conclusion, il est important de s'aligner sur l'approche différenciée adoptée par le *Data Act* et de prendre en compte la diversité inhérente aux services PaaS. Plutôt que de chercher à établir un processus de migration standardisé, il s'agit de privilégier une approche flexible qui reconnaisse la spécificité de chaque type de service et permette l'adaptation des processus de migration en conséquence.

Question 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 ?

Dans ce contexte de l'article 29 de la loi SREN, nous partageons notre analyse des difficultés techniques de migration d'applications reposant sur des services PaaS.

Comme indiqué précédemment, il n'est pas possible de tirer de généralités sur le PaaS. Nous partageons le constat sur le PaaS Kubernetes, qui est assez standard avec un langage déclaratif standardisé. Cependant, pour les autres solutions PaaS, cela dépend du service et du niveau de performance attendu.

Pour un client avec une volumétrie limitée et sans exigence de performance, il est possible que la migration d'une base de données managée soit relativement simple. Cependant, pour un client utilisant une base de données relationnelle managée avec des contraintes de performance, même avec des services standards, il y aura un travail important d'adaptation nécessitant de revoir le design, de modifier du code et de faire des tests de performance. Même sur des solutions simples comme PostgreSQL, il peut y avoir des écarts de version ou de paramètres.

Pour des services plus complexes comme les bases de données NoSQL, même avec des solutions open source (par exemple, Apache Druid ou Clickhouse), la migration peut nécessiter plusieurs mois et un support de consultants dédiés de l'éditeur. Pour les bases de données spécifiques (par exemple, Aurora, CosmoDB), chaque solution a ses spécificités et il est nécessaire de retravailler le design et potentiellement le code applicatif, car les API/SDK ne sont pas les mêmes.

En conclusion, la majorité des services PaaS peuvent être considérés comme spécifiques car, au-delà de similitudes fonctionnelles, ils diffèrent trop souvent dans leurs interfaces, leurs comportements ou leurs limitations.

Il est à noter aussi une spécificité pour les services d'IA Générative où l'on entraîne un modèle de langage large (LLM) de l'*hyperscaler*. En effet, les données du client auront participé à l'entraînement

du modèle de l' *hyperscaler*. L' *hyperscaler* peut proposer au client d'exporter les données générées par l'IA Générative, mais il ne pourra proposer d'extraire la partie d'apprentissage que le client a apportée au LLM de l' *hyperscaler*.

Question 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 ?

Dans le contexte de cette consultation, il est pertinent d'examiner les services spécifiques des fournisseurs de services *cloud* et leurs impacts sur la migration des applications.

Plus que les spécificités d'un service ou d'un autre, l'impact sur la décision de migration du client est davantage lié à la criticité de l'application et à l'impact que ces différences de services auront sur l'application. La criticité de l'application détermine souvent la tolérance du client aux interruptions de service et aux modifications nécessaires pour adapter l'application à un nouvel environnement *cloud*. Les applications critiques nécessitent une planification minutieuse et des tests rigoureux pour garantir une migration réussie sans impact négatif sur les opérations.

L'usage de technologies propriétaires versus open-source ou inner-source au niveau applicatif limite également grandement les possibilités du client d'adapter son application à ces différences. Les technologies propriétaires peuvent offrir des fonctionnalités avancées et des optimisations spécifiques, mais elles peuvent également créer des dépendances fortes qui compliquent la migration vers d'autres fournisseurs. À l'inverse, les technologies open-source ou inner-source offrent une plus grande flexibilité et interopérabilité, mais peuvent nécessiter des efforts supplémentaires pour atteindre des niveaux de performance et de fonctionnalité comparables.

L'uniformisation des services *cloud* nous apparaît comme une mauvaise réponse à un problème de maîtrise du code côté applicatif chez le client. Plutôt que de chercher à uniformiser les services *cloud*, l'enjeu est de renforcer les compétences en matière de développement et de gestion d'applications ce qui ne relève pas du cadre de cette consultation. Cela inclut notamment la capacité à écrire du code portable et à utiliser des outils et des *frameworks* qui facilitent l'interopérabilité entre différents environnements *cloud*.

En conclusion, l'impact des services spécifiques des fournisseurs de services *cloud* sur la migration des applications est davantage lié à la criticité de l'application et à l'usage de technologies propriétaires versus open-source ou inner-source.

Question 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 ?

Nous partageons le constat de l'Arcep concernant les difficultés techniques de migration liées aux services auxiliaires. Pour le premier projet d'un client sur une infrastructure d'un *hyperscaler*, il faut non seulement réfléchir à la zone d'atterrissage (*landing zone*) qui permet de poser tout l'outillage client, mais comme le préconisent les « *cloud adoption frameworks* » des principaux fournisseurs de services *cloud*, il faut également repenser la gouvernance.

Cela inclut en particulier la gestion des identités et des droits, l'organisation des ressources et des projets, ainsi que les aspects FinOps (gestion financière des opérations *cloud*).

Les fournisseurs de services *cloud*, notamment les *hyperscalers*, ont développé des fonctionnalités spécifiques et innovantes qui répondent aux besoins de leurs clients et constituent des éléments différenciants de leurs offres. Cette différenciation, qui reflète la dynamique d'innovation du marché, peut néanmoins complexifier les projets de migration, notamment dans des domaines comme la gestion des identités et des accès où chacun a développé ses propres concepts et mécanismes. Par exemple, les systèmes de gestion d'annuaire, de droits et de fédération d'identité présentent des spécificités propres à chaque fournisseur, ce qui nécessite une adaptation technique lors d'une migration.

A minima, il faut prévoir un travail spécifique autour de l'Identity and Access Management (IAM) et du *Single Sign-On* (SSO) pour tout projet de migration. Ces éléments sont cruciaux pour assurer une gestion sécurisée et efficace des accès et des identités dans un environnement *multi-cloud*. Les différences dans la gestion des identités et des droits entre les *hyperscalers* nécessitent une adaptation spécifique pour chaque environnement.

Un changement de fournisseur de services *cloud* peut aussi être l'occasion de moderniser la modélisation de son système d'information (SI) plutôt qu'une migration automatique et « à l'identique ». Cette approche permet de tirer parti des avantages spécifiques de chaque fournisseur de services *cloud* et d'optimiser la gestion des ressources et des services.

Question 33. 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 ?

Il existe des difficultés pour la récupération des données liées à l'utilisation d'un service SaaS. Toutefois, l'hétérogénéité des services SaaS étant très forte, il semble difficile de dégager des généralités. Chaque service SaaS a ses propres spécificités en termes de formats de données, d'API, de protocoles de sécurité et de mécanismes d'exportation des données. Cette diversité rend la récupération des données complexe et nécessite souvent des approches sur mesure.

Les principales difficultés rencontrées incluent :

1. Formats de données propriétaires : De nombreux services SaaS utilisent des formats de données propriétaires qui ne sont pas facilement exportables ou compatibles avec d'autres systèmes. Cela peut nécessiter des conversions de format et des adaptations spécifiques pour intégrer les données dans un nouvel environnement.
2. API limitées ou complexes : Les API fournies par les services SaaS pour l'exportation des données peuvent être limitées en termes de fonctionnalités ou complexes à utiliser. Les utilisateurs doivent souvent naviguer dans une documentation technique détaillée et comprendre comment utiliser les API pour extraire les données de manière efficace.
3. Problèmes de performance : L'exportation de grandes quantités de données depuis un service SaaS peut poser des problèmes de performance, notamment en termes de temps de transfert et de charge sur les systèmes. Les utilisateurs doivent planifier ces opérations pour minimiser les interruptions de service et garantir l'intégrité des données.
4. Sécurité et conformité : La récupération des données doit se faire en respectant les protocoles de sécurité et les exigences de conformité réglementaire. Cela inclut la gestion des accès, le chiffrement des données en transit et au repos, et la conformité aux réglementations telles que le RGPD.
5. Dépendances et intégrations : Les services SaaS sont souvent intégrés à d'autres systèmes et applications au sein de l'entreprise. La récupération des données doit prendre en compte ces dépendances et garantir que les intégrations restent fonctionnelles après la migration.

Dans ce contexte, Orange s'engage pleinement dans la mise en œuvre des dispositions de la loi SREN et du *Data Act* visant à faciliter la portabilité des données des services SaaS. Cette mise en œuvre doit être différenciée selon deux cas de figure distincts.

- Pour les services SaaS développés et opérés directement par Orange, nous œuvrons activement à développer des interfaces standardisées et des procédures harmonisées pour l'export des données, conformément aux exigences réglementaires. Cette approche, basée sur des API documentées et des formats d'échange normalisés, permettra de faciliter la portabilité des données tout en garantissant leur intégrité et leur utilisabilité.
- Pour les services SaaS commercialisés par Orange en tant que revendeur, notamment ceux des grands éditeurs de logiciels, nous nous engageons à accompagner nos clients dans l'utilisation des mécanismes d'export et de portabilité mis en place par les éditeurs concernés.

Cette double approche reflète notre engagement à contribuer à l'objectif d'interopérabilité et de fluidité du marché porté par la réglementation européenne, tout en tenant compte des spécificités de notre positionnement sur le marché des services *cloud*.

Question 34. Identifiez-vous des difficultés pour la récupération des données liées à l'utilisation d'un service SaaS ? Si oui, dans quel contexte ?

Dans le contexte de l'article 28 de la loi SREN et du *Data Act*, il est essentiel de distinguer deux situations différentes concernant l'exportation des données des services SaaS, selon le positionnement d'Orange sur le marché.

Pour les services SaaS développés et édités par Orange, nous nous engageons à mettre en œuvre l'ensemble des exigences réglementaires relatives à l'exportation des données. Conformément aux

dispositions qui seront définies au niveau européen d'ici septembre 2025, nous développons des solutions d'export basées sur des formats standardisés etinteropérables, excluant l'utilisation de formats propriétaires. Cette approche vise à faciliter la portabilité des données et à minimiser les efforts de transformation lors des migrations.

Pour les services SaaS que nous commercialisons en tant que revendeur, les modalités d'export des données sont définies et mises en œuvre par les éditeurs de ces solutions. Dans ce cas, notre rôle consiste à :

- Informer clairement nos clients des conditions et modalités d'export proposées par l'éditeur
- Accompagner nos clients dans l'utilisation des fonctionnalités d'export mises à disposition
- Faciliter le dialogue avec l'éditeur pour les aspects techniques de l'export

Dans tous les cas, la documentation exhaustive des formats et schémas de données constitue un élément essentiel pour garantir une migration réussie. Cette documentation doit permettre aux clients de comprendre précisément la structure des données exportées et les éventuelles transformations nécessaires pour leur réutilisation.

En conclusion, Orange s'engage à respecter pleinement les exigences de la loi SREN et du *Data Act* en matière d'exportation des données pour ses propres services SaaS, en anticipant notamment l'adoption des normes d'interopérabilité européennes. Pour les services SaaS que nous revendons, nous assurons la transparence sur les conditions d'export et accompagnons nos clients dans leur mise en œuvre.

Question 35. 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 ?

La détermination du périmètre des données exportables constitue effectivement un enjeu particulièrement sensible et complexe pour les services SaaS, qui se distingue nettement des problématiques rencontrées pour les autres types de services *cloud*.

Cette spécificité s'explique d'abord par la nature même des services SaaS, où les données sont fortement intégrées dans l'application et son fonctionnement. En effet, contrairement aux services IaaS ou PaaS où l'utilisateur conserve un contrôle direct sur ses données et où la séparation entre données utilisateur et infrastructure est plus nette, les services SaaS présentent une imbrication étroite entre les données, les fonctionnalités applicatives et les processus métier.

La loi SREN, dans son article 28, définit les données exportables comme "*les données d'entrée et de sortie, y compris les métadonnées, générées directement ou indirectement ou co-générées par le client par l'utilisation du service d'informatique en nuage*". Cette définition, bien que précise dans son énoncé, soulève des questions d'interprétation particulières dans le contexte SaaS, notamment concernant :

- La qualification des données co-générées lors de l'utilisation du service, qui peuvent résulter à la fois des actions de l'utilisateur et des traitements propres au logiciel
- Le périmètre des métadonnées exportables, particulièrement crucial dans le SaaS où elles incluent souvent des paramètres de configuration métier essentiels au fonctionnement du service

- La délimitation entre les données relevant de la propriété intellectuelle du fournisseur (exclues du périmètre par la loi) et celles appartenant à l'utilisateur

Cette différence significative entre SaaS et autres services *cloud* s'explique également par le niveau d'abstraction plus élevé des services SaaS, où l'utilisateur interagit uniquement avec l'interface applicative sans accès aux couches techniques sous-jacentes. Cette caractéristique rend plus complexe l'identification et l'extraction des données qui lui appartiennent.

Question 36. Comment définissez-vous, dans le cadre des contrats liants un clients à un fournisseur de services *cloud*, le périmètre des données exportables ?

La définition du périmètre des données exportables constitue un élément essentiel dans la mise en œuvre des dispositions de la loi SREN et du *Data Act*. Cette définition doit concilier les droits des utilisateurs à la portabilité de leurs données avec la protection légitime des droits de propriété intellectuelle et des secrets d'affaires des fournisseurs.

L'article 28 de la loi SREN définit les données exportables comme "les données d'entrée et de sortie, y compris les métadonnées, générées directement ou indirectement ou bien cogénérées par le client par l'utilisation du service d'informatique en nuage, à l'exclusion de tout actif ou des données du fournisseur de services d'informatique en nuage ou d'un tiers, lorsque cet actif ou ces données sont protégés au titre de la propriété intellectuelle ou du secret des affaires".

Dans ce contexte réglementaire en évolution, Orange travaille à l'adaptation de ses contrats pour intégrer progressivement ces nouvelles exigences. Cette adaptation devra tenir compte des normes d'interopérabilité qui seront définies au niveau européen, notamment concernant les formats d'export des données. En effet, ces standards, qui ne sont pas encore établis, joueront un rôle déterminant dans la définition précise des modalités techniques d'export.

La mise en œuvre de ces dispositions nécessitera une clarification du périmètre des données concernées, en distinguant :

- les données appartenant au client
- les données générées par l'utilisation des services
- les éléments exclus d'office par la réglementation car protégés par des droits de propriété intellectuelle ou le secret des affaires

Conformément au considérant 15 du *Data Act* qui précise que "les données représentent la numérisation des actions de l'utilisateur et des événements", une attention particulière devra être portée à la définition des données générées par l'utilisation du service, qu'elles soient enregistrées intentionnellement ou résultent indirectement de l'action de l'utilisateur.

En conclusion, Orange s'engage à adapter ses dispositions contractuelles pour répondre aux exigences de la loi SREN et du *Data Act*, en tenant compte des futures normes d'interopérabilité européennes. Cette adaptation progressive visera à établir un cadre clair et équilibré, garantissant à la fois la portabilité effective des données des clients et la protection légitime des droits de propriété intellectuelle et des secrets d'affaires.

Question 37. 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 ?

La définition du périmètre des données exportables pour les services SaaS soulève des difficultés pratiques significatives qui méritent une analyse approfondie au regard de l'article 28 de la loi SREN.

En effet, bien que la loi SREN définisse les données exportables comme "*les données d'entrée et de sortie, y compris les métadonnées, générées directement ou indirectement ou cogénérées par le client*", l'application pratique de cette définition aux services SaaS soulève des questions d'interprétation complexes. Cette complexité découle de la nature même des services SaaS, qui présentent une très grande diversité de fonctionnalités et de modèles d'utilisation.

Un défi majeur réside dans la détermination de la pertinence des données à exporter. En effet, de nombreux services SaaS sont conçus pour être utilisés de manière standardisée, avec des niveaux de personnalisation volontairement limités pour garantir la cohérence et la performance du service. Dans ce contexte, les paramètres de configuration, bien qu'ils constituent techniquement des données générées par l'utilisation du service, sont souvent intrinsèquement liés à l'architecture spécifique du SaaS concerné.

Cette réalité technique pose un défi particulier au regard du considérant 92 du *Data Act* qui évoque la nécessité de "*faciliter le processus de réalisation de l'équivalence fonctionnelle*". En effet, les paramètres et configurations qui sont pertinents et fonctionnels dans un service SaaS peuvent s'avérer inutilisables ou dénués de sens dans un autre service, même si celui-ci propose des fonctionnalités similaires. La simple exportation de ces données ne garantit donc pas leur utilisabilité effective dans un autre environnement.

Les difficultés rencontrées par les clients et les fournisseurs pour définir le périmètre des données exportables sont donc multiples :

- la détermination de la pertinence réelle des données dans un contexte de migration
- l'identification des données qui conservent leur sens hors du contexte spécifique du SaaS d'origine
- la distinction entre les paramètres spécifiques à l'architecture du SaaS et les données métier réutilisables

En conclusion, la définition du périmètre des données exportables pour les services SaaS nécessite une approche approfondie qui prenne en compte non seulement la possibilité technique d'exporter les données, mais aussi leur pertinence et leur utilisabilité effective dans un autre contexte.

Question 38. Identifiez-vous d'autres difficultés techniques en cas de changement de fournisseur, que vous souhaitez porter à la connaissance de l'Arcep ?

Dans le cadre de l'analyse des difficultés techniques liées au changement de fournisseur de services *cloud*, il est essentiel de souligner que l'approche unitaire par niveau (IaaS vers IaaS, PaaS vers PaaS, SaaS vers SaaS) adoptée dans la consultation ne reflète pas pleinement la complexité des architectures *cloud* modernes et qu'il s'agit de prendre en compte une réalité plus complexe, particulièrement dans le contexte des applications *Cloud Native*. Ces applications se caractérisent par une utilisation combinée de multiples services à différents niveaux, créant des interdépendances significatives qui complexifient considérablement les processus de migration.

Une difficulté technique majeure, non abordée dans l'approche unitaire, réside dans l'interconnexion des différents services. Un client adoptant une approche *Cloud Native* construit généralement ses applications en combinant des services IaaS basiques avec des services PaaS et SaaS, le tout étant relié par des services techniques servant de "colle" applicative. Cette architecture complexe soulève des défis particuliers lors d'un changement de fournisseur, notamment lorsque des différences dans les interactions entre les services IaaS basiques avec les autres services.

Par ailleurs, une transformation technique majeure est en cours avec la containerisation des applications, c'est-à-dire le passage des machines virtuelles (VM) aux containers. Cette évolution, qui touchera une grande partie des applications dans les années à venir, représente un changement structurant tant sur le plan technique qu'organisationnel. Cette transition ajoute une complexité supplémentaire aux processus de migration, car elle modifie fondamentalement l'architecture des applications et leur mode de déploiement rendant nécessaire leur réécriture complète.

La diversité des cas d'usage et des configurations techniques rencontrés dans ce contexte rend particulièrement difficile l'établissement de règles générales pour les migrations et doit être prise en compte, notamment en ce qui concerne :

- les interdépendances entre services de différents niveaux
- l'impact de la containerisation sur les processus de migration

En conclusion, les difficultés techniques liées au changement de fournisseur de services *cloud* ne peuvent être pleinement appréhendées à travers une approche unitaire par niveau. La réalité des architectures *Cloud Native*, combinée à l'évolution vers la containerisation, nécessite une approche plus globale qui prenne en compte l'interconnexion complexe des services à différents niveaux.

Question 39. Que pensez-vous de la description présentée par l'Autorité des différents modèles d'architectures multi-*cloud* et des besoins d'interopérabilité correspondants ?

L'examen des différents modèles d'architectures multi-*cloud* et les besoins d'interopérabilité correspondants montre que les systèmes d'information font par nature appel à des ressources informatiques multiples devant être interconnectées entre elles. Cette architecture et ses contraintes (latence, coûts d'interconnexion) ne sont pas spécifiquement liées au développement du *cloud*, mais sont inhérentes à la complexité des systèmes d'information modernes. Les entreprises doivent souvent gérer des environnements hybrides et multi-*cloud* pour répondre à leurs besoins spécifiques en termes de performance, de résilience et de conformité.

Au niveau d'Orange Business, nous avons constaté que les plateformes de déploiement multi-*cloud* telles qu'Azure Arc n'ont pas rencontré un succès commercial significatif. Ces plateformes sont par

nature propriétaires et offrent un niveau de service dégradé par rapport aux fonctionnalités accessibles directement via la console du fournisseur de *cloud*. Les clients préfèrent souvent utiliser les outils et les interfaces natives des fournisseurs de *cloud* pour bénéficier de toutes les fonctionnalités et de la performance optimale.

Les besoins d'interopérabilité dans un environnement multi-*cloud* sont variés et dépendent des cas d'usage spécifiques des clients.

Les principaux besoins incluent :

1. Interopérabilité des réseaux : Les entreprises doivent pouvoir interconnecter leurs réseaux privés avec les réseaux des différents fournisseurs de *cloud*. Cela inclut la gestion des adresses IP, des VPN, des pare-feux et des Load Balancers. Les différences dans la gestion des réseaux entre les fournisseurs peuvent compliquer cette interopérabilité.
2. Portabilité des données : Les entreprises doivent pouvoir transférer et synchroniser des données entre différents environnements *cloud*. Cela inclut la gestion des bases de données, des systèmes de fichiers et des services de stockage d'objets. Les différences dans les formats de données et les API peuvent poser des défis supplémentaires.
3. Interopérabilité des applications : Les entreprises doivent pouvoir déployer et gérer des applications sur plusieurs environnements *cloud*. Cela inclut la gestion des conteneurs, des micro services et des environnements de développement. Les différences dans les outils de gestion des applications et les orchestrateurs de conteneurs peuvent compliquer cette interopérabilité.
4. Interopérabilité des services de sécurité : Les entreprises doivent pouvoir appliquer des politiques de sécurité cohérentes sur plusieurs environnements *cloud*. Cela inclut la gestion des identités et des accès, la surveillance des menaces et la conformité réglementaire. Les différences dans les services de sécurité et les modèles de facturation peuvent poser des défis supplémentaires.
5. Interopérabilité des services d'observabilité : lorsque les composants d'une application métier sont distribués sur plusieurs *cloud*, l'incidentologie et la détection préventive des anomalies peuvent être rendues particulièrement ardues en raison de l'hétérogénéité des métriques, de l'absence de centralisation des alertes et des journaux ou de la difficulté à définir des indicateurs composites (*ie* basés sur des métriques « multicloud »),

En conclusion, les différents modèles d'architectures multi-*cloud* présentent des besoins d'interopérabilité variés et complexes. Les plateformes de déploiement multi-*cloud* propriétaires, telles qu'Azure Arc, n'ont pas rencontré un succès commercial significatif en raison de leur nature propriétaire et de leur niveau de service dégradé par rapport aux fonctionnalités accessibles directement via la console des autres fournisseurs de *cloud*.

Question 40. 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 ?

L'analyse des cas d'usage présents et futurs d'une architecture "*multi-cloud* intégré" nécessite de prendre en compte à la fois des opportunités offertes par cette architecture et des défis réels qu'elle présente.

Dans le contexte de l'article 28 de la loi SREN, qui impose des obligations d'interopérabilité et de portabilité, les architectures *multi-cloud* peuvent effectivement permettre aux entreprises de tirer parti des services spécifiques de différents fournisseurs.

Par exemple, une organisation peut choisir de déployer ses données sur un *cloud* particulier pour bénéficier de services spécialisés tout en maintenant d'autres composants applicatifs sur un autre *cloud*.

Cependant, plusieurs freins significatifs limitent aujourd'hui l'adoption généralisée des architectures *multi-cloud* intégrées :

- Premièrement, la complexité technique constitue un défi majeur. L'intégration entre différents environnements *cloud* soulève des questions de performance, particulièrement en ce qui concerne les communications inter-*cloud*. Cette problématique est d'autant plus critique que les applications modernes nécessitent souvent des échanges de données fréquents et volumineux entre leurs différents composants.
- Deuxièmement, conformément au considérant 92 du *Data Act* qui souligne l'importance "*des capacités, des informations, une documentation, une assistance technique adéquates*", la gestion d'une architecture *multi-cloud* nécessite une multiplication des compétences techniques. En effet, les équipes doivent maîtriser les spécificités de chaque plateforme de services *cloud*, ce qui représente un investissement considérable en formation et en ressources humaines.
- Troisièmement, bien que les fournisseurs développent des fonctionnalités innovantes, leur utilisation optimale nécessite souvent une intégration poussée au sein d'un même environnement *cloud*. Les performances et la facilité d'intégration sont généralement optimisées lorsqu'un même périmètre applicatif est porté par un seul et même *cloud*.

Le coût total de possession d'une architecture *multi-cloud*, incluant les aspects techniques, humains et organisationnels, peut s'avérer significativement plus élevé qu'une approche *mono-cloud*.

Néanmoins, certains cas d'usage spécifiques peuvent justifier une approche *multi-cloud*, notamment :

- l'exploitation de services spécialisés uniquement disponibles chez certains fournisseurs
- les exigences de conformité réglementaire ou de souveraineté des données
- la recherche de résilience accrue pour des applications critiques

En conclusion, si le *multi-cloud* intégré peut présenter des avantages dans certains cas d'usage spécifiques, sa mise en œuvre soulève des défis significatifs en termes de complexité technique, de compétences requises et de coûts.

Question 41. 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 que l'interopérabilité des services *cloud* doit passer par des API. Ces API sont d'ailleurs en plein développement et constituent le moteur de l'« *infrastructure as code* ». Les API permettent aux utilisateurs de gérer et de provisionner des ressources *cloud* de manière automatisée, en utilisant des fichiers de configuration et des scripts.

Pour assurer une interopérabilité efficace entre services *cloud*, il est important que les API soient bien documentées et accessibles. Lorsque l'on souhaite intégrer une infrastructure *cloud* dans une console externe, il est important d'avoir une liste exhaustive des API et qu'elles soient en libre accès par Internet. Cela permet aux utilisateurs de découvrir et d'utiliser les API nécessaires pour gérer leurs ressources *cloud*.

Toutefois, une seule interconnexion requiert souvent plusieurs API, et il est difficile pour un utilisateur de savoir comment utiliser et agencer ces API entre elles. Pour remédier à cette complexité, il est essentiel que la documentation des API inclue des informations détaillées sur leur utilisation et leur agencement, qui sont détaillés dans notre réponse à la question 42.

En conclusion, pour assurer une interopérabilité efficace entre services *cloud*, les API doivent être bien documentées et accessibles et les bonnes pratiques de documentation promues pour faciliter l'utilisation des API et l'interopérabilité entre services *cloud*. Cela permettra aux utilisateurs de gérer et de provisionner leurs ressources *cloud* de manière automatisée et efficace, en utilisant des fichiers de configuration et des scripts.

Question 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 ?

Dans le cadre de l'article 28 de la loi SREN, qui impose la mise à disposition d'interfaces de programmation d'applications pour garantir l'interopérabilité des services *cloud*, la documentation des API constitue un élément important pour garantir une interopérabilité effective entre services *cloud* et doit être exhaustive et accessible.

En effet, l'interopérabilité des services *cloud* repose sur des API bien documentées qui constituent le moteur de l'"infrastructure as code". Cette approche permet aux utilisateurs de gérer et de provisionner leurs ressources *cloud* de manière automatisée, via des fichiers de configuration et des scripts.

La liste des API doit être complète et celles-ci doivent être accessibles librement via Internet, permettant aux utilisateurs d'explorer et d'utiliser les API nécessaires à la gestion de leurs ressources *cloud*.

Conformément au considérant 92 du *Data Act* qui souligne l'importance d'une "*documentation et assistance technique adéquates*", la documentation doit inclure :

- une description détaillée des fonctionnalités et cas d'usage
- des exemples concrets d'utilisation
- des guides de démarrage rapide
- des schémas d'architecture d'interconnexion
- des références techniques complètes
- des tutoriels et cas pratiques

La fourniture de la documentation n'est pas une condition suffisante dans la mesure où les API peuvent évoluer régulièrement :

- Premièrement, les évolutions des API doivent faire l'objet d'une notification claire et anticipée aux utilisateurs. Cette exigence de transparence est fondamentale pour permettre aux entreprises de planifier et d'adapter leurs développements. Ces évolutions doivent être documentées de manière exhaustive, précisant la nature des changements, leur impact sur les fonctionnalités existantes, les modifications nécessaires côté utilisateur et le calendrier de mise en œuvre.
- Deuxièmement, une période de rétrocompatibilité suffisante doit être garantie pour permettre aux utilisateurs d'adapter leur code aux nouvelles versions des API. Cette période doit tenir

compte des contraintes opérationnelles des entreprises, notamment leurs cycles de développement et de déploiement. Cette exigence est particulièrement importante dans le contexte du multi-*cloud* où les entreprises doivent gérer des intégrations complexes avec plusieurs fournisseurs.

La complexité des interconnexions, qui nécessitent souvent l'utilisation combinée de plusieurs API, renforce l'importance de ces garanties de stabilité. Les mises à jour doivent être gérées de manière à ne pas perturber les intégrations existantes tout en permettant l'évolution des services.

En conclusion, nous recommandons que les lignes directrices de l'ARCEP établissent un cadre clair concernant :

- le contenu minimal de la documentation des API
- les modalités de notification des évolutions
- les durées minimales de rétrocompatibilité
- les conditions de mise à jour des API

Cette approche permettrait de faciliter l'interopérabilité effective des services *cloud* tout en préservant la stabilité nécessaire aux développements des entreprises utilisatrices, conformément aux objectifs de la loi SREN et du *Data Act*.

Question 43. Identifiez-vous d'autres modèles d'interopérabilité entre systèmes informatiques que les API ? Le cas échéant, lesquels ?

Il existe d'autres modèles d'interopérabilité alternatifs aux API, principalement deux approches : les consoles multi-*cloud* et les initiatives de fédération de services spécialisés.

Les consoles multi-*cloud*, telles qu'Azure Arc, constituent une première approche d'interopérabilité. Ces solutions visent à offrir une interface unifiée pour la gestion et la supervision des ressources déployées sur différents fournisseurs *cloud*. Cependant, conformément au considérant 92 du *Data Act* qui souligne l'importance d'une "*assistance technique adéquate*", ces solutions présentent des limitations significatives. Leur nature propriétaire et leur complexité d'intégration peuvent restreindre leur efficacité opérationnelle et créer de nouvelles formes de dépendance vis-à-vis des fournisseurs.

Par ailleurs, des initiatives plus ciblées de fédération de services émergent pour répondre à des besoins d'interopérabilité spécifiques. Par exemple, des projets comme Liko pour Kubernetes ou Spire pour la gestion d'identité décentralisée proposent des solutions d'interopérabilité focalisées sur des services particuliers. Ces initiatives, bien que plus marginales, présentent l'avantage de cibler précisément certains types de services plutôt que de tenter de couvrir l'ensemble du spectre IaaS/PaaS/SaaS.

En effet, en se concentrant sur des services spécifiques, ces solutions peuvent mieux répondre aux exigences de sécurité et de performance propres à chaque type de service.

Cependant, ces alternatives aux API présentent certaines limitations :

- une couverture fonctionnelle souvent restreinte par rapport aux interfaces natives
- une complexité d'intégration qui peut nécessiter des efforts significatifs
- des risques potentiels de dégradation des performances
- une possible création de nouvelles dépendances techniques

En conclusion, bien que ces modèles alternatifs d'interopérabilité puissent compléter l'approche par API dans certains cas d'usage spécifiques, ils ne constituent pas une solution universelle aux enjeux d'interopérabilité des services *cloud*.

Question 44. Identifiez d'autres enjeux et difficultés techniques relatifs au changement de fournisseur et au développement du *multi-cloud* ?

Dans le contexte de cette consultation, il est pertinent d'examiner les enjeux et difficultés techniques relatifs au changement de fournisseur et au développement du *multi-cloud*.

- sur le changement de fournisseur :

Comme mentionné précédemment, plus les services proposés au client sont personnalisés, plus il lui sera coûteux de migrer le service en question dans un autre environnement. Le changement de fournisseur est souvent assimilé au transfert de données au sens de fichiers à plat type S3, ce qui est restrictif. Cette vision compare ce changement à un changement de fournisseur *cloud* grand public (par exemple, de iCloud vers Google Cloud).

En effet, la plupart du temps, le changement de fournisseur est beaucoup plus complexe car l'extraction de données permettant une réutilisation est très compliquée pour différentes raisons :

1. Automatisation limitée : L'automatisation est difficile en raison de l'absence de formats universels. Cela nécessite des interventions manuelles complexes au niveau technique (utilisation de logiciels spécifiques pour migrer les données), mais aussi organisationnelles (connaissance approfondie des deux environnements, phase de migration proprement dite).
2. Exportation des traitements appliqués sur les données (en sus des données elles-mêmes) afin qu'ils puissent être eux aussi migrés
3. Ressources nécessaires : Les ressources nécessaires pour réaliser ces migrations sont de type Professional Services, c'est-à-dire des ressources qualifiées pour effectuer des évaluations (*assessment*), mener des projets de transition (*move to*) et gérer une période de double run. Ces ressources sont essentielles pour garantir une migration réussie et minimiser les interruptions de service.

- sur le développement du *multi-cloud* :

La recherche de l'interopérabilité engendre de l'instabilité. La complexité engendrée par le paramétrage de systèmes d'information croisés sur plusieurs plateformes fait que le modèle *multi-cloud* est peu attractif pour les clients. Le *multi-cloud* est souvent provoqué par du « *shadow-IT* » et provoque des problèmes de gouvernance.

Le modèle *multi-cloud* présente plusieurs défis :

1. Complexité technique : La gestion de plusieurs environnements *cloud* simultanément nécessite une coordination étroite et une compréhension approfondie des interactions entre les différentes plateformes. Cela inclut le paramétrage des systèmes d'information croisés, la gestion des dépendances entre les applications et la synchronisation des configurations.
2. Instabilité : La recherche de l'interopérabilité entre les différentes plateformes de services *cloud* peut engendrer de l'instabilité. Les différences de concepts et d'architectures entre les fournisseurs de *cloud* compliquent la gestion des ressources et des services.

3. Problèmes de gouvernance : Le *multi-cloud* est souvent provoqué par du « *shadow-IT* », c'est-à-dire l'utilisation non autorisée de services *cloud* par des départements ou des individus au sein de l'entreprise. Cela peut entraîner des problèmes de gouvernance, notamment en termes de sécurité, de conformité et de gestion des coûts.

En conclusion, les enjeux et difficultés techniques relatifs au changement de fournisseur et au développement du *multi-cloud* sont significatifs. Les lignes directrices de l'Arcep devraient prendre en compte ces défis et promouvoir des pratiques de migration et d'interopérabilité qui respectent la diversité des offres de services *cloud* tout en facilitant le changement de fournisseur et le recours simultané à plusieurs fournisseurs de services *cloud*. Pour les clients, il est essentiel de planifier soigneusement les migrations et de renforcer la gouvernance pour tirer parti des avantages du *multi-cloud* tout en minimisant les risques et les coûts associés.

Sur la transparence des offres de référence techniques et la normalisation

Question 45. 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 ?

L'article 28, II de la loi SREN mentionne l'importance de définir des exigences essentielles d'interopérabilité, de portabilité et de mise à disposition d'interfaces de programmation d'applications (API) pour faciliter le changement de fournisseur et le recours simultané à plusieurs fournisseurs de services *cloud* (*multi-cloud*). Dans ce contexte, il est pertinent d'examiner les codes de conduite et recommandations d'application volontaire qui pourraient être pertinents pour préciser les règles et modalités de mise en œuvre de ces exigences essentielles.

À notre connaissance, le code SWIPO (*Switching Cloud Providers and Porting Data*) est le plus adapté au contexte des services *cloud*. Le code SWIPO a été développé en application de l'article 6 du règlement établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne (« *Free flow of non-personal data* »). Il fournit un ensemble de préconisations destinées à faciliter la portabilité des données et le changement de fournisseur.

1. Portabilité des Données :

Le code SWIPO propose des recommandations spécifiques pour assurer la portabilité des données entre différents fournisseurs de services *cloud*. Il inclut des bonnes pratiques pour l'exportation et l'importation des données, la transformation des formats de données, et la gestion des métadonnées. Ces recommandations sont essentielles pour garantir que les utilisateurs peuvent récupérer et réutiliser leurs données sans perte de qualité ou de fonctionnalité.

2. Interopérabilité des Services :

Le code SWIPO met également l'accent sur l'interopérabilité des services *cloud*. Il propose des lignes directrices pour l'utilisation des API et des interfaces standardisées, facilitant ainsi l'intégration des services *cloud* dans des environnements *multi-cloud*. L'interopérabilité est cruciale pour permettre aux utilisateurs de combiner et d'intégrer des services de différents fournisseurs, maximisant ainsi la flexibilité et l'efficacité de leurs infrastructures *cloud*.

3. Transparence et Information :

Le code SWIPO encourage la transparence et l'information des utilisateurs. Il recommande que les fournisseurs de services *cloud* fournissent des informations claires et détaillées sur les conditions de portabilité des données, les API disponibles, et les processus de migration. Cette transparence est essentielle pour permettre aux utilisateurs de prendre des décisions éclairées et de planifier efficacement leurs migrations.

4. Engagement des Parties Prenantes :

Le code SWIPO a été développé avec la participation de multiples parties prenantes, y compris des fournisseurs de services *cloud*, des utilisateurs, et des chercheurs. Cette approche collaborative garantit que les recommandations sont équilibrées et prennent en compte les besoins et les contraintes de tous les acteurs du secteur.

Question 46. 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 ?

Dans le contexte de l'article 29 de la loi SREN qui impose une obligation d'équivalence fonctionnelle pour les services IaaS, il est important d'analyser les mesures actuellement mises en œuvre et d'identifier les axes d'amélioration potentiels.

Les services IaaS reposent sur des concepts technologiques relativement matures et bien établis, couvrant un périmètre fonctionnel délimité. Cette maturité contribue à une compréhension partagée des fonctionnalités fondamentales entre les différents acteurs du marché, facilitant théoriquement l'équivalence fonctionnelle requise par la réglementation.

Cependant, il convient de noter que des différences techniques significatives subsistent entre les technologies des différents fournisseurs. Bien que ces écarts puissent sembler mineurs d'un point de vue purement fonctionnel, ils peuvent avoir un impact substantiel sur l'utilisation effective des services par les clients.

Par exemple, certaines différences architecturales fondamentales existent entre les approches des différents fournisseurs de services *cloud* :

- la gestion des pools de ressources et des quotas partagés, n'est pas systématiquement proposés par l'ensemble des fournisseurs de services IaaS
- la structure des machines virtuelles caractéristique des approches technologiques des différents fournisseurs
- les mécanismes de gestion des ressources et d'optimisation des performances

Un point particulièrement critique, qui n'est pas explicitement couvert par les obligations actuelles d'équivalence fonctionnelle, concerne les performances. En effet, un même dimensionnement de ressources entre un *cloud* source et un *cloud* cible ne garantit pas nécessairement des performances équivalentes, ce qui a pour conséquence la nécessité de procéder à une validation approfondie du bon fonctionnement de ses applications après migration, alors même que les caractéristiques techniques semblent identiques.

Pour améliorer l'équivalence fonctionnelle, plusieurs mesures supplémentaires pourraient être envisagées :

- la standardisation des métriques de performance pour faciliter la comparaison entre fournisseurs
- l'établissement de méthodologies communes de validation des migrations
- la mise en place d'outils de test et de validation standardisés
- le développement de référentiels de bonnes pratiques pour la migration

En conclusion, bien que les services IaaS bénéficient d'une certaine maturité technologique facilitant l'équivalence fonctionnelle, des différences techniques significatives subsistent et doivent être prises en compte. Il s'agit aujourd'hui d'encourager le développement de standards et de méthodologies permettant une meilleure prévisibilité des performances post-migration, tout en reconnaissant la nécessité de validation spécifique par les clients.

Question 47. 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 ?

Dans le contexte de l'article 29 de la loi SREN qui prévoit la publication d'une offre de référence technique d'interopérabilité par les fournisseurs de services *cloud*, la définition des informations minimales requises nécessite une approche équilibrée qui tienne compte des réalités du marché et des standards existants.

L'établissement du contenu de ces offres de référence devrait idéalement s'appuyer sur des normes internationales établies par des organisations multi-acteurs, sur le modèle de l'IETF (*Internet Engineering Task Force*), intégrant non seulement les fournisseurs, mais aussi les utilisateurs et les chercheurs. Cette approche collaborative permettrait d'éviter que les standards des *hyperscalers* ne s'imposent par défaut, conformément à l'esprit du *Data Act* qui vise à promouvoir un marché plus ouvert et compétitif. Pour autant, cet effort de normalisation pourrait freiner l'innovation sur le marché.

Il est important de noter que pour certains services de base, considérés comme des commodités, des standards de fait existent déjà. Par exemple, le stockage objet est effectivement normé de facto, le service S3 d'AWS étant devenu un standard compatible avec les autres services *cloud* comme Blob (Microsoft), Google Storage, ou même des solutions d'éditeurs tiers comme Scalify et l'offre Cloud Avenue d'Orange Business.

Cependant, la situation est plus complexe pour les services à valeur ajoutée. Par exemple, dans le domaine des containers, les services *cloud* (Kubernetes, AKS, GKE, Tanzu de VMware) proposent des fonctionnalités enrichies qui dépassent le simple cadre d'un service standard.

En conclusion, l'offre de référence technique d'interopérabilité devrait :

- s'appuyer sur des standards internationaux reconnus
- inclure une représentation neutre de l'environnement *cloud*
- proposer des mécanismes de traduction vers les services natifs
- préserver la capacité d'innovation sur les services à valeur ajoutée

Cette approche permettrait de faciliter l'interopérabilité et la portabilité tout en préservant la dynamique d'innovation du marché, conformément aux objectifs de la loi SREN et du *Data Act*.

Question 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 ?

Au regard des complexités techniques et opérationnelles évoquées dans notre réponse à la question 47, une approche trop ambitieuse d'harmonisation complète des offres de référence risquerait de se heurter à des difficultés de mise en œuvre significatives, ce qui motive à adopter une approche progressive et pragmatique.

Dans un premier temps, l'objectif prioritaire devrait être que chaque fournisseur de services *cloud* explique clairement les modalités d'export des données vers d'autres environnements. Cette exigence fondamentale, qui s'inscrit dans l'esprit de l'article 28 de la loi SREN relatif à la portabilité des données, constituerait déjà une avancée significative pour les utilisateurs.

Cette approche plus ciblée permettrait de :

- répondre au besoin immédiat de transparence sur la portabilité des données
- faciliter la planification des migrations par les utilisateurs
- éviter les complexités inutiles dans la mise en œuvre

- maintenir une certaine flexibilité dans la présentation des offres

En conclusion, plus qu'une harmonisation complète de la forme des offres de référence, nous recommandons de concentrer les efforts sur la clarification des modalités d'export des données, qui sont essentielles pour la portabilité effective des services *cloud*.

Question 49. 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 ?

Dans le contexte de l'article 29 de la loi SREN et de la question de la normalisation supplémentaire des services IaaS, nous partageons l'analyse de l'Autorité quant au faible besoin d'harmonisation supplémentaire de ces services.

En effet, les services IaaS présentent aujourd'hui un niveau de similarité raisonnable entre les différents fournisseurs, résultat d'une maturation technologique et d'une standardisation de fait des pratiques du marché. Cette situation s'inscrit dans la logique du considérant 81 du *Data Act* qui reconnaît les services IaaS comme une catégorie distincte de services *cloud* avec des caractéristiques bien définies.

Toutefois, une tentative d'harmonisation plus poussée soulèverait des problématiques significatives. Les différences qui subsistent entre les services IaaS relèvent souvent de points très précis et spécifiques, intimement liés aux technologies sous-jacentes utilisées par chaque fournisseur. Vouloir harmoniser ces aspects reviendrait en réalité à imposer une standardisation des technologies elles-mêmes, plutôt que des services qu'elles permettent de fournir.

Une telle approche présenterait plusieurs risques majeurs :

- elle pourrait conduire à devoir imposer une technologie unique, ou à en écarter certaines, pour obtenir un comportement strictement identique entre les différents services
- elle risquerait de freiner l'innovation technologique dans le secteur
- elle pourrait créer des contraintes artificielles non justifiées par les besoins réels des utilisateurs

Cette analyse est cohérente avec le considérant 92 du *Data Act* qui met l'accent sur la facilitation du "*processus de réalisation de l'équivalence fonctionnelle*" plutôt que sur une standardisation technique complète.

En conclusion, nous estimons qu'une normalisation supplémentaire des services IaaS n'est pas nécessaire et pourrait même s'avérer contre-productive. L'accent devrait plutôt être mis sur le maintien et l'amélioration de l'interopérabilité fonctionnelle existante, conformément aux objectifs de la loi SREN et du *Data Act*.

Question 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 ?

Dans le contexte de l'article 28 de la loi SREN relatif aux exigences d'interopérabilité et de portabilité, l'analyse du besoin de normalisation des services PaaS nécessite une approche différenciée selon les types de services concernés :

- Pour certains services PaaS fondamentaux, une normalisation apparaît à la fois réalisable et bénéfique. Ces services présentent une hétérogénéité relativement limitée entre les différents fournisseurs, ce qui rend possible une harmonisation qui contribuerait significativement à la portabilité des applications. Cette approche s'inscrit dans l'esprit du considérant 92 du *Data Act* qui vise à "*faciliter le processus de réalisation de l'équivalence fonctionnelle*".
- De même, les services PaaS "simples", tels que les services de notification ou les files d'attente de messages (Message Queue), pourraient bénéficier d'une harmonisation basée sur l'adoption de formats standards. L'utilisation de spécifications comme CloudEvents, par exemple, renforcerait non seulement la portabilité des applications mais améliorerait également l'interopérabilité dans un contexte *multi-cloud*, conformément aux objectifs de la loi SREN.
- Cependant, la situation est plus complexe pour les services PaaS avancés, particulièrement les "*database services*". Ces services couvrent un large spectre de cas d'usage, au point qu'un même fournisseur propose souvent plusieurs variantes d'un même type de service pour répondre à différents besoins. Cette diversité, reconnue par le considérant 81 du *Data Act* qui évoque différents modèles de fourniture de services, rend une harmonisation globale peu pertinente.

En conclusion, nous recommandons une approche de normalisation à deux niveaux :

- une harmonisation ciblée pour les services PaaS fondamentaux et simples
- une approche plus souple pour les services PaaS avancés

Question 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 ?

Dans le contexte de l'article 28 de la loi SREN qui impose des exigences d'interopérabilité, la question de la normalisation des services auxiliaires, particulièrement les services IAM (*Identity and Access Management*) et d'observabilité, mérite une attention particulière.

Concernant les services IAM, notre expérience montre que leur hétérogénéité découle principalement des différences conceptuelles inhérentes aux architectures internes des plateformes *cloud*, plutôt que de divergences fonctionnelles fondamentales. Cette situation, qui complexifie inutilement l'intégration pour les utilisateurs, pourrait être significativement améliorée par des travaux de normalisation ciblés.

Une telle normalisation des services IAM présenterait un double avantage :

- d'une part, elle réduirait la complexité d'intégration pour les utilisateurs, que ce soit dans un contexte *mono-cloud* ou *multi-cloud*.
- d'autre part, et c'est peut-être le plus important, elle contribuerait à améliorer la sécurité globale des environnements clients en facilitant une mise en œuvre plus cohérente et mieux maîtrisée de la gestion des droits et des accès.

Par ailleurs, les services d'observabilité (monitoring, log, audit, alerting) constituent un autre domaine où des travaux de normalisation apparaissent particulièrement pertinents.

Une meilleure interopérabilité de ces services permettrait d'améliorer significativement :

- la sécurité des applications
- leur résilience opérationnelle
- la capacité à mettre en œuvre des pratiques avancées

En particulier, la normalisation faciliterait la corrélation des métriques et des journaux dans des environnements hybrides ou multi-*cloud*, une capacité très utile pour la détection et la résolution des incidents de sécurité, conformément aux exigences du considérant 92 du *Data Act* qui évoque la nécessité d'une "*assistance technique adéquate*".

Cette approche de normalisation des services auxiliaires devrait être considérée comme prioritaire car elle permettrait :

- de réduire la complexité technique pour les utilisateurs
- d'améliorer la sécurité globale des environnements
- de faciliter l'adoption de bonnes pratiques
- de renforcer la résilience des architectures *cloud*

En conclusion, nous soutenons l'initiative de travaux de normalisation sur les services auxiliaires, en commençant par les services IAM et d'observabilité. Cette normalisation contribuerait non seulement à faciliter l'interopérabilité technique, mais aussi à renforcer la sécurité et la résilience des environnements *cloud*, conformément aux objectifs de la loi SREN et du *Data Act*.

Question 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 ?

Dans le contexte de l'article 28 de la loi SREN et de la question de la normalisation des structures et formats d'échanges de données entre services SaaS du même type, nous considérons qu'une telle normalisation n'est ni souhaitable, ni pertinente.

Cette position s'appuie sur les considérations suivantes :

Tout d'abord, les services SaaS se caractérisent par leur forte différenciation fonctionnelle et leur capacité à répondre à des besoins métiers spécifiques. Cette différenciation, qui constitue le cœur de leur proposition de valeur, s'inscrit dans la logique du considérant 81 du *Data Act* qui reconnaît différents modèles de fourniture de services *cloud* portant des niveaux différents d'obligations.

Ensuite, la normalisation des structures et formats d'échanges de données entre services SaaS du même type présenterait plusieurs inconvénients majeurs :

- Premièrement, elle risquerait de freiner l'innovation en imposant des contraintes artificielles aux fournisseurs de services SaaS. En effet, la capacité à développer des fonctionnalités innovantes et différenciantes, qui peuvent nécessiter des structures de données spécifiques, est essentielle dans ce marché dynamique.
- Deuxièmement, conformément au considérant 92 du *Data Act* qui met l'accent sur la facilitation du "processus de réalisation de l'équivalence fonctionnelle", l'enjeu principal pour les services SaaS n'est pas tant la standardisation des formats que la capacité à exporter et réimporter les données de manière cohérente.

- Troisièmement, une normalisation forcée des structures de données pourrait conduire à un appauvrissement des fonctionnalités proposées, les fournisseurs devant se conformer à un plus petit dénominateur commun pour assurer la compatibilité.

En conclusion, plutôt qu'une normalisation des structures et formats d'échanges, nous recommandons de mettre l'accent sur la portabilité effective des données, en laissant aux fournisseurs la flexibilité nécessaire pour innover et différencier leurs services.

*

**

Question 53. Avez-vous d'autres commentaires sur les enjeux soulevés dans cette consultation publique ?

En complément des réponses précédentes, nous souhaitons mettre en avant certains enjeux supplémentaires qui n'ont pas été suffisamment abordés.

1. Non-encadrement des frais de connectivité :

Le *Data Act* introduit des mesures importantes pour encadrer les frais de transfert entre les *clouds*. Bien que les réponses précédentes aient abordé les coûts de transfert de données, il est crucial de souligner que les frais peuvent varier en fonction des types d'interconnexion et des stratégies d'investissement des fournisseurs d'une part et des architectures des clients d'autre part.

2. Intégration des retours d'expérience dans les recommandations concernant la portabilité des données et des applications :

La loi SREN et le *Data Act* mettent l'accent sur la portabilité des données et des applications. Cependant, la mise en œuvre de cette portabilité nécessite des efforts concertés pour développer des standards communs et des outils de migration efficaces. Il est essentiel de promouvoir des initiatives de normalisation au niveau international, impliquant des acteurs multiples (fournisseurs, utilisateurs, chercheurs) pour établir des normes interopérables et faciliter la portabilité des services *cloud*.

3. Innovation et Compétitivité :

Tout en régulant les services *cloud*, il est important de préserver l'innovation et la compétitivité du secteur. Les régulations ne doivent pas freiner l'innovation technologique, ni imposer des contraintes excessives aux fournisseurs de services *cloud*. Il est important de trouver un équilibre entre la régulation et la promotion de l'innovation, en soutenant les initiatives de recherche et développement et en encourageant la collaboration entre les acteurs du secteur.

En conclusion, les enjeux supplémentaires liés à l'encadrement des frais de connectivité, à la portabilité des données et des applications, à la sécurité et à la conformité, ainsi qu'à l'innovation et à la compétitivité, méritent une attention particulière dans le cadre de la régulation des services *cloud*. Les lignes directrices de l'Arcep devraient intégrer ces considérations pour promouvoir un écosystème *cloud* sécurisé, interopérable et innovant.

Question 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 ?

Au-delà des sujets abordés dans les sections précédentes de cette consultation, nous souhaitons attirer l'attention de l'Arcep sur d'autres enjeux relatifs à la régulation des services *cloud* :

1. Interopérabilité des services de sécurité :

L'interopérabilité des services de sécurité est un aspect clé pour garantir la protection des données dans un environnement *multi-cloud*. Les fournisseurs de services *cloud* doivent collaborer pour développer des standards communs et des API interopérables pour les services de sécurité, tels que l'Identity and Access Management (IAM) et le Single Sign-On (SSO). Cela permettra de renforcer la sécurité des données et de faciliter la gestion des identités et des accès dans un environnement *multi-cloud*.

2. Transparence des pratiques contractuelles :

La transparence des pratiques contractuelles est essentielle pour garantir une concurrence équitable et protéger les droits des utilisateurs. Les fournisseurs de services *cloud* doivent fournir des informations claires et compréhensibles sur les conditions contractuelles, les frais de transfert de données, les politiques de résiliation et les niveaux de service. Il est important de promouvoir des pratiques contractuelles transparentes et équitables pour renforcer la confiance des utilisateurs dans les services *cloud*.

3. Impact Environnemental :

L'impact environnemental des services *cloud* est un enjeu de plus en plus important. Les fournisseurs de services *cloud* doivent adopter des pratiques durables et réduire leur empreinte carbone. Le *Data Act* et la loi SREN doivent encourager les initiatives de durabilité, telles que l'utilisation d'énergies renouvelables, l'optimisation de l'efficacité énergétique des centres de données et la promotion de l'économie circulaire.

En conclusion, les enjeux relatifs à l'interopérabilité des services de sécurité, à la transparence des pratiques contractuelles et à l'impact environnemental méritent une attention particulière dans le cadre de la régulation des services *cloud*.

*** **

*** **