



Global
Strategy
Group

Le Cloud européen : de grands enjeux pour l'Europe et cinq scénarios avec des impacts majeurs d'ici 2027-2030

Avril 2021



Mettre le cloud européen au service de l'économie de la vie.

Mettre les données, virtuelles par essence, dans un stockage virtuel, était depuis longtemps une évidence prévisible, que la technologie a fini par imposer. Malheureusement, comme souvent, l'Europe a mis plus longtemps que beaucoup d'autres à le comprendre, laissant à Microsoft, Amazon et Google plus de 60% du marché du cloud public mondial.

Aujourd'hui, cette absence de l'Europe est très grave et il convient d'y remédier au plus vite.

D'abord, c'est un enjeu économique : D'ici à 2027, le marché du cloud en Europe pourrait atteindre plus de 260 milliards d'euros (contre 53 milliards d'euros aujourd'hui), ce qui le mettrait au même niveau que le marché actuel des télécommunications (environ 250 milliards d'euros en 2020). Et si les opérateurs de Cloud localisaient leurs opérations et leurs investissements en Europe, cela pourrait permettre en plus de créer environ 550 000 emplois entre 2021 et 2027 et déclencher des investissements significatifs (de l'ordre de 200 Md€ s sur la période 2021-2027). Cela serait aussi l'occasion de soutenir l'industrie des applications : le cloud n'est rien sans l'ensemble des services qui l'utilisent ; un cloud européen pourrait permettre de développer plus rapidement les entreprises européennes du logiciel, dans toutes les acceptions du mot. Cela permettrait aussi de développer dans un contexte sécurisé, les industries de la santé, de l'éducation, de la culture, des médias, de la sécurité, de l'assurance, de la finance ; tous secteurs fondamentaux dans la future économie de la vie. Cela devrait donc constituer un élément essentiel de la relance européenne.

C'est aussi un enjeu technologique : Investir dans le cloud permettrait à l'Europe de se positionner en tant que leader dans des technologies de pointe telles que les processeurs, la 5G, le cryptage quantique, le Edge computing... Et plus loin encore, le biomimétisme. Toutes technologies fondamentales dans les autres secteurs de l'économie de la vie : la logistique, la gestion de l'eau et de l'air, les énergies renouvelables.

C'est encore un enjeu stratégique : Un cloud européen permettrait à l'Europe de garantir sa souveraineté numérique en lui assurant la maîtrise de la gestion des données personnelles et industrielles, ce qui n'est absolument pas assuré dans le contexte juridique et réglementaire actuel (règlement RGPD, invalidation du Privacy Shield, Cloud Act).

Dans ce domaine comme dans beaucoup d'autres, le problème est mondial ; la solution est européenne ; le problème est politique et culturel ; la solution est industrielle.

Jacques Attali



Avertissement

Le présent rapport (« Rapport ») a été préparé par KPMG SA (« KPMG ») pour Talan SAS, InfraNum, OVHcloud et Linkt (Affiliée du groupe Altitude) (« Mandataires ») conformément au contrat signé avec eux en date du 15 janvier 2021 (« Contrat ») et sur la base du champ d'application et des limites précisées ci-dessous.

Le Rapport a été rédigé dans le seul objectif d'étudier la conjoncture et les défis du marché européen du cloud, tel que stipulé dans le Contrat. Il ne doit être utilisé à aucune autre fin et dans aucun autre contexte, faute de quoi KPMG, ses filiales et les autres entités appartenant au Réseau KPMG déclinent toute responsabilité envers toute personne se fondant sur le présent Rapport.

Le Rapport se destine à l'usage exclusif des Mandataires aux termes du Contrat. Aucune autre personne que les Mandataires n'est autorisée à utiliser le présent Rapport à quelque fin que ce soit. KPMG, ses filiales et les autres entités liées déclinent toutes responsabilités et obligations envers toute personne se fondant sur le présent Rapport ou son contenu, autre que les Mandataires.

Conformément aux termes du Contrat, le champ d'application de la présente étude a été limitée par le temps qui lui a été consacré et par les informations et explications fournies à KPMG. Les informations présentées dans le présent Rapport ont été obtenues par KPMG auprès des Mandataires et de sources tierces expressément mentionnées dans les différentes sections du Rapport. KPMG n'a pas cherché à corroborer ces informations ou à en valider la plausibilité. En outre, les résultats des analyses présentées dans le Rapport ont été obtenus sur la base des informations disponibles au moment où le Rapport a été préparé et ne peuvent être invoqués ultérieurement.

Tous droits d'auteur et autres droits de propriété rattachés au Rapport appartiennent à KPMG, sauf stipulation explicite contraire dans la présente communication ou dans le Contrat.

Toute décision d'investissement, d'exercice d'une activité professionnelle, d'entrée sur ou de sortie de l'un des marchés évoqués dans le Rapport doit uniquement être prise après avoir obtenu des conseils indépendants ; les tiers ne doivent en aucun cas se fonder sur les informations contenues dans le Rapport. KPMG ne fournit aucun service ni conseil commercial, financier, d'investissement ou autres par l'intermédiaire du Rapport. Le présent Rapport ne remplace pas de tels conseils ou services professionnels, et ne peut par conséquent constituer le fondement d'une décision ou action susceptible d'affecter vos activités. Avant de prendre une décision ou une action susceptible d'affecter vos activités, veuillez consulter un conseiller professionnel qualifié. En particulier, le Rapport ne vaut pas recommandation ou approbation de KPMG d'investir ou autrement de participer à, de quitter ou d'utiliser d'une quelconque manière les marchés ou entreprises mentionnés dans le Rapport. KPMG et les Mandataires, leurs filiales et les autres entités liées déclinent toute responsabilité découlant de l'utilisation (ou du défaut d'utilisation) du Rapport, y compris toutes actions ou décisions résultant de l'utilisation (ou du défaut d'utilisation) du Rapport.

Le présent Rapport a été rédigé en anglais et traduit en français et en allemand. En cas de contradiction entre les versions française, allemande et anglaise, la version anglaise prévaut.

Ce livre blanc a été construit à partir de données et ressources émanant d'une variété de sources, dont plus de 250 interactions avec des décideurs publics et privés européens

Entretiens avec des dirigeants d'entreprises françaises et allemandes

Plus de 50 entretiens conduits auprès de **dirigeants** français et allemands de grandes et moyennes entreprises (CAC 40, DAX, SBF 120...), **experts technologiques et juridiques**, afin de nourrir notre analyse de la conjoncture du marché et tester nos recommandations.

Études de marché et documents publics

Des **études de marché** détaillées émanant d'entreprises et **organisations partenaires**, spécialisées et concernées par les **défis et enjeux du cloud computing** ainsi que par les **questions relatives à la souveraineté des données des documents publics et juridiques**.

Échanges avec des experts du cloud computing

Échanges permanents avec des **experts du cloud computing**, y compris des experts internes (de KPMG et d'autres équipes contributrices), des économistes et des organismes publics pour **tester et ajuster nos recommandations** et leviers d'action.

Sondage web mené auprès de dirigeants européens

Un sondage web d'environ 40 questions, soumis à près de **200 dirigeants d'entreprises françaises et allemandes** (CA annuel moyen ≈ 150 M€), mesurant leur niveau de cloudification, **leur sensibilité aux enjeux de souveraineté lors du choix d'un prestataire cloud** et **leur perception de la souveraineté des données**.

La présente étude a été menée **sur une période de 8 semaines** entre janvier et mars 2021 par une équipe KPMG dédiée associant KPMG GSG (Strategy) et KPMG Avocats.

InfraNum, fédération française des infrastructures du numérique, a soutenu et activement contribué à ce rapport en sus de trois autres parties prenantes

Éléments clés sur la fédération InfraNum



- **Fondée en 2012** dans le but d'accompagner la mise en œuvre du plan national français pour le très haut débit
- Une fédération de **plus de 200** membres (entreprises très actives sur **les marchés des infrastructures numériques**, tels que les fournisseurs de fibre optique, les acteurs IOT, les acteurs des télécommunications et les fournisseurs d'équipements)
- **Principaux objectifs :**
 - Soutenir le **développement numérique français**
 - Promouvoir le développement **des usages numériques en France, en soutenant les entreprises dans la mise en œuvre d'une infrastructure numérique neutre, ouverte et partagée**
 - Développer des **partenariats entre acteurs publics et privés** pour permettre aux collectivités locales de développer les usages citoyens, de renforcer la **valeur de leur économie locale et de mettre l'accent sur les actifs propres à chaque région**

Éléments clés sur les autres contributeurs

En dehors d'InfraNum, trois autres contributeurs ont pris part à cette étude publiée par KPMG :



- **Talan**, cabinet de conseil européen spécialisé dans la transformation numérique



- **OVHcloud**, fournisseur cloud européen



- **Linkt**, opérateur français de télécommunications B2B

La participation active d'InfraNum et des contributeurs nous a permis de forger des **convictions fortes sur l'avenir du marché européen du cloud**, ses risques et ses défis.

Le Cloud européen : de grands enjeux pour l'Europe et cinq scénarios avec des impacts majeurs d'ici 2027-2030

Executive summary (1/3)

- 1 Le cloud européen est un marché de taille significative, déjà fortement attractif et avec un grand potentiel de croissance : de 53 Mds€ en 2020, le marché devrait atteindre 560 Mds€ d'ici à 2030¹, avec une croissance moyenne annuelle dépassant les 25%**
 - Les **services cloud**, qui englobent le cloud privé, public et hybride et les services de IaaS, PaaS et SaaS, **couvrent un large éventail des besoins IT des entreprises, et offrent des bénéfices indéniables** :
 - **Variabilisation de la structure de coûts**, avec un modèle de « paiement à l'usage », sans exigence d'investissements
 - **Flexibilité et évolutivité**, avec la possibilité d'augmenter ou de réduire instantanément les capacités de stockage / calcul pour répondre aux besoins des clients
 - **Capacité de se concentrer sur son cœur de métier**, en externalisant partiellement ou totalement les activités déploiement / maintenance vers les fournisseurs
 - Le **marché européen du cloud est en plein essor**, avec **de très forts enjeux de création de valeur pour l'économie européenne** :
 - Une taille de marché attendue à ~260 Mds€ d'ici à 2027, contre 53 Mds€ à ce jour, comparable au marché actuel des télécommunications (~250 Md€ en 2020)
 - Un paysage concurrentiel dominé par 3 « hyperscalers » basés aux Etats-Unis (avec par exemple 70% de la part de marché du IaaS), mais avec des opérations limitées en Europe
 - Les enjeux pour l'Europe sont d'environ 550 000 emplois et ~200 Mds d'investissements sur la période 2021-2027, dans la configuration où les opérateurs de Cloud localisent leurs opérations et leurs investissements en Europe
- 2 D'un point de vue juridique et réglementaire, le marché du cloud présente des risques élevés et une profonde incohérence entre les réglementations américaines et européennes, rendant la situation actuelle de marché non pérenne**
 - Depuis 2016, **plusieurs réglementations sur les données ont été mises en œuvre** aux États-Unis et dans l'Union Européenne (RGPD, US-EU Privacy Shield, Cloud Act), visant à **établir un cadre juridique strict concernant les flux de données ; mais l'invalidation du Privacy Shield** par la Cour de justice de l'UE en 2020 **a mis en évidence la profonde incompatibilité** de la réglementation américaine avec les principes du RGPD, qui semblent irréconciliables
 - En conséquence, **les entreprises transférant des données à caractère personnel des Européens sur des serveurs d'entreprises non-européennes (même si ces serveurs sont localisés en Europe) n'ont plus de fondement juridique** pour le faire, et s'exposent à **des risques juridiques, mais aussi industriels** compte tenu du fait que les fournisseurs de cloud internationaux ont accès à leurs données confidentielles et industrielles
 - Nos entretiens² montrent que cette **situation soulève des inquiétudes** et **conduit à des risques financiers et commerciaux**, par exemple :
 - Des licenciements pouvant être annulés car les preuves fournies par l'entreprise sont hébergées dans les data centers d'un prestataire cloud non-conforme
 - Une entreprise européenne pouvant être dans l'impossibilité d'utiliser les preuves pertinentes d'un vol de données de clients, car ces données sont extraites d'un système de contrôle d'accès stocké et traité aux États-Unis alors qu'un tel traitement est dépourvu de tout fondement légal

Le Cloud européen : de grands enjeux pour l'Europe et cinq scénarios avec des impacts majeurs d'ici 2027-2030

Executive summary (2/3)

3

- **La migration vers le cloud est un passage obligé mais très contraint pour les DSI, avec de multiples critères de choix, dont la sécurité et la souveraineté des données parmi les plus importants. La faible connaissance des offres garantissant la souveraineté ralentit la migration vers le cloud ou conduit les DSI à renoncer aux critères de souveraineté. Pourtant, les acteurs européens proposent les principaux services répondant aux besoins des entreprises et développent des écosystèmes complémentaires riches sur le SaaS et le PaaS, tout en affichant des modèles tarifaires et commerciaux plus transparents**
 - Le choix d'un fournisseur par un décideur cloud (les DSI notamment) est basé sur **plusieurs critères** ; parmi les plus importants, figurent la **sécurité et la souveraineté des données** ; cependant, malgré l'importance de ce critère, **le manque de connaissances sur les offres garantissant réellement cette souveraineté des données est un frein dans la migration vers le cloud ou conduit les DSI à renoncer à cette souveraineté des données**
 - **Pourtant, les acteurs européens offrent la plupart des services pour répondre aux besoins des entreprises et proposent une offre de plus en plus large de services SaaS et PaaS grâce à leurs écosystèmes**, permettant de couvrir une largeur et une profondeur de services progressivement comparable aux hyperscalers
 - **De plus, les modèles tarifaires des fournisseurs européens apparaissent plus transparents** que ceux des hyperscalers, qui **dominent à ce jour le marché avec des pratiques d'acquisition de clients souvent agressives et non conventionnelles** (par exemple, ventes liées des services SaaS et IaaS), mais aussi des **conditions de sortie complexes, qui rendent difficile pour les utilisateurs du cloud de quitter son fournisseur ou de passer d'un fournisseur à un autre**

4

L'actuel paradigme du marché européen du cloud ne semble pas pérenne sur le long terme et pourrait suivre cinq scénarios plausibles dans le futur

- **Quatre macro-tendances et de multiples tensions rendent le marché européen actuel du cloud non pérenne** dans sa forme actuelle :
 - L'incompatibilité entre les règles du RGPD et les règles extraterritoriales américaines, font porter des risques juridiques et commerciaux aux entreprises européennes recourant à des fournisseurs cloud américains
 - Les pratiques anticoncurrentielles et les fortes barrières commerciales à l'entrée qui ont été construites empêchent toute équité concurrentielle sur le marché européen
 - La demande croissante de protection des données personnelles et des données industrielles illustre la sensibilisation progressive du marché à la confidentialité et à la souveraineté des données
 - Les enjeux économiques visibles et massifs apparaissent du fait de la forte croissance de la demande de services cloud (surtout SaaS) en Europe
- **5 scénarios, chacun avec leurs propres avantages et échelles temporelles, pourraient conduire à un nouveau paradigme du marché en Europe :**
 - Le cloud comme bien commun, porté par l'interopérabilité volontariste entre services de cloud, des écosystèmes cloud sectoriels locaux et le développement du multi-cloud, permettant la mise en place d'un écosystème européen, stimulant la croissance des opérateurs européens et améliorant les bénéfices pour les clients (moins de lock-in, plus d'interopérabilité). Ce scénario pourrait se concrétiser à travers l'initiative Gaia-X qui vise à établir un écosystème cloud interopérable fondé sur des principes et des valeurs stricts
 - Montée en puissance des fournisseurs européens, notamment sous-tendue par les besoins des marchés émergents encore sous-adressés et non préemptés (notamment l'edge computing, l'Intelligence Artificielle pour les données industrielles et le développement d'offres souveraines) et par les dépenses publiques (projets B2G). Ce scénario pourrait se concrétiser avec le soutien des autorités de l'UE qui prônent la création d'un marché unique des données (IPCEI, Data Governance Act, EU cloud rulebook, etc....)

Le Cloud européen : de grands enjeux pour l'Europe et cinq scénarios avec des impacts majeurs d'ici 2027-2030

Executive summary (3/3)

- Vague réglementaire (similaire à celle observée sur le marché des télécoms il y a quelques années), avec la mise en place d'un régulateur du marché cloud imposant des contraintes aux prestataires cloud, notamment les hyperscalers, au moyen de leviers tels que la transparence tarifaire et commerciale, une vraie interopérabilité et un accès ouvert à l'innovation. Ce scénario est fortement soutenu par de nombreux décideurs qui s'attendent à une concurrence plus saine avec un changement progressif pour l'écosystème et les fournisseurs de cloud de l'UE
- Européanisation des fournisseurs de cloud, soit à travers l'européanisation de leurs opérations (par exemple, dépenses de R&D locales, achats locaux, création de valeur locale), soit par le contrôle européen effectif de leurs filiales locales (comme c'est déjà le cas dans certains pays), les autorités européennes assurant ainsi notamment une création de valeur effective régionalement, et un respect strict des réglementations européennes
- Séparation des activités cloud, soit fonctionnelle (séparation entre les divisions cloud et les autres, avec une répartition claire en termes de personnels, bureaux, propriété intellectuelle), soit structurelle (séparation des activités cloud dans une entité juridique distincte, comme cela est en débat aux Etats-Unis), gage d'une plus grande équité concurrentielle entre prestataires européens et américains

Les impacts économiques (valeur captée, emplois créés et investissements) **pourraient varier considérablement en fonction du scénario ; l'Europe pourrait perdre de 20 à 50% de l'impact économique attendu** en cas d'activation insuffisante des différents leviers identifiés dans les 5 scénarios

5 À court terme, pour atténuer les risques de ce marché du cloud très incertain, plusieurs initiatives¹ devraient être mises en œuvre par les décideurs publics et privés

- Il existe de fortes incertitudes concernant le futur du marché cloud européen, avec des impacts majeurs pour les principales parties prenantes (entreprises et services publics) qui doivent migrer vers le cloud
- **Ces incertitudes peuvent être atténuées par un certain nombre d'initiatives et de décisions :**
 - Les DSI, CTOs et RSSIs doivent envisager un certain nombre de bonnes pratiques pour une migration conforme et sécurisée : maîtrise de l'usage effectif de l'IT dans le cloud (données et charge de travail), impulsion d'un changement culturel vers une stratégie cloud proactive, et sélection et gestion précautionneuses des plateformes cloud (à travers notamment l'évaluation fine des prestataires)
 - Les Directeurs Juridiques devraient suivre finement la réglementation changeante et complexe des données : cartographie des transferts de données, évaluation des outils de transfert, réalisation d'une évaluation des risques en cas de non-conformité. Au-delà de la conformité réglementaire, le chiffrage des données peut garantir la souveraineté mais uniquement dans des conditions extrêmement strictes de mise en œuvre
 - Les Directeurs Marketing devraient développer une promesse client responsable et durable en termes de protection des données, valoriser des certifications cloud comme argument commercial et marketing, et se différencier de la concurrence par la garantie d'une conformité effective au RGPD
 - Les décideurs publics devraient apporter un soutien plus fort à la migration vers le cloud, avec des politiques publiques normalisées, une politique de dépenses dédiées au cloud computing et la mise en œuvre d'un programme de formation notamment pour les décideurs informatiques des collectivités territoriales. La lenteur relative de l'adoption du cloud par les autorités locales est un grand marché pour les opérateurs de cloud européens en mesure de répondre aux exigences en matière de souveraineté des données des collectivités

Note : (1). Résultat de plus de 50 entretiens poussés conduits auprès de dirigeants français et allemands



Sommaire

Le marché du Cloud européen : un marché à fort enjeu pour l'Europe, dont la taille devrait quadrupler d'ici 2027 **10**

La migration vers le cloud : une étape indispensable mais contraignante **22**

Incertitudes sur la réglementation des données : quels sont les risques pour les entreprises européennes ? **39**

5 scénarios pour le futur du marché européen du cloud..... **55**

Pour aller plus loin : bonnes pratiques et initiatives à mettre en place pour les parties prenantes du secteur privé et public..... **72**

Annexes

Chapitre 1 **81**

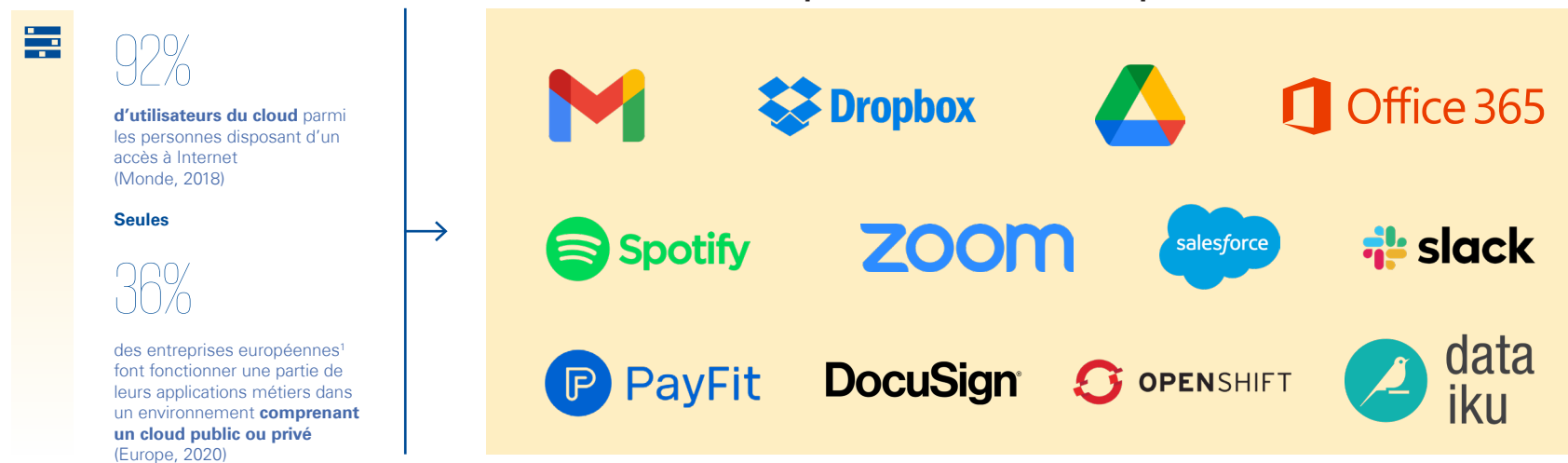
Chapitre 3 **89**

1



Le marché du
Cloud européen:
un marché à
fort enjeu pour
l'Europe, dont
la taille devrait
quadrupler d'ici
2027

Au cours de la dernière décennie, les particuliers et professionnels ont largement adopté les applications cloud, alors que les entreprises affichent un retard notable



- **Les applications cloud** se définissent comme des **applications accessibles par Internet** et hébergées sur des serveurs physiques
- Les entreprises peuvent choisir de louer² tout ou partie des **composantes cloud « as a service »** : hardware / infrastructure IaaS, plateformes PaaS ou logiciels SaaS

Notes : (1). Enquête menée auprès de sondés représentant env. 150 000 entreprises européennes (dont 83 % de petites entreprises, 14 % de moyennes et 3 % de grandes) (2). Ou de posséder (pour le IaaS)
Sources : Eurostat, Flexera, Vision Computer Solutions, Recherches et analyses GSG

Par rapport au modèle traditionnel, le cloud offre plus de flexibilité et une plus grande gamme de services aux entreprises, tout en limitant fortement les investissements

TRADITIONNEL (serveurs internes dans un espace propre ou tiers)

CLOUD (serveurs loués auprès d'un tiers)

Paiement des actifs

Avec des dépenses incrémentales pour l'achat de hardware / serveurs

Capacités limitées et non flexibles

Lenteur d'ajustement des capacités (p. ex., nécessité d'acheter, d'installer et de configurer des serveurs à chaque nouveau besoin additionnel en terme de capacités)

Forts besoins internes

Avec des équipes dédiées pour assurer la maintenance de l'infrastructure de calcul / stockage



Paiement à l'usage

Avec des services loués sans exigence d'investissements

Capacités flexibles et « illimitées »

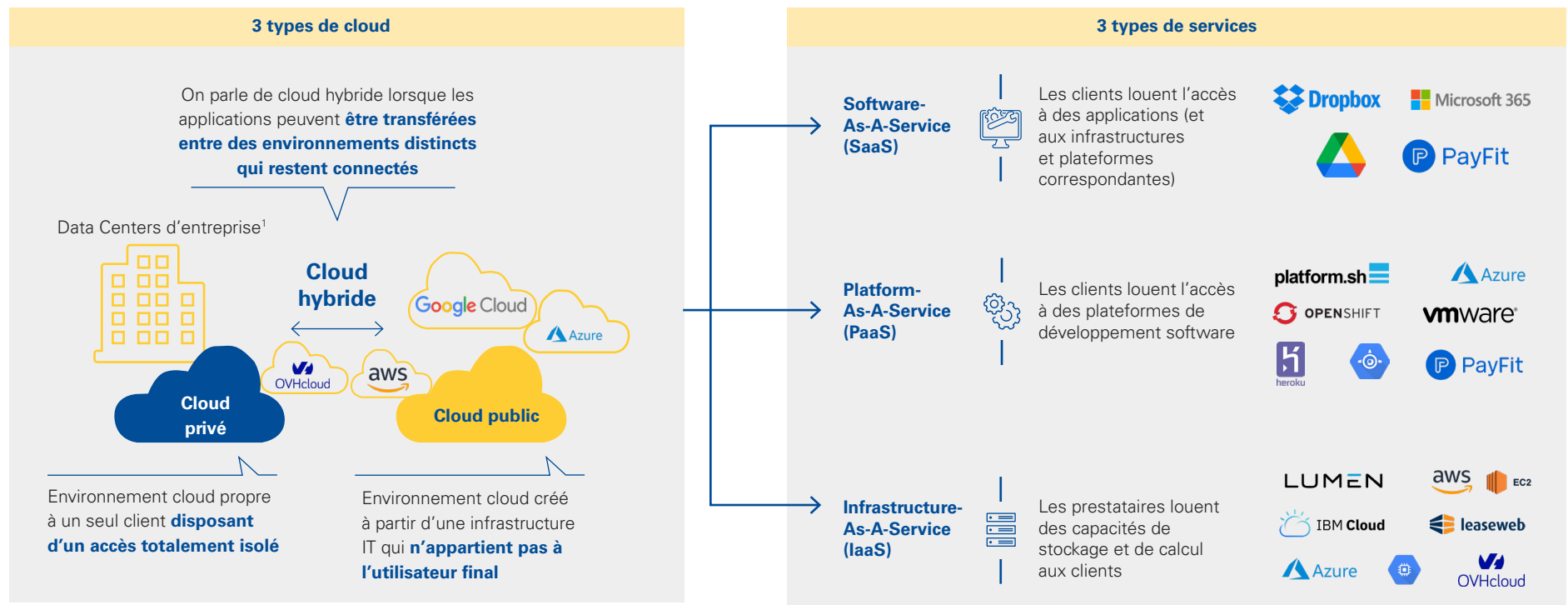
Possibilité d'augmenter ou de réduire instantanément des capacités de calcul / stockage prêtes à l'emploi

Besoins internes limités

Externalisation partielle (IaaS et PaaS) ou totale (SaaS) du déploiement et/ou de la maintenance à un prestataire externe

Le marché s'accorde pour regrouper le large éventail d'offres disponibles autour de six segments de marché constituant le « cloud »

Présentation de l'environnement du cloud computing en fonction du type de cloud et de services



Note : (1). Data Centers qui sont situés soit dans l'entreprise (on-premises), soit hébergés par un fournisseur cloud (hosted private cloud)
Source : Recherches et analyses GSG

NON-EXHAUSTIF

Les services du cloud couvrent un large éventail de solutions IT pour les entreprises, allant d'outils collaboratifs à des outils métiers plus spécifiques

Principaux usages pour chaque type de modèle de service



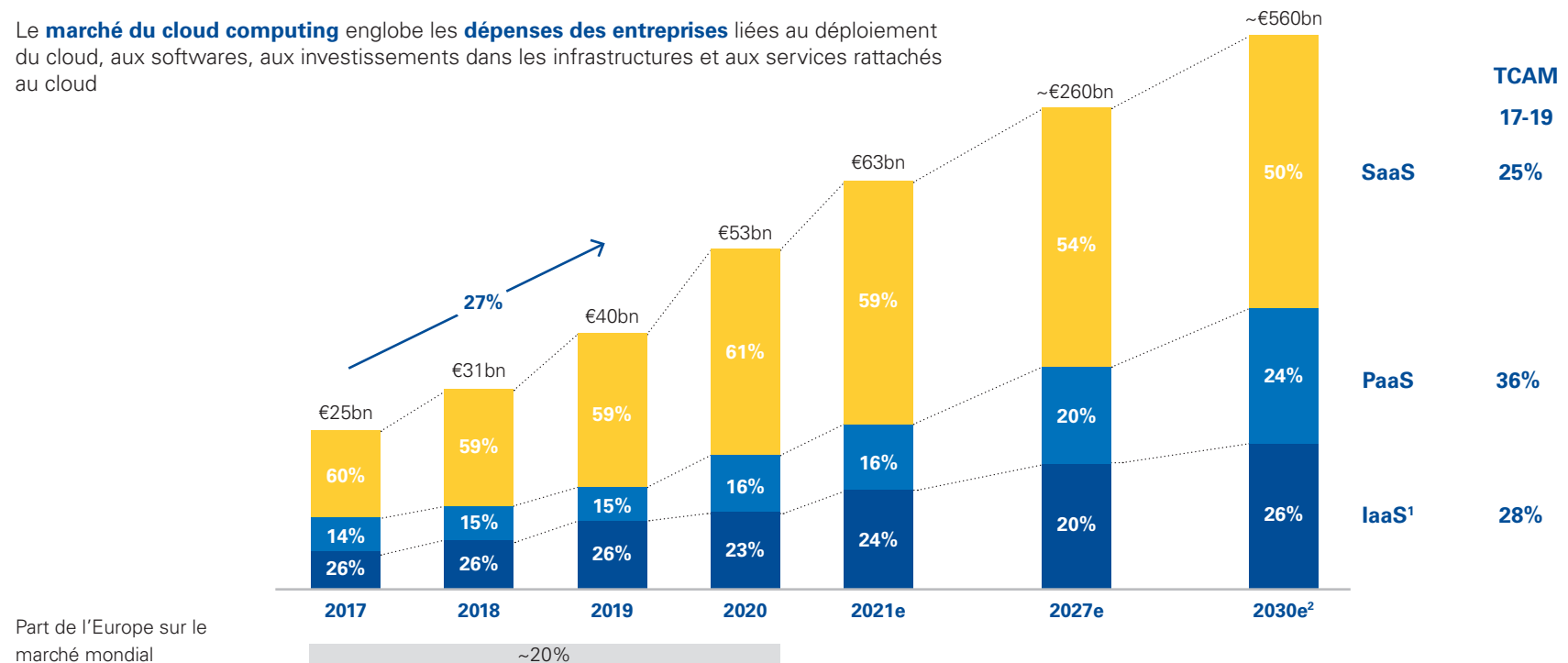
#X Classement basé sur le CA des services par catégorie¹

Note : (1). Chiffre d'affaires 2020 en Europe (IDC)
Sources : Gartner, Chiffre d'affaires des services cloud IT selon IDC, Recherches et analyses GSG

Le marché européen est un marché en forte croissance (+27 % par an entre 2017 et 2019), estimé à 53 Mds€ en 2020 et qui devrait atteindre 300 à 500 Mds en 2027

Évolution du marché européen¹ des services cloud IaaS, PaaS et SaaS (2017-2030, Md€)

Le **marché du cloud computing** englobe les **dépenses des entreprises** liées au déploiement du cloud, aux logiciels, aux investissements dans les infrastructures et aux services rattachés au cloud



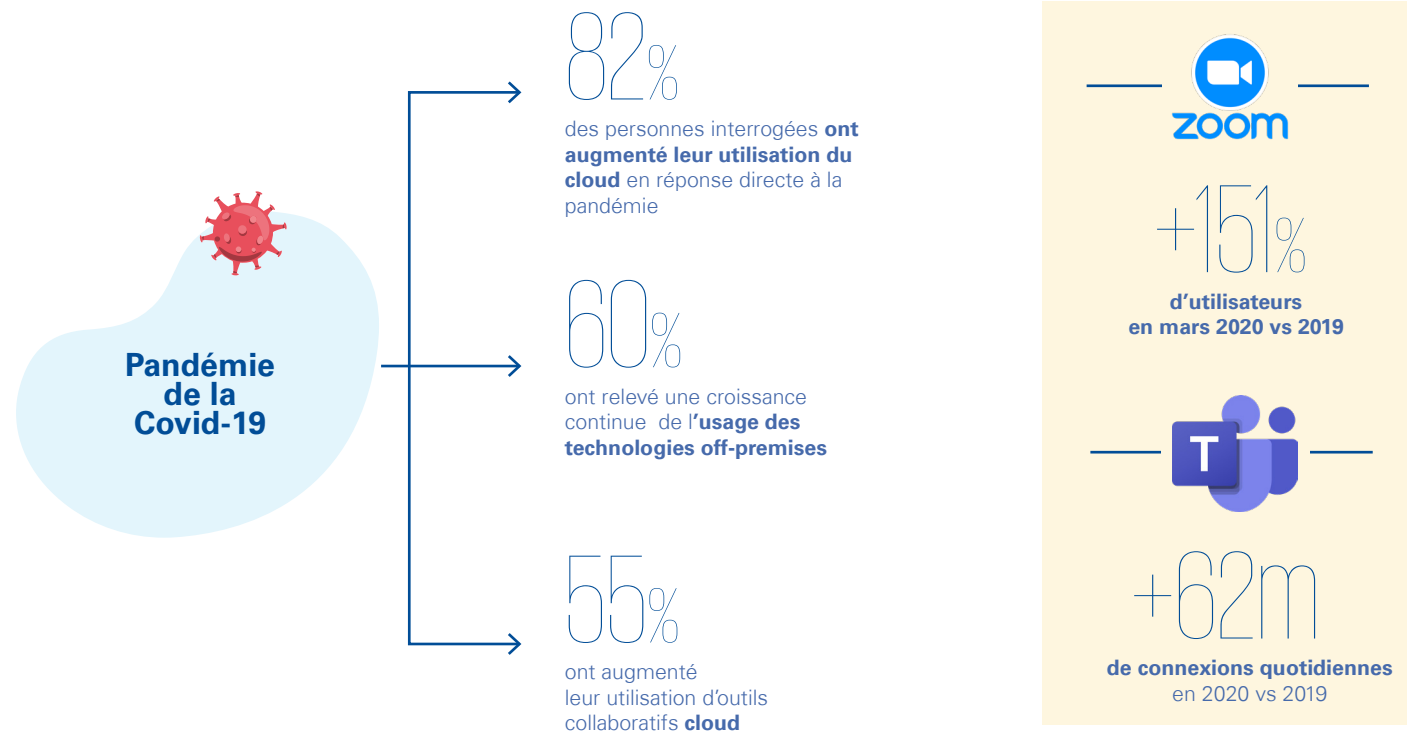
Notes: (1). IaaS market includes Public IaaS, Hosted private cloud and Baremetal cloud (2). GSG forecast

Notes : (1). Le marché IaaS englobe le IaaS public, le hosted private cloud et le baremetal cloud (2). Estimations GSG

Sources : IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018-2021 (IaaS, PaaS et SaaS), IDC Predictions 2021 European Cloud Predictions, IDC 2019 Forecast (hosted private cloud), Recherches et analyses GSG

La récente pandémie de la Covid-19 a accéléré la « cloudification » et a démontré le rôle stratégique du cloud en tant qu'infrastructure vitale et facteur de résilience

État des lieux de la migration cloud au niveau mondial post Covid-19¹ (2020)



Note : (1). Sur les 250 dirigeants IT sondés dans le monde

Sources : Cabinet de gestion d'actifs IT Snow Software, GLG Industry Insights, Entretiens experts, Recherches et analyses GSG

Les enjeux pour les fournisseurs européens de cloud sont, d'ici 2027, un marché de ~260 Mds€ , 550 k emplois créés et 200 Mds d'investissements (entre 2021 et 2027)



260 Mds€

Taille du marché du cloud prévue en 2027

Comparable aux marchés européens suivants

250 Mds€ in 2020

Marché des télécommunications

190 Mds€ in 2018

Marché du textile



550-600 K

D'emplois créés
pour un marché d'environ 260 Md€ en 2027

De nombreux emplois en région, dans les data centers ou dans les bureaux locaux :

- Développeurs
- Chargés de projet
- Data analysts
- Business developers
- Commerciaux
- Etc.



200 Mds€

d'investissements prévus
sur la période 2021-2027

Principaux domaines d'investissement des fournisseurs de cloud dans les 10 prochaines années :

- Amélioration de l'efficacité énergétique
- Basculement de l'architecture des data centers vers les processeurs ARM aux performances accrues
- R&D dans des domaines comme l'Intelligence Artificielle ou la recherche de médicaments

Même s'il devrait, à terme, atteindre une taille équivalente au marché des Telco, le marché du cloud apparaît encore comme très peu mature par rapport à ce marché



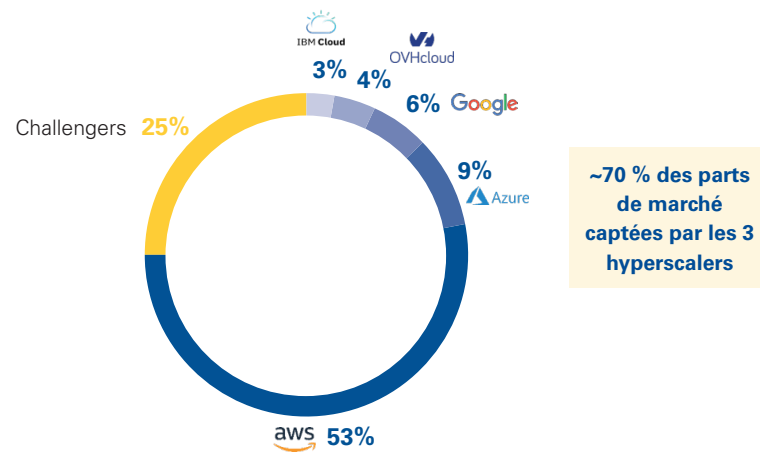
- En Europe, le marché du cloud devrait atteindre **une taille comparable à celui des télécoms à horizon 2030**
- Le marché du cloud devrait évoluer comme le secteur des télécoms, et atteindre un niveau de maturité équivalent, notamment grâce à **l'intervention des pouvoirs publics**, pour devenir :
 - un marché très concurrentiel, où **les licences et la forte concurrence plus de 200 opérateurs mobiles¹** en Europe en 2018) généreront une **concurrence saine sur les prix** et une **pression suffisante sur les marges bénéficiaires**
 - un marché très réglementé, régi par les **pouvoirs publics, les autorités de la concurrence** (par exemple, ARCEP), **les agences nationales publiques et les régulateurs** (par exemple, BEREC, organisme européen de réglementation des télécoms) **défendant l'innovation et la protection du client et réglementant les projets de consolidation**

Notes : (1). MNO : Mobile Network Operators (2). Prévisions GSG, basées sur une hypothèse de stabilité / croissance faible du marché vs la situation actuelle (~250 Md€)
Sources : Gartner T3 2019 (cloud public), IDC 2019 Forecast (cloud privé), ETNO 2020, The Delta Perspective 2019, Recherches et analyses GSG



Faiblement concurrentiel, le marché du cloud est dominé par trois « hyperscalers » internationaux américains (exemple, ~70 % de part de marché de l'IaaS)

Part de marché des principaux acteurs du cloud computing européen (IaaS) (S1 2020)



Panorama des acteurs clés du cloud en France et en Allemagne (IaaS, notamment hosted private cloud et PaaS) (2020)

	France	Allemagne
Leader	aws	aws
#2	Azure	Azure
#3	OVHcloud	Google
#4	orange	T-Mobile Systems
#5	Google	IBM Cloud
#6	IBM Cloud	ORACLE

La grande majorité (~70 %) des dépenses d'infrastructure cloud (IaaS) des entreprises européennes est captée par des fournisseurs de cloud non-européens

Les investissements en infrastructure et technologies cloud sont eux aussi souvent réalisés hors Europe, exemple. :

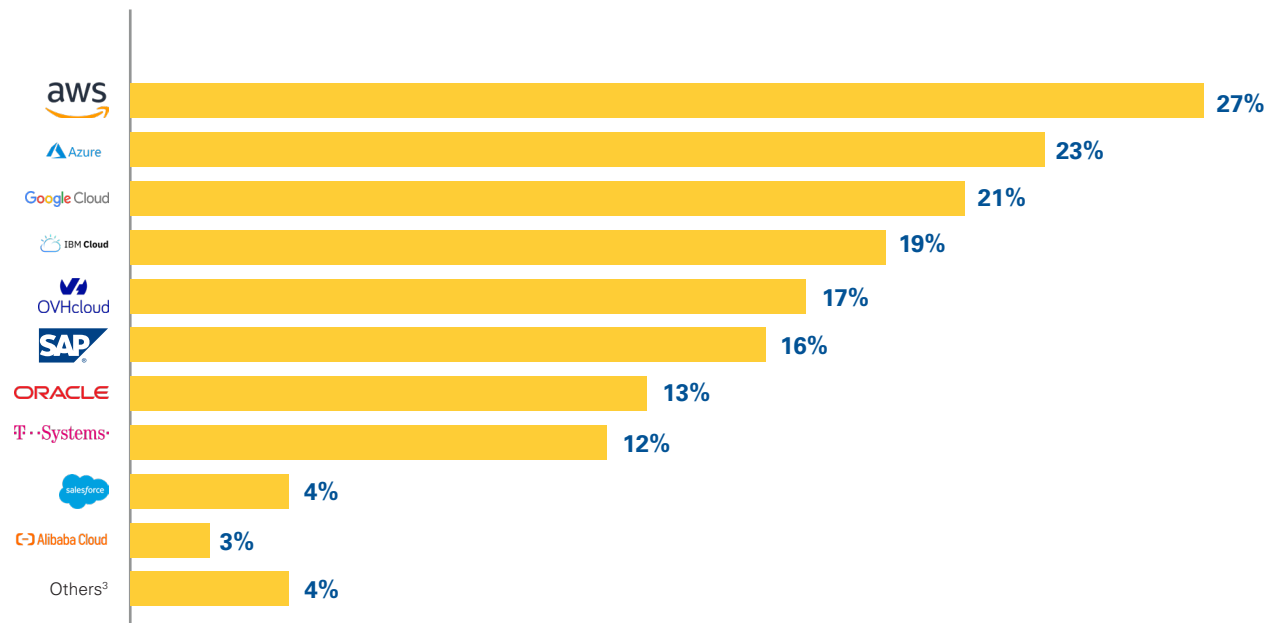
- Google Cloud a investi plus de 13 Mds\$ dans son activité de cloud computing en 2019, dont seulement 23 % en dehors des Etats-Unis (dont en Europe)
- Les investissements d'AWS sont principalement situés aux Etats-Unis, ainsi qu'en Inde (prévisions 2020-2022 : 7,8 Mds\$)

Cependant, **les spécialistes du cloud et les opérateurs télécoms européens gagnent progressivement des parts de marché sur leurs marchés nationaux respectifs** (exemple, OVHcloud et Deutsche Telecom se classent 3e et 4e dans leurs pays sur les marchés IaaS et PaaS)

Cette domination se confirme par les résultats de notre enquête, qui montrent que les dirigeants européens préfèrent AWS, Azure et GCP aux autres fournisseurs

Fournisseurs de services cloud des entreprises des répondants¹

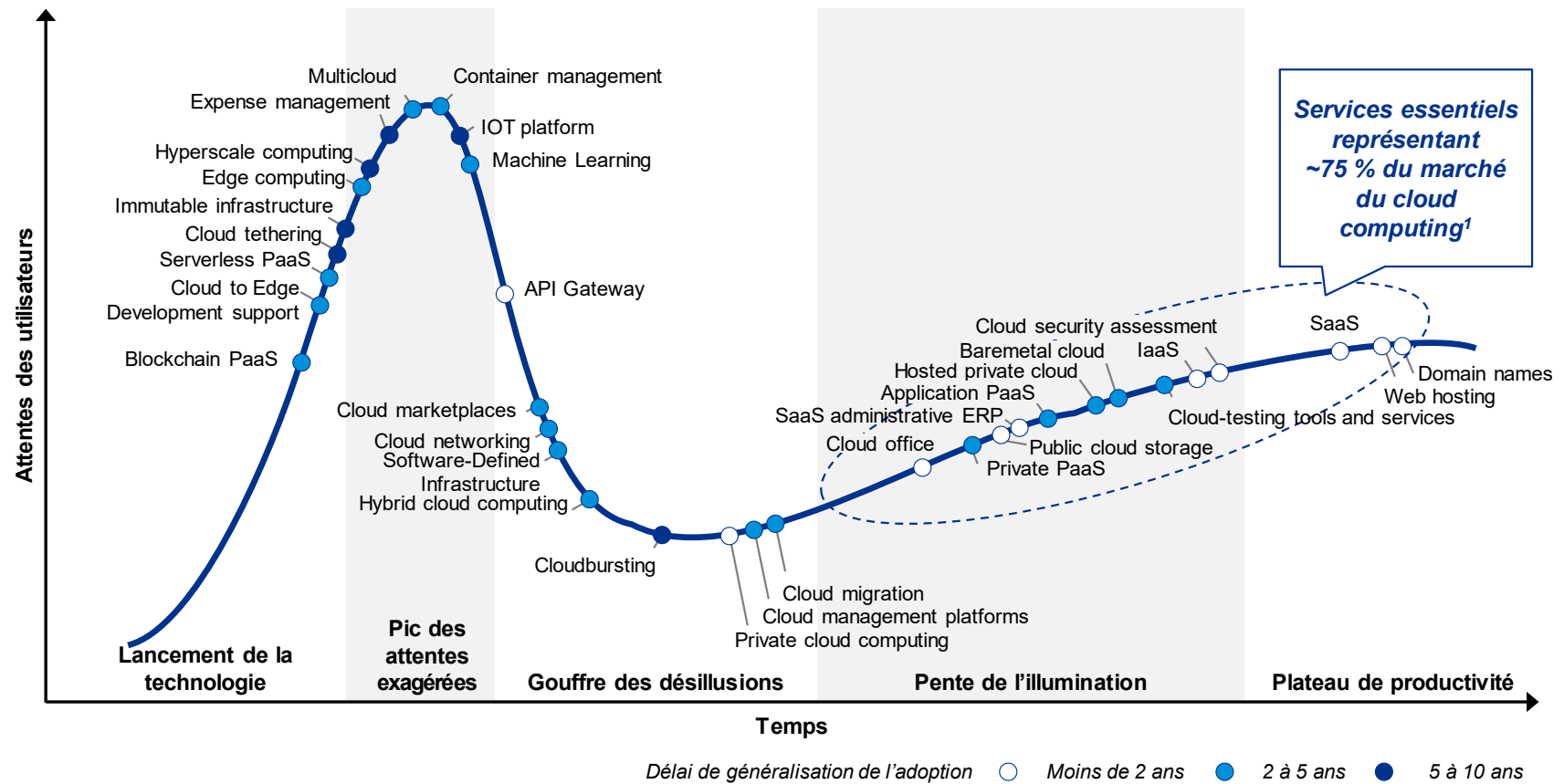
Qui sont vos fournisseurs de services cloud², en particulier pour le IaaS et le PaaS ? (Plusieurs réponses possibles)



Notes : (1). Réponses recueillies auprès de 200 dirigeants français et allemands (2). Pourcentage basé sur la présence du fournisseur dans l'entreprise, et non sur le budget IT associé (3). Liste des autres fournisseurs cloud mentionnés : HCL, Scaleway, Veeva Systems, Huawei, TCS, QAD DynaSys Cloud
Sources : Sondage GSG, Analyses GSG

Le marché du cloud computing est un marché encore peu mature, qui connaîtra un grand nombre d'innovations dans les années à venir

Gartner hype cycle du cloud computing [2018]



Note : (1). Soit environ 75 % du marché cloud correspondant à la liste des services cloud essentiels délimités par le cercle en pointillés

Sources : Courbe Gartner hype cycle du cloud computing (2018), IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018-2021, Recherches et analyses GSG

2



La migration
vers le cloud :
une étape
indispensable
mais
contraignante

La migration vers le cloud et l'adoption croissante de solutions sur le cloud sont portées par des logiques d'optimisation opérationnelle et financière

Sélection des principaux motifs d'adoption du cloud (non-exhaustifs)

Exemple de situation	Variabilisation des coûts	Flexibilité dans l'utilisation des capacités	Collaboration entre les équipes, et échange de données sécurisé	Agilité et fluidité du déploiement	Sécurité et nouveau paradigme de résilience	Agilité de déploiement des activités stratégiques
						
	- Le Directeur des Système d'Informations et le Directeur Financier d'une PME supportent des coûts fixes élevés liés à l'exploitation de leurs data centers on-premise, et envisagent une migration sur le cloud... ...afin de transformer les coûts fixes des data centers (serveurs propres) en coûts variables (cloud), et assurer ainsi une marge globale plus stable	- Le fondateur d'une startup, dont le produit SaaS récemment mis sur le marché connaît une forte croissance en terme de nombre d'utilisateurs, souhaite pouvoir : - Être flexible dans l'utilisation des capacités de stockage / calcul pour satisfaire la demande... - ... tout en pouvant réduire à tout moment les capacités utilisées si nécessaire	- À cause de la Covid-19, un employé ne peut plus rencontrer ses clients en physique et doit donc échanger des informations avec celui-ci en ligne, et notamment des documents volumineux et confidentiels - L'employé utilise donc une solution cloud SaaS mise en place par son entreprise, servant d'interface sécurisée entre les deux organisations	- Le DSI d'une entreprise souhaite gagner en agilité IT et éviter la gestion manuelle de ses data centers (câbles, racks...), et envisage ainsi la migration vers le cloud pour gérer son infrastructure « as code » et non pas comme infrastructure physique	- Le DSI d'une entreprise souhaite sécuriser les données de son entreprise et améliorer sa résilience aux sinistres - Un particulier a des difficultés de stockage des fichiers volumineux et envisage le transfert de ces fichiers sur le cloud pour : - Faciliter l'accès à ces données, pour lui et ses proches - Se prémunir contre la perte ou le vol de ces données	- Le dirigeant d'une entreprise souhaite améliorer la performance de ses activités existantes et en développer de nouvelles, en ayant recours aux nouvelles technologies : - Optimisation du parcours client - Lancement de produits via l'Intelligence Artificielle - Déploiement rapide des nouvelles activités

Ces raisons qui encouragent la migration vers le cloud ressortent de nos différents échanges avec les décideurs impliqués sur les sujets cloud (1/2)

Verbatims de décideurs européens impliqués sur les sujets cloud

Variabilisation des coûts

« Le remplacement de nos systèmes traditionnels vieillissants a été pour nous l'occasion idéale de migrer sur le cloud pour avoir une structure de coûts plus variable pour nos systèmes IT. »

DSI d'une entreprise du secteur énergétique

Flexibilité dans l'utilisation des capacités

« Pour s'adapter instantanément aux pics d'activité, le cloud computing est la meilleure option, par comparaison avec des infrastructures internes coûteuses dont la montée en puissance est plus lente. »

DSI d'une entreprise publique française

Collaboration entre les équipes, et échange de données sécurisé

« Grâce au cloud, le télétravail imposé lors de la période du confinement a pu être rapidement mis en place ; nos équipes ont été à même de collaborer efficacement, où qu'elles se trouvaient et sur n'importe quel terminal. »

DSI d'un cabinet de conseil international

« Pour une petite startup comme la nôtre, avec des ressources financières limitées, et ne pouvant investir dans une infrastructure interne et des équipes IT permanentes, le cloud est la meilleure solution. »

DG d'une startup française

« Pendant la première semaine du confinement de mars 2020, l'usage de Teams a été multiplié par 20. Nous n'aurions jamais été en mesure de faire cela en interne dans un délai si court. »

DSI d'une entreprise du secteur énergétique

« Les outils collaboratifs sur le cloud nous permettent de partager des fichiers sensibles avec nos clients via des canaux sécurisés et chiffrés. »

DSI d'un cabinet de conseil international

Ces raisons qui encouragent la migration vers le cloud ressortent de nos différents échanges avec les décideurs impliqués sur les sujets cloud (2/2)

Verbatims de décideurs européens impliqués sur les sujets cloud

Agilité et fluidité du déploiement

« La taille et la couverture géographique du fournisseur cloud sont essentielles, car il lui faut pouvoir s'adapter constamment à nos besoins globaux. »

DSI d'une multinationale de l'industrie chimique

« Comme nous envisageons de nous développer en Amérique du Nord, nous ne pouvons plus nous reposer sur nos data centers français et nous envisageons d'utiliser également le cloud public. »

DSI d'une entreprise du secteur du gaming

Sécurité et nouveau paradigme de résilience

« Les données clients représentent un actif clé pour mon entreprise. En cas de sinistre, la résilience de mon activité est assurée car mes données sont sécurisées dans des data centers de sauvegarde, gérés par des fournisseurs cloud. »

DSI d'une banque internationale

« En faisant migrer nos données vers des environnements cloud, nous avons eu automatiquement accès aux technologies de cybersécurité et technologies de la feuille de route de notre fournisseur cloud. »

DSI d'une banque internationale

Agilité de déploiement des activités stratégiques

« Comme nous avons développé une plateforme de jeu de qualité basée sur le cloud pour notre marché national, il était logique de permettre aux acteurs étrangers du même secteur de l'utiliser sur leur propre marché - nous sommes ainsi devenus un fournisseur SaaS. »

DSI d'une entreprise du secteur du gaming

« Nous avons choisi de migrer vers le cloud car les solutions les plus innovantes sont fournies en SaaS. »

DSI d'une banque internationale

La sélection des fournisseurs de cloud s'effectue sur plusieurs critères, les plus importants étant la sécurité et la souveraineté des données

Principaux critères d'achat sur le marché du cloud computing (sur la base des réponses fournies par les dirigeants interrogés¹)

KPC	Poids	Motif
Résilience et sécurité des services		“Notre fournisseur cloud doit être en mesure de garantir une infrastructure et des services hautement sécurisés , afin de prévenir les violations de données internes et externes. ” (DSI français)
Risques réglementaires et conformité (dont la souveraineté des données)		“Lors du choix d'un fournisseur cloud, la souveraineté des données et la conformité réglementaire sont des critères tout aussi importants que la qualité du service. ” (DSI allemand)
Certifications et normes		“Comme nous manipulons des données de santé sensibles , nous ne pouvons pas nous permettre d'utiliser des services cloud non certifiés . Nous avons donc dû choisir notre fournisseur de cloud en conséquence.” (DSI français)
Largeur et qualité du portefeuille de services		“ L'évolutivité et la fiabilité ainsi que l'accès à des technologies de base et innovantes sont nos principales priorités lors du choix d'un fournisseur cloud” (DSI français)
Coût		“Nous avons besoin de fournisseurs de cloud capables de couvrir nos besoins fonctionnels et d'infrastructure à des prix raisonnables et transparents..” (DSI allemand)
Notoriété et références de l'entreprise		“Nous devons pouvoir compter sur un fournisseur cloud fiable et de grande envergure , capable de nous accompagner sur le long terme , en couvrant nos besoins technologiques et notre expansion géographique. ” (DSI allemand)

Note : (1). Réponses recueillies auprès de 76 DSI français et allemands (résultats à la fois quantitatifs et qualitatifs)
Sources : Sondage GSG, Analyses GSG

Légende :



Les décideurs interrogés estiment la souveraineté des données comme étant importante, notamment la conformité au RGPD et la localisation des data centers

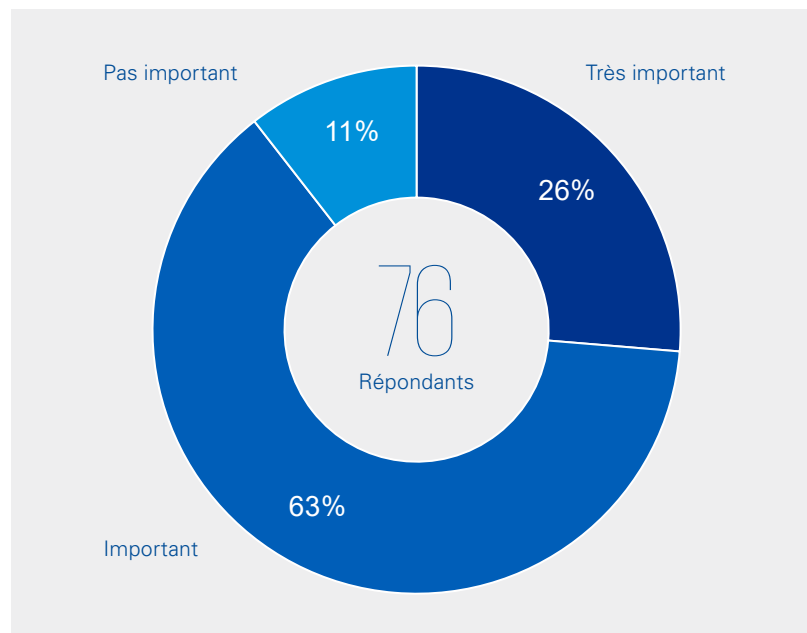


Risques réglementaires et conformité (dont la souveraineté des données)

La **souveraineté des données** est mentionnée comme un critère **important dans la sélection d'un fournisseur cloud** par la grande majorité des décideurs interrogés...



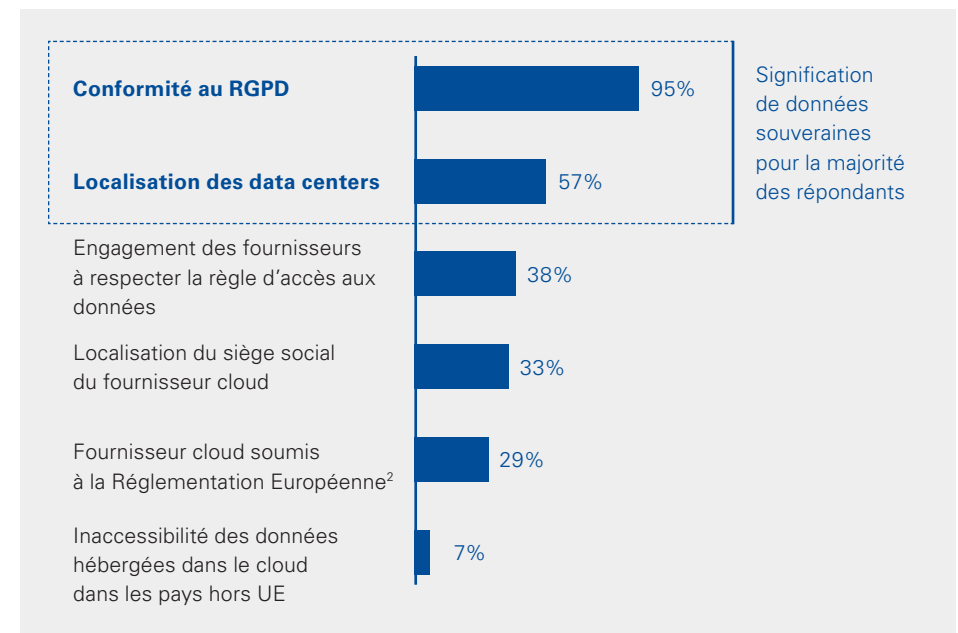
Dans quelle mesure la souveraineté des données est-elle un **critère de choix de votre/vos fournisseur(s) cloud?**¹



... Toutefois, la souveraineté semble avoir plusieurs significations, **et notamment deux dimensions** (conformité au RGPD et localisation des data centers)



Selon vous, lesquels de ces critères **décrivent le mieux la souveraineté des données ?** (Plusieurs réponses possibles)¹



Notes : (1). Réponses recueillies auprès de 76 DSI's français et allemands (2). Fournisseur cloud soumis à la réglementation européenne mais pas à une législation extraterritoriale (ex., Cloud Act)
Sources : Sondage GSG, Analyses GSG

Bien que la souveraineté soit importante dans le choix du fournisseur, les dirigeants déclarent ne disposer que d'options limitées pour les services cloud



Risques réglementaires et conformité (dont la souveraineté des données)

Arbitrage aux dépens de la souveraineté des données, avec une offre de services souverains jugée trop limitée

“Nous **refusons de mettre en œuvre une stratégie cloud** globale pour des raisons de souveraineté des données, mais en période de pics d'activité, **le cloud reste la solution de repli la plus rapide et efficace**”

DSI d'un prestataire de services logistiques européens

“J'aimerais voir émerger des **fournisseurs de cloud européens**, car cela faciliterait les discussions en interne sur la migration vers le cloud, limitée à cause des problèmes de souveraineté. Mais est-ce que ça arrivera, et quand ? Je ne peux pas attendre des années avec mes systèmes vieillissants...”

DSI d'une entreprise pétrolière et gazière internationale

“A date, il n'existe aucune offre souveraine satisfaisante pour les données de santé. La migration des données vers un cloud souverain semble seulement concevable à moyen terme et pas avant 2022.”

DSI d'une entreprise publique française

Acceptation d'une souveraineté des données partielles

“Nous avons choisi un fournisseur de cloud américain dès que notre **service juridique a validé le contrat** (qui n'a pas été revu depuis, **malgré les évolutions réglementaires majeures**).”

DSI d'une entreprise pétrolière et gazière internationale

“Nos **inquiétudes quant à la souveraineté des données** ont été levées par l'assurance d'avoir des données localisées exclusivement dans l'Union européenne, même si celles-ci sont **détenues par des fournisseurs américains**.”

DSI d'une entreprise pétrolière et gazière internationale

“Même lorsque notre fournisseur cloud nous garantit un hébergement des données en Europe, il y a tout de même **des transferts de données en dehors de l'Europe**, comme pour la maintenance ou le support technique.”

DSI d'une entreprise pétrolière et gazière internationale

Le manque de connaissance des offres garantissant la souveraineté des données limite la croissance du marché européen du cloud ce qui conduit certaines entreprises à ralentir, voire abandonner leur migration



Risques réglementaires et conformité
(dont la souveraineté des données)

Abandon de la migration cloud à cause des préoccupations autour de la souveraineté des données

“

“Une note des ministères de l'Intérieur et de la Culture français **interdit le stockage de documents publics dans des data centers non souverains**. Cela rend **toute migration cloud impossible dû au nombre limité d'offres souveraines sur le marché.**”

DSI d'une entreprise publique française

“

“Nous refusons catégoriquement de placer les **données de nos clients** sur le cloud pour **des raisons de souveraineté**. Nous avons donc opté pour un **stockage on-premise de toutes nos données et tous nos logiciels.**”

DSI d'une entreprise internationale du secteur du gaming

“

“Le Comité exécutif a été très clair concernant la localisation des données de nos clients. **Elles doivent rester en interne et ne peuvent être en aucun cas hébergées par des tiers**”

DSI d'un prestataire de services logistiques européen

“

“Comme nous n'avons **aucune garantie** quant à la **localisation des différents composants de la chaîne de valeur** du fournisseur cloud (stockage, calcul, maintenance), nous **n'avons pas d'autre choix que d'utiliser des data centers gérés en interne pour nos données sensibles.**”

CIO, international bank

“

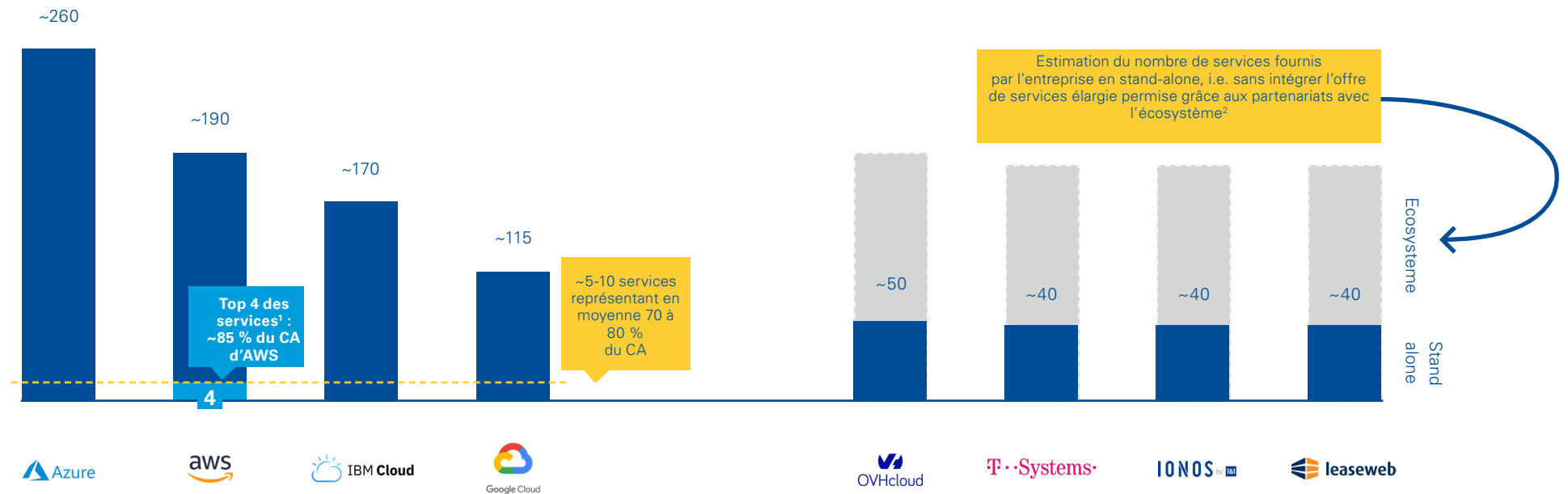
“Lorsque nos données sont **stockées on-premise**, les audits de souveraineté sont assez simples à conduire, ce qui est **techniquement impossible** lorsqu'on utilise **les installations d'un fournisseur tiers.**”

Directeur Juridique d'un prestataire de services logistiques européen

Les hyperscalers offrent un large éventail de services, mais la majorité de leurs chiffres d'affaires est générée par un nombre limité de services



Nombre de services et produits cloud (clouds privés, publics et hybrides) de certains fournisseurs majeurs du cloud [2020]



Notes : (1). Services de base : EC2 (Elastic Compute Cloud, capacité de calcul), EBS (Elastic Block Store, stockage de blocs), RDS (Relational Database Service), S3 (Simple Storage Service, stockage d'objets) (2).

Voir slides suivantes pour des informations additionnelles sur l'écosystème européen

Sources : Recherches et analyses GSG, Sites web d'entreprises, Cloud PegBoard, Cloudability State of Cloud 2018

L'écosystème cloud Européen semble très dense, avec une grande variété d'acteurs, qui ne sont pas uniquement des fournisseurs de cloud généralistes



Un écosystème Européen de fournisseurs technologiques dense (liste non-exhaustive)

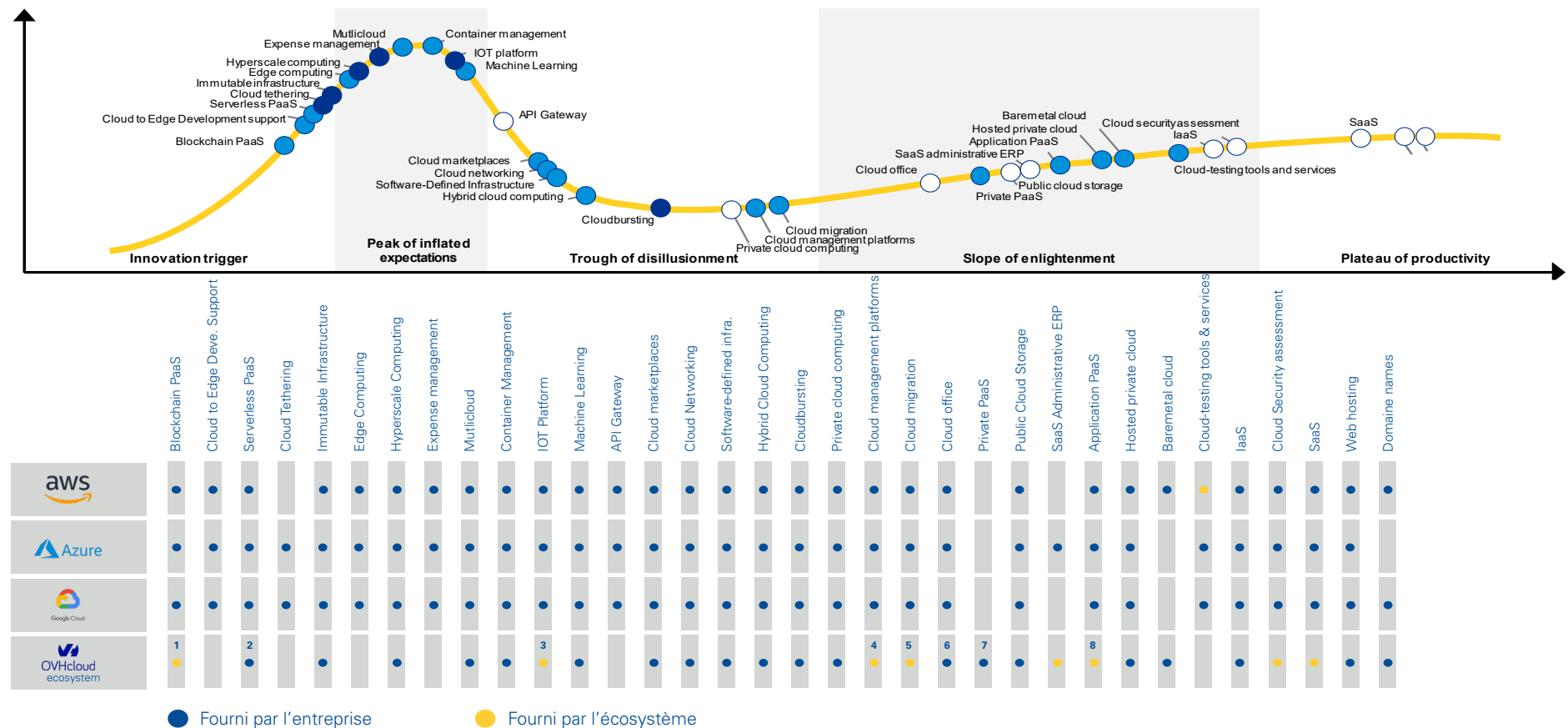


En s'appuyant sur cet écosystème, les acteurs européens peuvent proposer une largeur et une profondeur de gamme comparable à celle des hyperscalers



Largeur et qualité du portefeuille de services

Positionnement de l'offre des fournisseurs de cloud sur la courbe hype cycle du cloud computing [2018]



Notes : (1). TON Ventures (2). Google Anthos, Clever Cloud (3). SmartHub (4). Cloudify (5). Capgemini, Atos, Sopra Steria, Partito (6). Sharepoint, Office 365 (7). Google Anthos (8). Platform.sh, Clever Cloud
Sources : Gartner hype cycle du cloud computing (2018) , Wipro, Sites web d'entreprises, Recherches et analyses GSG

Grâce à un écosystème dense, les challengers Européens, comme OVHcloud, offrent un portefeuille de services exhaustifs couvrant les besoins des clients (1/3)



Services des fournisseurs et leur couverture fonctionnelle¹ – Offres principales



Note : (1). D'après les informations communiquées sur les sites web des entreprises

Sources : Gartner, IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018-2021, Sites web d'entreprises, Recherches et analyses GSG

Grâce à un écosystème dense, les challengers Européens, comme OVHcloud, offrent un portefeuille de services exhaustifs couvrant les besoins des clients (2/3)



Largeur et qualité du portefeuille de services

Services des fournisseurs et leur couverture fonctionnelle¹ – Offres principales



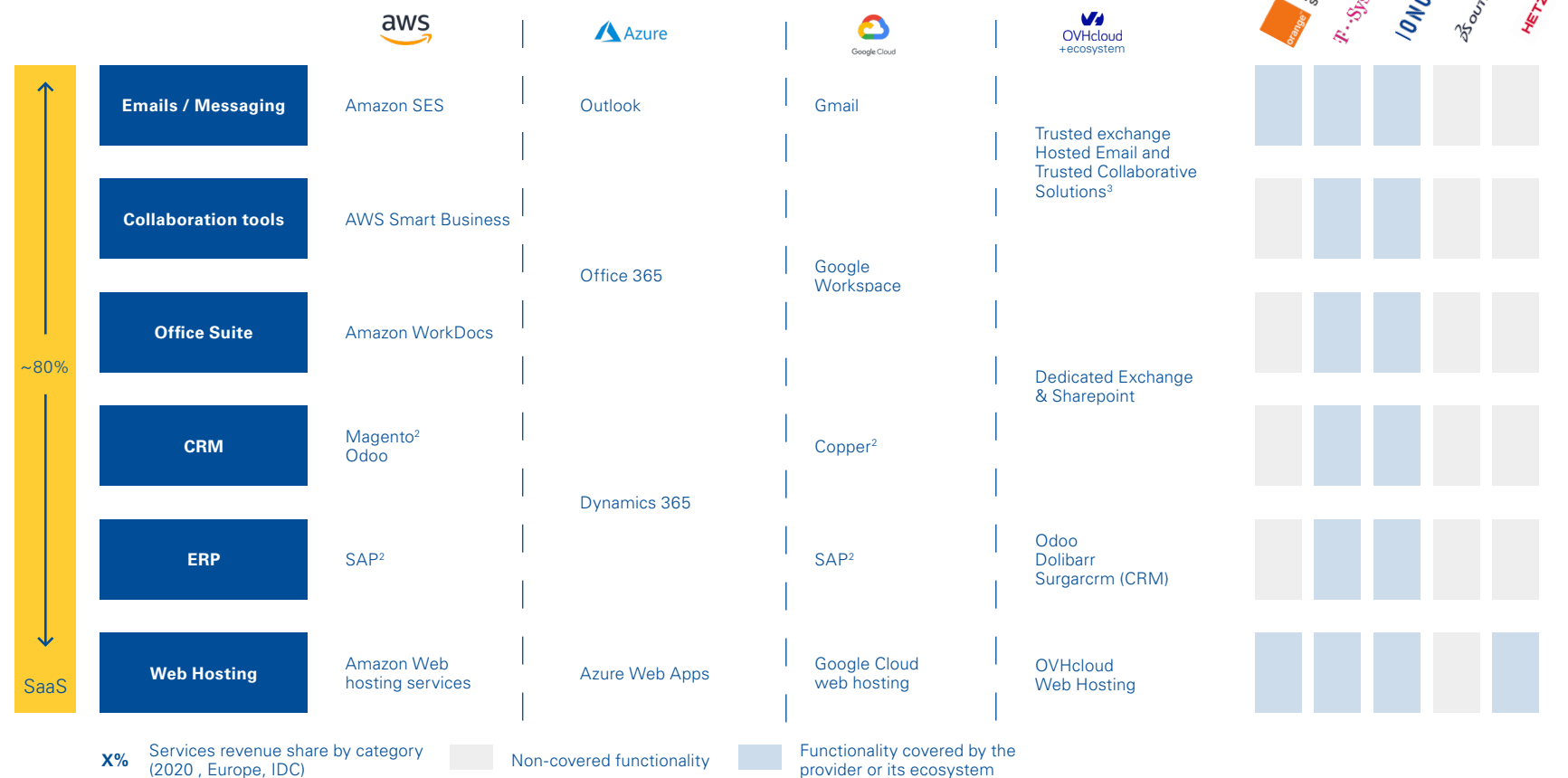
Notes : (1). D'après les informations communiquées sur les sites web des entreprises (2). Exemples d'offres disponibles sur la marketplace
 Sources : Gartner, IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018-2021, Sites web d'entreprises, Recherches et analyses GSG

Grâce à un écosystème dense, les challengers Européens, comme OVHcloud, offrent un portefeuille de services exhaustifs couvrant les besoins des clients (3/3)



Largeur et qualité du portefeuille de services

Services des fournisseurs et leur couverture fonctionnelle¹ – Offres principales



Notes : (1). D'après les informations communiquées sur les sites web des entreprises (2). Exemples d'offres disponibles sur la marketplace (3). Autres partenaires (non-exhaustifs) : Zimba, Dropcloud et Nextcloud
 Sources : Gartner, IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018-2021, Sites web d'entreprises, Recherches et analyses GSG

Malgré l'attractivité relative des prix affichés, les fournisseurs internationaux dominent le marché grâce à des pratiques d'acquisition client agressives et offres groupées...



Gestes commerciaux lors de la phase d'acquisition client

“Pour faciliter notre migration vers le cloud d'un fournisseur cloud international, j'ai été accompagné **gratuitement** pendant six mois par **cinq consultants à temps plein**”

DSI d'une entreprise publique française

“Je me suis vu offrir un bon d'achat de **100 M€** par un fournisseur cloud international **en échange d'un contrat d'exclusivité de 5 ans**”

DG d'une fintech allemande

“Ma première année en tant qu'utilisateur de services d'un fournisseur global de cloud **ne m'a rien coûté**, ce qui nous a fortement **motivé à migrer vers le cloud**.”

DSI d'une PME française éditrice de logiciels

“L'objectif de certains fournisseurs de cloud mondiaux est **d'enfermer les clients dans leur écosystème le plus rapidement possible**, c'est pourquoi **le chargement des données** (contrairement au téléchargement) **est gratuit**.”

DSI d'un cabinet de conseil international

Vente liée, groupée ou échange de services

“La signature d'un **contrat d'approvisionnement stratégique** clé avec un fournisseur cloud international était **soumise à une condition sine qua non** : la migration de nos données sur son cloud public.”

DSI d'une entreprise pétrolière et gazière internationale

“Au début, je souhaitais me servir d'Office 365 dans un autre environnement cloud, différent de l'infrastructure Microsoft, mais je me suis **rapidement heurté à la réalité : ça aurait été beaucoup plus onéreux**.”

DSI d'une PME française éditrice de logiciels

“L'une des raisons qui ont accéléré notre décision de changer notre fournisseur de cloud sont les pratiques commerciales agressives **des vendeurs**. Nous avons **été contraints de prendre et de payer des services additionnels dont nous n'avions pas besoin**.”

DSI d'un cabinet de conseil international

“Des fournisseurs d'outils de bureau renommés **commercialisent des offres IaaS et SaaS groupées** à des prix extrêmement attractifs, coûtant **cinq fois moins cher que les offres IaaS des concurrents**.”

DSI d'un prestataire de services logistiques européen

... notamment en proposant des offres groupées SaaS et IaaS pour des logiciels fonctionnant historiquement sur un environnement local



Une base clients historiquement importante utilisant des logiciels **desktop**, aujourd'hui exploitée par certains hyperscalers...

De¹

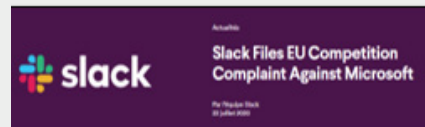
à



Office 365

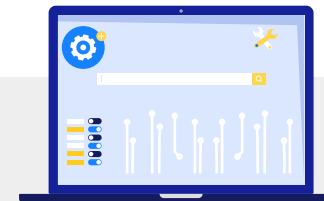


... à travers le groupement et la vente liée d'offres **IaaS + SaaS**, parfois en violation du principe BYOL (« Bring Your Own License ») avec la mise en place de contraintes techniques et financières...



“ Microsoft a **illégalement** lié son produit Teams à sa suite Office qui domine le marché, en l'installant de force, **en empêchant sa suppression et en en dissimulant le vrai coût aux entreprises clientes**”

Communiqué de presse de Slack, juillet 2020



En conséquence, un certain nombre d'éditeurs historiques de logiciels groupent leurs produits traditionnels (désormais en SaaS) avec leurs produits IaaS...

Même si les deux catégories de produits sont historiquement séparées et peuvent techniquement l'être ²

Aux pratiques d'acquisition client s'ajoutent des conditions complexes de sortie qui rendent difficile pour l'utilisateur cloud de quitter ou changer de fournisseur



Coût

Fortes barrières à la sortie et enfermement propriétaire

“Une fois que l'on a téléchargé toutes les données sur le cloud d'un fournisseur cloud international, on s'aperçoit que **le coût de leur transfert ailleurs est extrêmement élevé.**”

DSI d'un cabinet de conseil international

“ Nous avons fait **le choix facile et rapide** d'utiliser des APIs propriétaires fournies par des fournisseurs cloud internationaux au lieu de développer les nôtres en interne, **sachant qu'il serait difficile et coûteux** d'en sortir.”

DSI d'une entreprise pétrolière et gazière internationale

“Pour les pouvoirs publics, les contrats cloud doivent légalement **être revus régulièrement**. Les fournisseurs de cloud public, avec **leur non-portabilité et leurs frais de sortie élevés, ne peuvent donc pas être une solution pour nous.**”

Responsable Technique et Infrastructure d'une collectivité locale française

“Nos développeurs ont fait le choix d'utiliser les solutions **propriétaires innovantes et faciles à utiliser** d'un fournisseur mondial de cloud. Nous n'y étions pas opposés, jusqu'à ce que nous soyons confrontés à **des problèmes de migration** et que nous **devions par conséquent dépasser le budget initialement fixé.**”

DSI d'un cabinet de conseil international



Contrats d'engagement de longue durée, aux conditions tarifaires peu précises

“Si vous décidez de résilier votre contrat avec certains fournisseurs cloud internationaux trois ans avant son terme, vous **devrez vous acquitter de la totalité du montant des trois années restantes.**”

DSI d'une PME française éditrice de logiciels

“Entre **les frais élevés de résiliation anticipée des contrats à durée déterminée et les clauses d'engagement de dépenses** fixées par certains fournisseurs cloud globaux, le changement de fournisseur cloud devient en fin de compte une **décision très coûteuse.**”

DSI d'une entreprise publique française

“Attirés en premier lieu par des prix de **stockage attractifs proposés** par le fournisseur de cloud mondial que nous avions choisi, et **non conscients des autres coûts associés**, nous avons vu notre facture globale augmenter très rapidement, **à mesure que nos systèmes devenaient de plus en plus complexes.**”

DG d'une Fintech allemande

“Aujourd'hui, nous ne sommes toujours pas capables de **prévoir nos dépenses cloud**, à cause de la **complexité du contrat**, de la difficulté à comprendre **le périmètre des services fournis** et de **notre manque de maturité à ce sujet.**”

DSI d'une entreprise pétrolière et gazière internationale

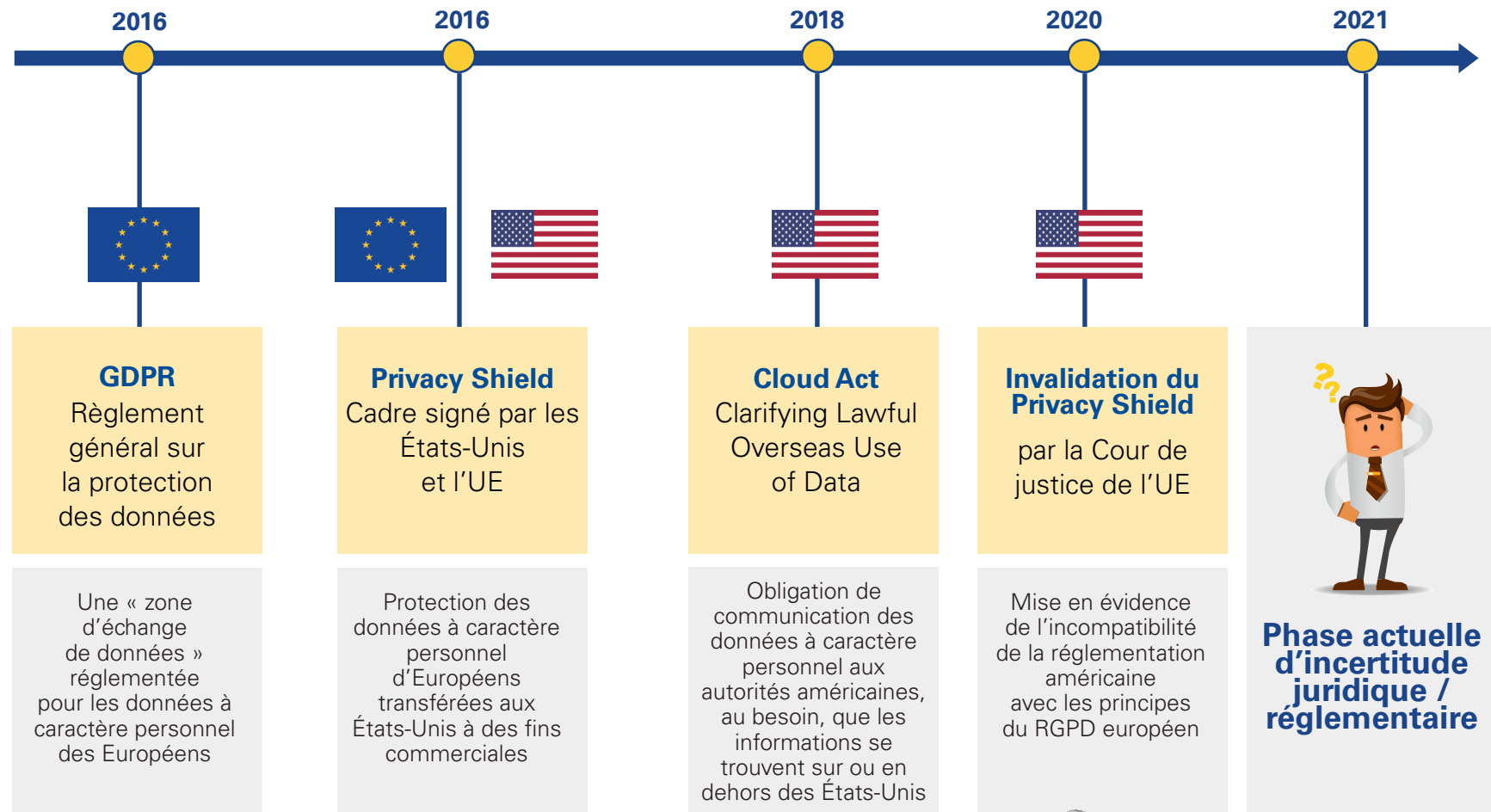
3



Incertitudes sur
la réglementation
des données :
quels sont les
risques pour
les entreprises
européennes ?

Depuis 2016, les nouvelles réglementations sur les données aux États-Unis et dans l'UE ont un impact fort sur le marché du cloud computing

Principales réglementations récentes relatives au marché cloud



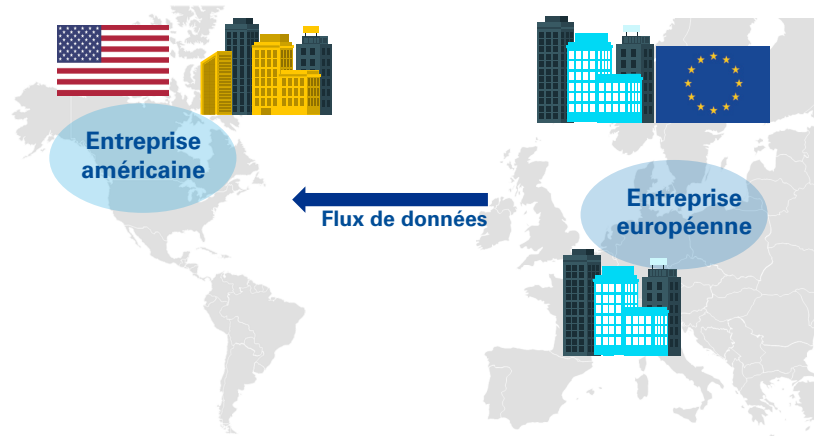
Sources : avocats de KPMG, et recherches et analyses GSG



Voir l'Annexe pour des informations supplémentaires

Ces réglementations cherchent à établir un cadre juridique strict concernant les flux de données européennes impliquant des entreprises américaines (dans et hors de l'UE)

Flux impliquant des entreprises américaines (hors de l'UE)



Ces transferts de données étaient autorisés, car le niveau effectif et adéquat de protection était assuré par le **Privacy**

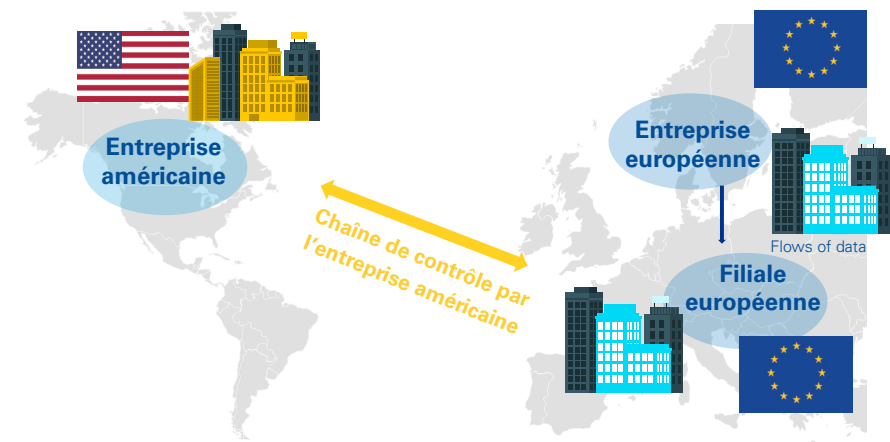
Shield

MAIS



Le 16 juillet 2020, la Cour de justice de l'UE a **invalidé l'accord Privacy Shield**, considérant que les programmes de surveillance américains n'étaient pas compatibles¹ avec les principes du RGPD (affaire Schrems II)

Flux impliquant des entreprises américaines (dans l'UE)



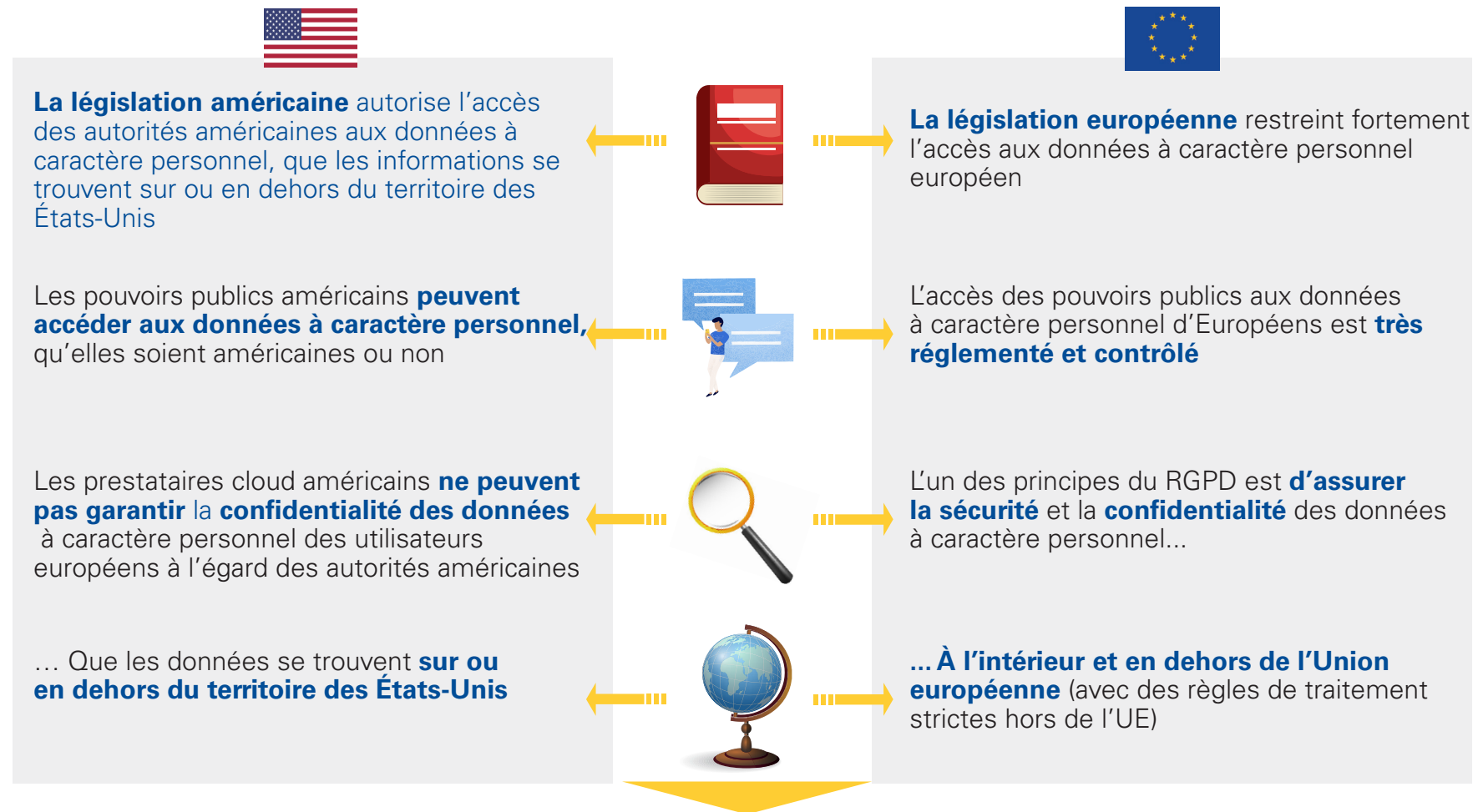
Ces transferts de données sont **autorisés par le RGPD moyennant un contrat de sous-traitance (contenant les clauses contractuelles types) et/ou un contrat conclu entre responsables de traitement conjoints**

MAIS



La législation nationale
(telle que le Cloud Act)
prévaut sur les cadres contractuels

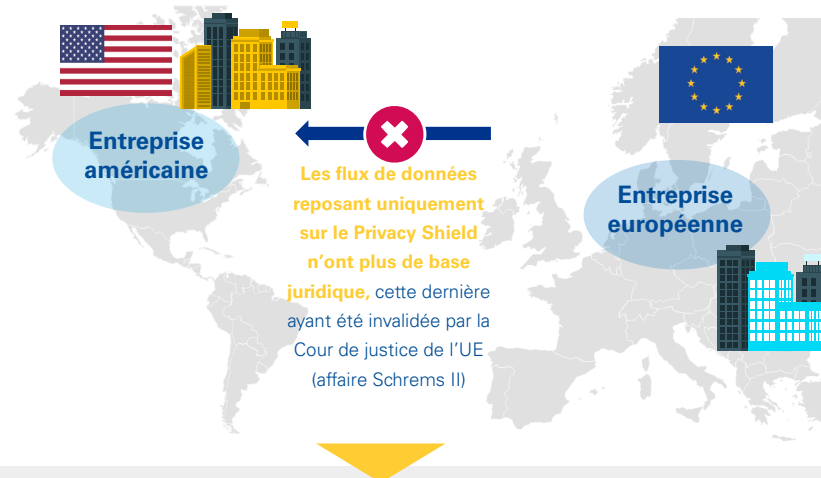
La réglementation américaine en vigueur apparaît fondamentalement irréconciliable avec les principes du RGPD européen, qui visent à protéger les données à caractère personnel des citoyens de l'UE



Cette incompatibilité réglementaire apparaît irréconciliable

Les entreprises transférant des données à caractère personnel d'Européens à des serveurs d'entreprises non-européennes n'ont plus de fondement juridique lié au Privacy Shield et sont ainsi passibles de poursuites judiciaires

En dehors de l'Union européenne



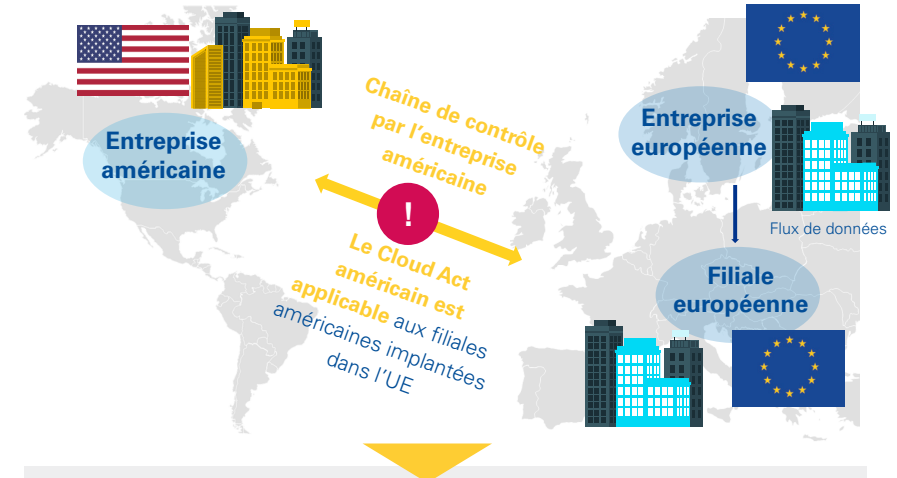
Le **Comité européen de la protection des données (CEPD)** a cherché à dissiper l'incertitude juridique découlant de l'invalidation du Privacy Shield en dressant une Feuille de route de redevabilité portant sur les transferts : **Know Your Transfers (KYT)**, comprenant cinq cas d'usage autorisés et deux interdits¹

L'expérience montre que les deux cas d'usage interdits sont en fait les cas de transferts de données les plus courants

Situation actuelle

L'incertitude juridique subsiste et ne peut être dissipée que par une **évolution de la législation américaine sur la protection de la vie privée**

Au sein de l'UE



La législation nationale prévalant sur les cadres contractuels, **le Cloud Act américain s'applique aux filiales américaines établies dans l'UE :**

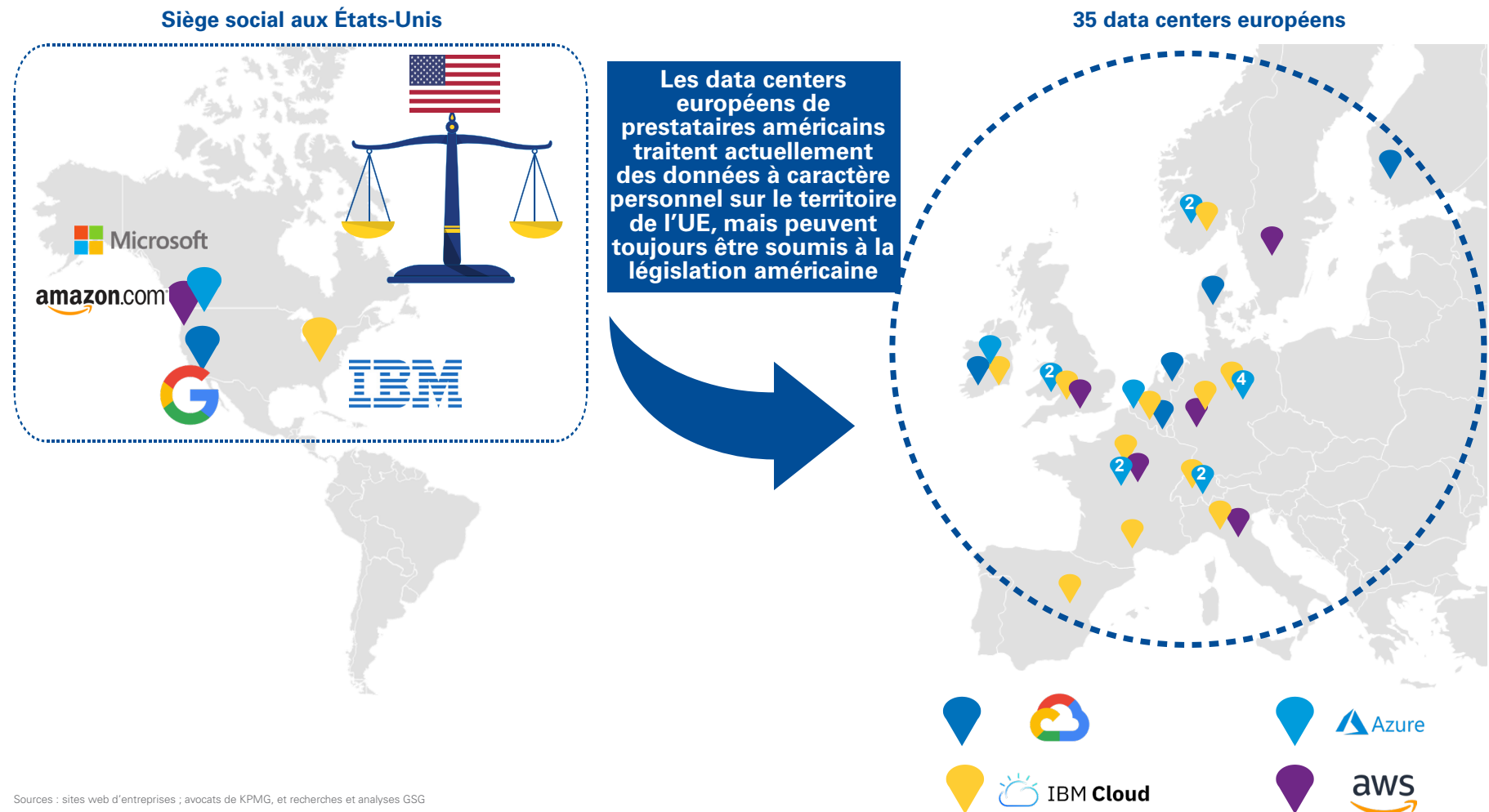
- les pouvoirs publics américains peuvent accéder aux données à caractère personnel détenues par des filiales européennes indépendamment de leur localisation
- les contrats conclus entre le responsable du traitement européen et les filiales européennes peuvent être contestés pour manquement au RGPD

Situation actuelle

Les entreprises soumises au RGPD peuvent être tenues responsables de tout manquement aux mesures de sécurité vis-à-vis des autorités de régulation, des clients et des consommateurs

La localisation des données à caractère personnel des Européens dans des data centers européens de prestataires américains n'en garantit toujours pas la sécurité puisqu'ils peuvent encore être soumis au droit américain

Data centers de prestataires cloud américains en Europe [2020]

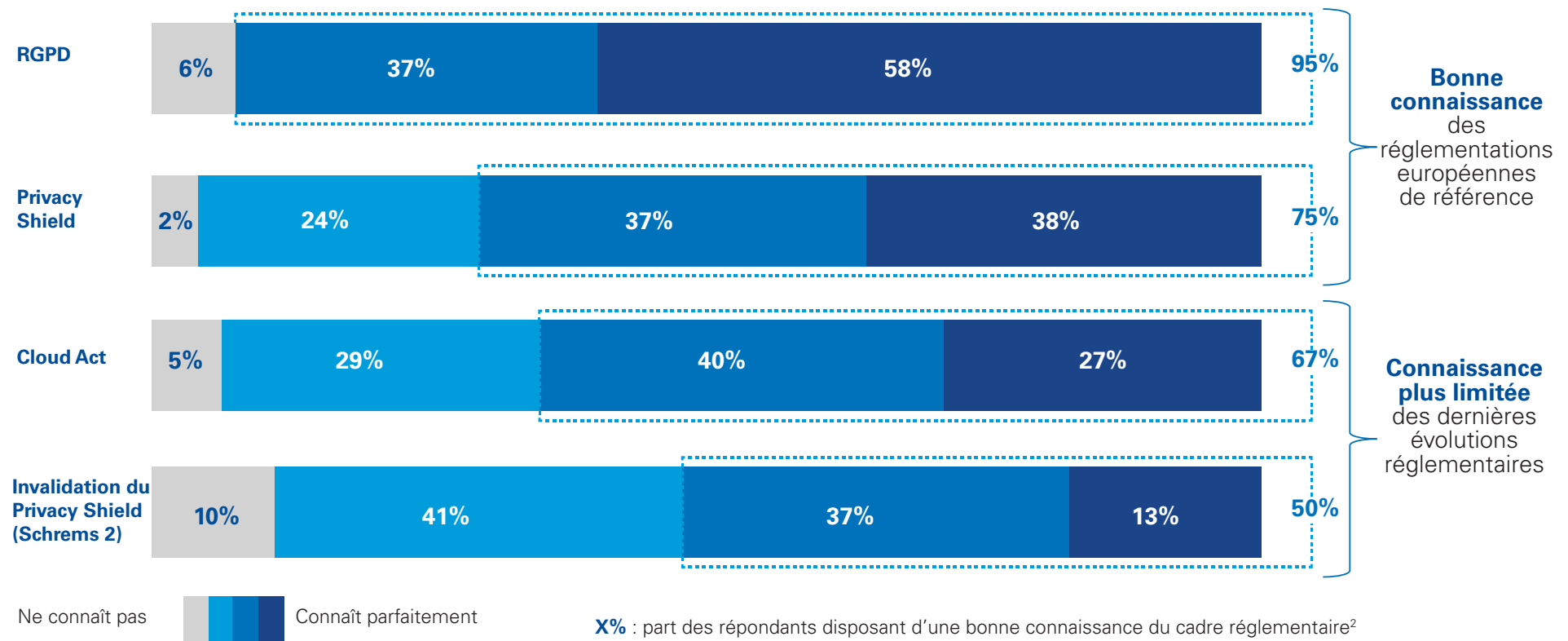


Parmi les décideurs du cloud computing, le niveau de connaissance des réglementations des données est variable (élevé pour le RGPD, mais limité pour le Cloud Act et Schrems 2)

Connaissance des différentes composantes des réglementations des données par les répondants européens



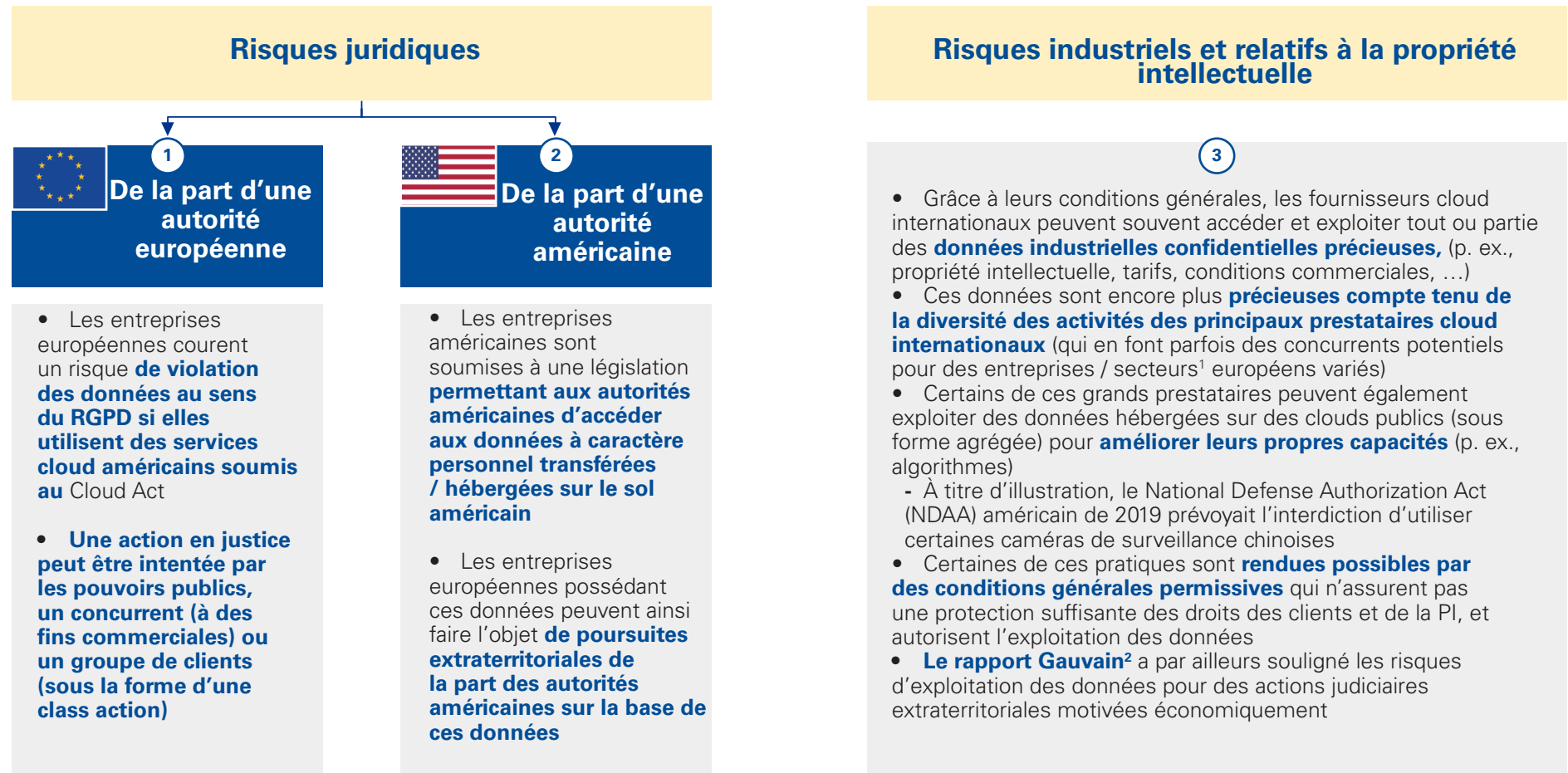
Veuillez préciser votre niveau de connaissance de ces **réglementations**¹



Notes : (1). Réponses recueillies auprès de 200 sondés français et allemands, dont 76 DSI et 124 Directeurs Marketing / Directeurs généraux / Directeurs juridiques / Directeurs opérationnels. En raison des arrondis, la somme n'est pas toujours égale à 100 % (2). Réponses allant de « Connaît bien » à « Connaît très bien »
Sources : sondage GSG ; analyses GSG

L'état d'incertitude actuel présente de multiples risques pour les entreprises européennes

Principaux risques identifiés pour les entreprises européennes recourant à des prestataires cloud américains / non-européens



Dans l'Union européenne, les entreprises ne respectant pas les principes du RGPD courent le risque de fortes pénalités financières (exemple : amende de 50 M€ infligée par la CNIL à Google)

Pénalités financières en cas de manquement au RGPD



De la part d'une autorité européenne

1

Art. 83 du RGPD



Conditions générales pour l'imposition d'amendes administratives

Selon les règles du RGPD, les pénalités financières peuvent s'élever jusqu'à 20 M€, ou représenter jusqu'à 4 % du chiffre d'affaires annuel, mais les sanctions ne sont pas appliquées uniformément dans l'UE

2018-2020

+280m€ d'amendes

160,000+ notifications de violations

Exemple de pénalités financières infligées à Google (2019)



- En janvier 2019, la CNIL¹ française a infligé une **pénalité financière de 50 M€ à Google LLC**, conformément au RGPD, **pour manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité**

« Les manquements constatés privent les utilisateurs de garanties fondamentales concernant des traitements pouvant révéler des pans entiers de leur vie privée »
(Communiqué de presse de la CNIL, 2019)

- Par ailleurs, la CNIL a annoncé la fin du délai de grâce le 31 mars 2021, date à laquelle les entreprises françaises devront impérativement respecter le RGPD



Note : (1). CNIL : Commission nationale de l'informatique et des libertés

Sources : DLA Piper GDPR Data Breach Survey 2020 ; avocats de KPMG, et recherches et analyses GSG

Aux États-Unis, le Cloud Act autorise l'accès des pouvoirs fédéraux aux données stockées dans les pays étrangers, en prévoyant des sanctions en cas de manquement

Principes autorisant l'accès des autorités américaines aux données



De la part d'une autorité américaine

2

Principe



Les données stockées en dehors des États-Unis par un prestataire de services soumis à la loi américaine peuvent être transmises au gouvernement américain sur assignation d'un tribunal

Existence d'accords



Dans le cadre du Cloud Act, et afin de faciliter et réglementer correctement l'échange d'informations, les pays peuvent conclure des **accords exécutifs** avec les États-Unis. Dans ce cas, les deux nations sont en droit de demander directement les preuves électroniques voulues aux fournisseurs, **sans impliquer l'autre gouvernement**.

Pénalités et situations possibles pour les entreprises européennes

Le Cloud Act ne prévoit pas expressément de sanctions en cas de manquement aux injonctions adressées aux prestataires de services. Conséquences potentielles :

Prestataire de services américain avec ou sans filiale en Europe

Les autorités compétentes peuvent se retourner contre le prestataire de services américain. Si une filiale existe en Europe, le prestataire américain exerce, en tant que société-mère, un contrôle sur ses filiales, et ainsi, sur leurs données.

Prestataire de services UE avec filiale aux É.-U.

Les autorités compétentes peuvent seulement se retourner contre la filiale aux É.U. du prestataire de services européen. Cette dernière peut ensuite faire appel devant le juge américain. En outre, celle-ci n'est pas dans l'obligation de fournir les informations si elle n'a ni contrôle juridique, ni accès technique aux données.

Prestataire de services UE sans filiale aux É.-U.

Pas de levier possible contre ces fournisseurs de services car :

- La Commission a précisé¹ que le RGPD exigeait des accords exécutifs (même si les demandes de transfert reposent sur la décision d'un tribunal étranger)
- De plus, les transferts de données à caractère personnel sont soumis à plusieurs autres conditions (p. ex., garanties adaptées)
- Si les prestataires européens respectent une décision d'un tribunal américain alors qu'il n'existe pas d'accords exécutifs entre les États-Unis et le pays de l'UE en question, alors le prestataire sera en violation du droit européen²

De plus, les contrats des fournisseurs cloud américains sont généralement des contrats d'adhésion, ce qui empêche pratiquement toujours les clients d'en négocier les conditions contractuelles

Exemples de dispositions excessives relevées dans les contrats de plusieurs fournisseurs cloud américains

3

Conditions excessives concernant la propriété intellectuelle des clients de prestataires cloud

Plusieurs prestataires cloud américains prévoient des **clauses de licence** obligeant le client à leur accorder **un droit et une licence libres de redevance, mondiaux et non exclusifs** pendant la durée de ses droits de propriété intellectuelle sur l'ensemble des technologies, marques, contenus, informations produites, données, matériaux et autres produits ou informations du client **fournis à ou mis à disposition du prestataire cloud par ses soins**

Ce genre de clause peut être très problématique, puisqu'une licence aussi large :

- est **imposée** par le prestataire cloud américain et **non-négociable** par le client,
- n'est pas toujours limitée à la fourniture du service
- permet au prestataire cloud **d'utiliser, de modifier, de copier et de distribuer les droits de propriété intellectuelle de ses clients** lorsque ces droits sont mis à disposition par le client lors de l'utilisation de services cloud

Conditions excessives concernant les paiements et la résiliation des contrats de prestataires cloud

S'agissant de la possibilité pour les entreprises de changer de fournisseur d'hébergement, plusieurs prestataires cloud et d'hébergement prévoient des **clauses de paiement restant en vigueur à la fin du contrat**. En d'autres termes, les clients se trouvent dans l'impossibilité de résilier ces contrats avant leur terme, et l'intégralité des paiements dus à leur titre survivent à leur résiliation ou à leur expiration.

Ce genre de clause est abusif puisqu'il :

- est **imposé** par le prestataire cloud américain et **non-négociable** par le client,
- prévoit que si le client souhaite résilier le contrat, il sera **toujours redevable de l'intégralité des sommes dues à ce titre**, même pour la période non consommée, étant précisé que dans certains contrats, les sommes dues pour une année peuvent se chiffrer à plusieurs milliers, voire millions d'euros



Nos entretiens montrent que cette situation soulève des craintes multiples pour les entreprises au vu des risques financiers et opérationnels associés (1/2)



CAS DE FIGURE 1 :

Un licenciement est annulé pour des motifs touchant à des données hébergées sur un cloud américain

- Un responsable commercial fournit des **données sensibles à un concurrent**

Dans le procès qu'il intente pour contester son licenciement, l'entreprise se défend en **produisant des données démontrant les manquements du responsable commercial** (accès non autorisé, emails, absence, temps de travail, etc.)

- Ces données sont soit hébergées dans des data centers de prestataires cloud américains, soient générées par des systèmes ou des outils cloud proposés par des fournisseurs américains

- **Ces preuves**, bien que techniquement valables, **peuvent être légalement contestées pour avoir été illégalement recueillies**

- Le juge peut par conséquent estimer que la décision de licenciement est infondée et condamner l'entreprise

CAS DE FIGURE 2 :

Une entreprise européenne ne peut pas agir en justice après le vol de données clients hébergées par des fournisseurs américains

- Une entreprise subit un **vol de données clients** qui étaient stockées et traitées aux États-Unis
- Suite à une enquête, l'entreprise parvient à **identifier les voleurs**, et envisage de **porter l'affaire au tribunal**
- Or l'entreprise constate que les **preuves pertinentes de ce vol de données** sont extraites d'un système de contrôle d'accès **stocké et traité aux États-Unis** alors qu'un tel traitement est dépourvu de base légale

- Les preuves accumulées par l'entreprise risquent fort d'être **contestables, ce qui l'empêchera d'obtenir une juste indemnisation pour ses dommages**. Par ailleurs, elle s'expose à l'invalidation du transfert et donc à la nécessité de redéployer les flux de données, assortie d'un risque d'amende administrative pour manquement au RGPD.



Nos entretiens montrent que cette situation soulève des craintes multiples pour les entreprises au vu des risques financiers et opérationnels associés (2/2)

CAS DE FIGURE 3 :

Les transferts de données à caractère personnel doivent dûment respecter le RGPD (même entre un franchiseur et son franchisé)

- Un groupe de distributeurs franchisés confie au franchiseur le **stockage des données à caractère personnel de leurs clients**
- Le franchiseur se voit accorder un accès à ces données dans le but de mener des **campagnes marketing** (par exemple, par email)
- Le transfert de données à caractère personnel n'ayant pas été assez encadré ou contrôlé, ni le franchiseur ni le franchisé n'ont pu clairement **savoir si un client avait donné ou retiré son consentement** à la réception d'emails pour les campagnes marketing

- **Certains clients portent plainte devant la CNIL, qui condamne le franchiseur et interdit le transfert de données**

- Les franchisés ne sont plus en mesure de conduire leurs campagnes marketing et **peuvent se retourner contre le franchiseur** au titre de leur manque à gagner effectif et prévisible

CAS DE FIGURE 4 :

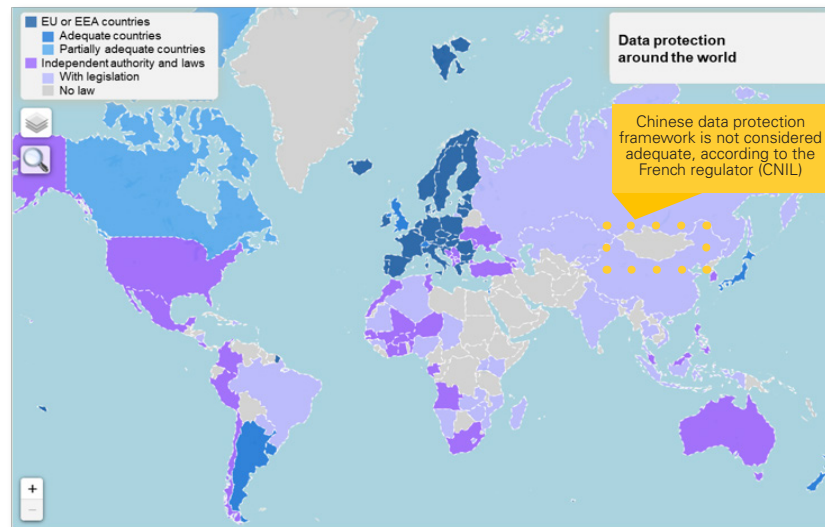
Les citoyens européens ne peuvent plus avoir de garantie sur la sécurité de leurs données de santé

- Une organisation chargée d'une concession de service public prévoyant **l'analyse de données de santé contracte avec un prestataire de services cloud américain pour le stockage de ces données**

- L'autorité déléguée peut adresser une injonction pour **changer d'hôte de données, voire résilier le contrat** sans dédommagement, au motif que les transferts de données de santé à un prestataire américain ne sont pas conformes au RGPD
- Les **citoyens** concernés par ce transfert de données **peuvent agir en justice** contre le délégataire.

Outre les États-Unis, d'autres pays, comme la Chine, prévoient des actions extraterritoriales posant les mêmes problèmes de souveraineté aux Européens

Les transferts de données entre l'Union européenne et la Chine doivent être assortis de mesures de sécurité adéquates...



- La réglementation chinoise **n'est pas jugée** adéquate par l'UE
- Par conséquent, les **transferts de données à caractère personnel** ne sont possibles entre la Chine et l'Union européenne que s'ils sont réglementés au travers de la mise en œuvre d'**outils de transfert** adéquats (par exemple: Clauses contractuelles types ou Règles d'entreprise contraignantes)

... mais n'empêchent pas le gouvernement chinois de mener des actions extraterritoriales pour des raisons de sécurité nationale

Loi chinoise sur la cybersécurité (2017)

- Prévoit des directives visant à maintenir la sécurité du réseau, défendre les droits et les intérêts des personnes physiques et des organisations et promouvoir le développement des technologies, avec :
 - **stockage des données sur le territoire chinois**
 - soumission des organisations et opérateurs de réseau à des **contrôles de sécurité conduits par le gouvernement**

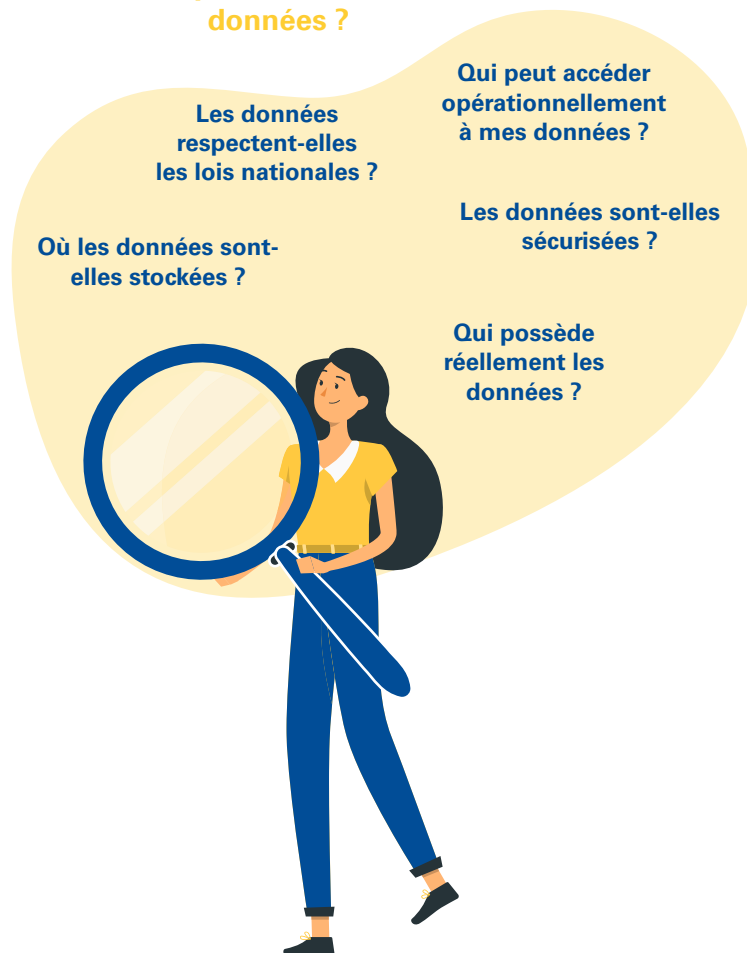
Loi chinoise sur la sécurité des données¹ (2021)

- **Champ d'application** : s'applique à toutes les « activités liées aux données », notamment la collecte, le traitement, le contrôle et le stockage de données touchant à la sécurité nationale, de secrets commerciaux et de données à caractère personnel
- **Application extraterritoriale** : l'Article 2 stipule que la compétence s'étend aux « organisations et personnes physiques situées en dehors de » Chine et exerçant des activités liées aux données et nuisant à la sécurité nationale de la Chine ou à l'intérêt général du peuple chinois

- Les **outils de transfert** qui ont été mis en place **ne semblent pas suffisants** pour protéger les données à caractère personnel des Européens
- Si les prestataires cloud chinois réussissent à gagner des parts de marché en Europe, **les entreprises européennes seront tenues d'accorder la même attention à la réglementation chinoise** que celle qu'elles prêtent actuellement à la réglementation américaine

En conclusion, la souveraineté des données européennes se fonde sur la combinaison d'environ huit critères à considérer comme un tout pour assurer une parfaite conformité et une complète prévention des risques

Qu'est-ce que la souveraineté des données ?



Qu'est-ce qu'un cloud souverain européen ?

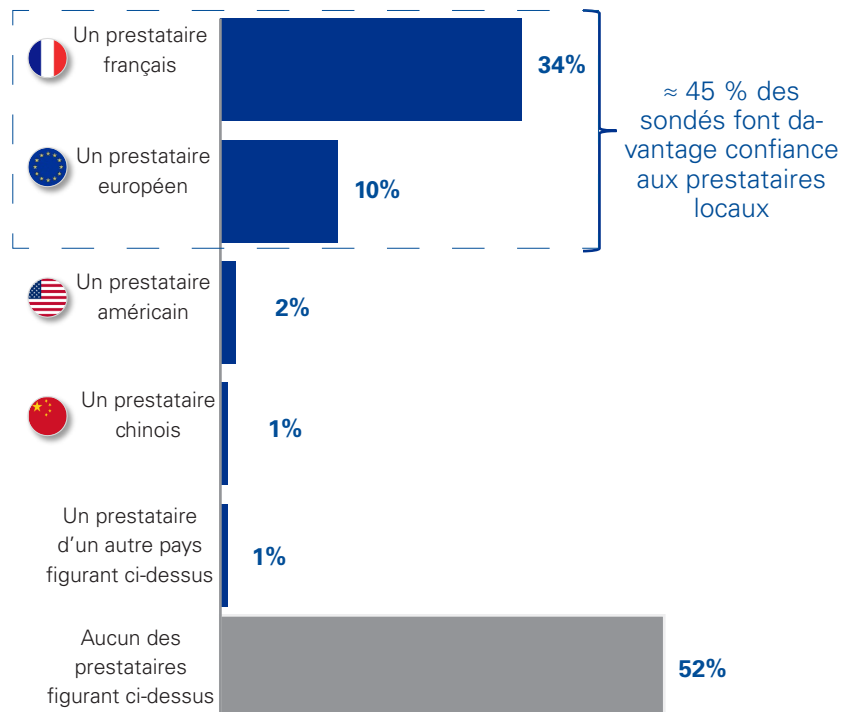
Localisation des données en Europe	- Les données se trouvent dans des data centers de l'Union européenne
Pas d'accès des pays non adéquats aux données	- Les données du prestataire de services sont techniquement inaccessibles aux pays non adéquats (ne respectant pas le RGPD)
Compétence exclusive de l'UE	- Le prestataire de services est exclusivement soumis à la compétence de l'UE et protégé des lois extraterritoriales
Conformité au RGPD pour les demandes d'autorités étrangères	- La politique concernant les réponses aux demandes d'autorités de pays non-UE est appropriée et conforme au RGPD
Pas d'utilisation des données clients	- Le prestataire de services s'engage (dans ses conditions de service) à ne pas utiliser les données clients, même pour optimiser ses services
Sous-traitants souverains	- Les sous-traitants du prestataire de services doivent aussi être souverains en remplissant des critères de souveraineté précis
Soutien européen	- Le support client doit être situé en Europe
Contrats soumis au droit national	- Le contrat signé doit être soumis au droit national

Dans les années à venir, la souveraineté des données va constituer un enjeu commercial du fait des attentes croissantes des consommateurs européens en la matière

Préoccupations des répondants quant à la souveraineté de leurs données



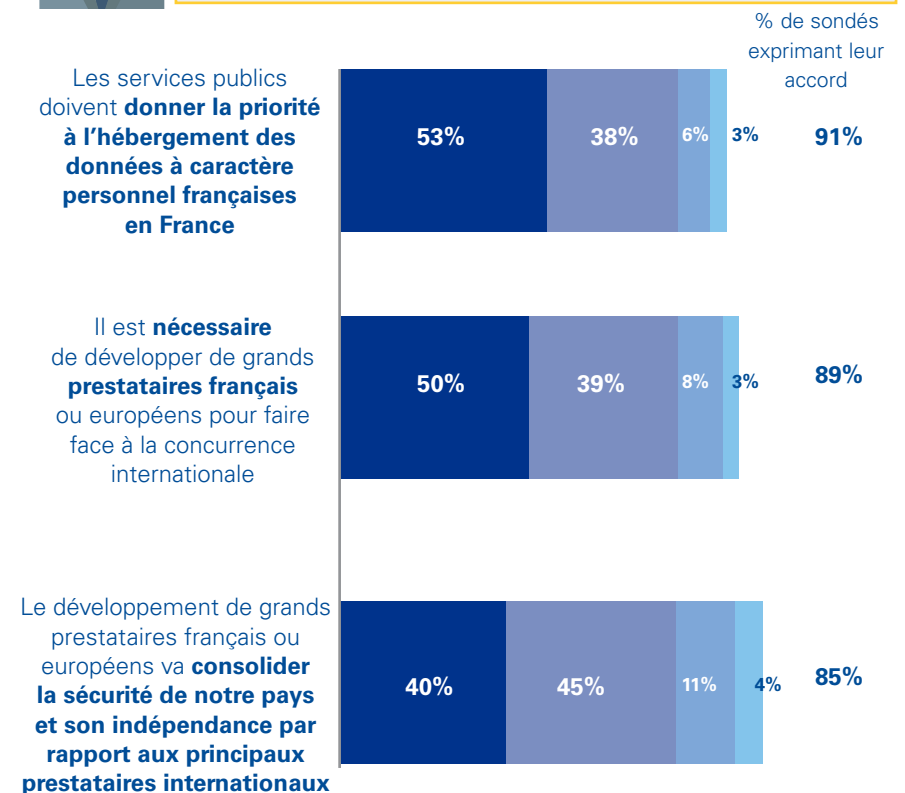
S'agissant de la protection de vos données à caractère personnel, à quel fournisseur faites-vous le plus confiance ?



Attentes des répondants quant à la souveraineté de leurs données



Dans quelle mesure êtes-vous d'accord ou non avec l'affirmation suivante en rapport avec la protection des données ?



Tout à fait d'accord



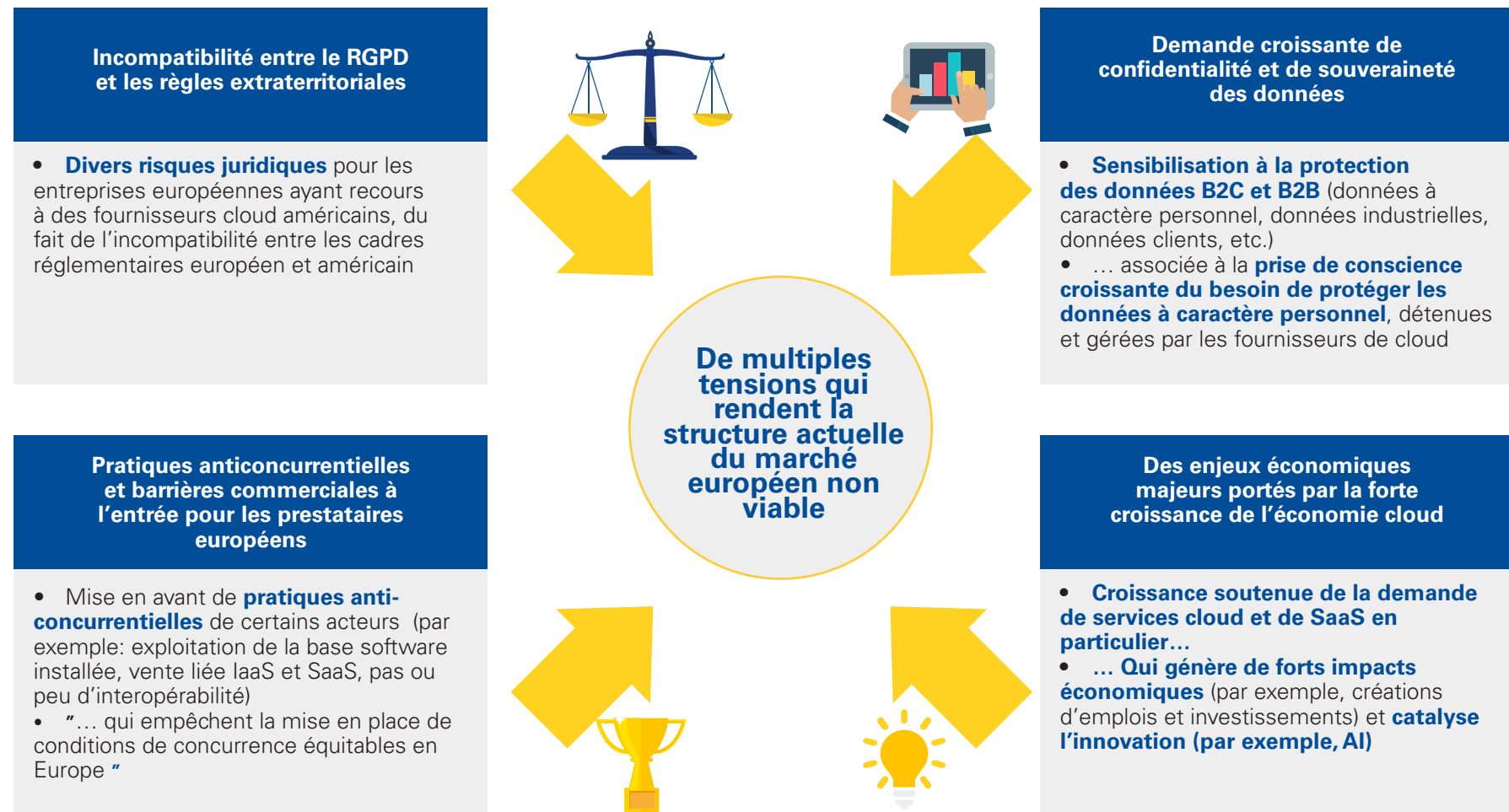
Pas du tout d'accord

4



5 scénarios
pour le futur
du marché
européen du
cloud

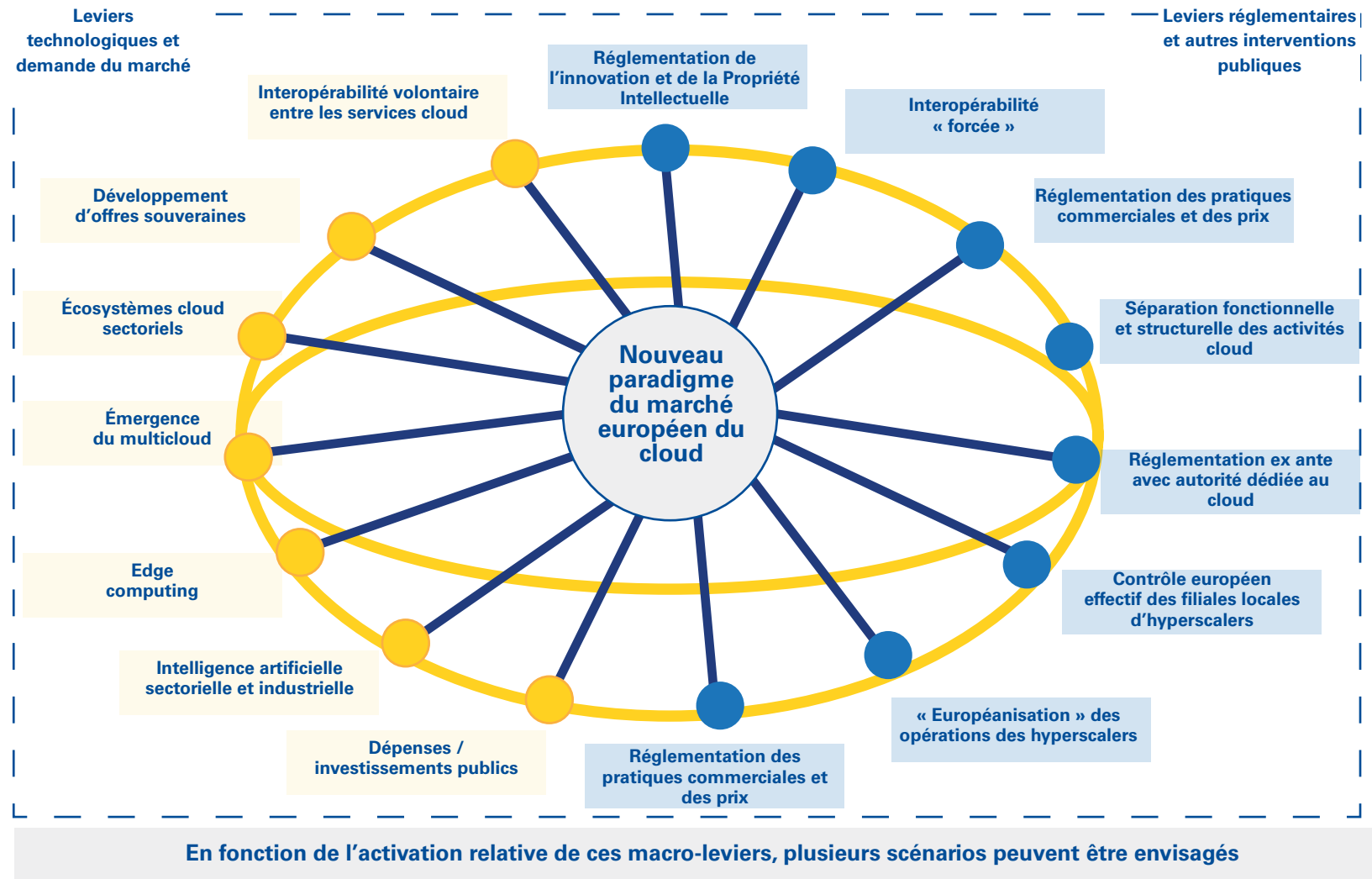
Le paradigme actuel du marché européen n'est pas pérenne, notamment du fait de quatre grands facteurs de marché



Le paysage du cloud computing européen pourrait évoluer suivant un de ces cinq scénarios...



Ces scénarios se caractérisent par la convergence de plusieurs macro-leviers, actionnés les uns par le marché, les autres par les régulateurs



Scénario 1 : le cloud comme bien commun

Leviers

Interopérabilité volontariste entre les services cloud

- **Interopérabilité volontaire** entre les prestataires cloud (en IaaS, PaaS, SaaS) grâce à des **APIs ouvertes**, permettant à tout acteur d'interagir avec les services de fournisseurs cloud, ...
- ... **Freinant ainsi la tendance actuelle aux services cloud propriétaires / non-réversibles**, sans intervention du régulateur pour « forcer » l'interopérabilité

Écosystèmes cloud sectoriels

- **Les acteurs industriels** partageant les mêmes besoins spécifiques de cloud computing convergent autour **d'écosystèmes cloud** communs (généralement sectoriels, par exemple: services financiers, énergie) en fonction de leurs attentes (par exemple: souveraineté, conformité au RGPD)...
- ... Ce qui leur permet de **devenir de facto des fournisseurs de cloud**, et de contourner (partiellement) les fournisseurs cloud internationaux (notamment américains et chinois)

Émergence du multicloud

- Modèle d'architecture cloud permettant de réaliser un seul déploiement cloud auprès de plusieurs fournisseurs de cloud, c'est-à-dire **permettant aux consommateurs de cloud européens de recourir plus facilement à plusieurs fournisseurs cloud...**
- ... Facilitant la mise en conformité au RGPD (plusieurs fournisseurs de cloud pour différents types de données) et limitant le lock-in auprès d'un seul fournisseur

Implications

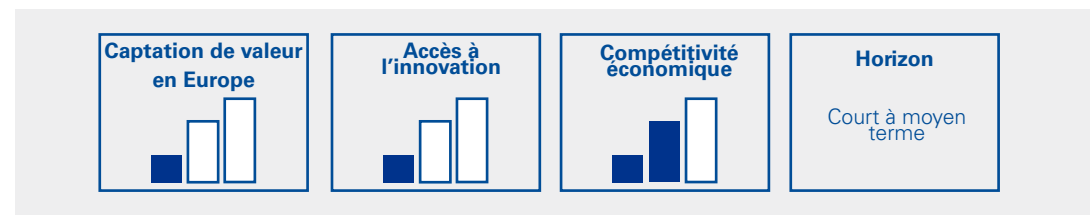
- Le scénario favoriserait la croissance de l'écosystème européen, ce qui va dans le sens du projet européen Gaia-X exemple : avec les APIs ouvertes, potentiel de création d'opportunités commerciales
- **Les consommateurs de cloud** devraient quant à eux bénéficier **d'un déclin du lock-in** (développement de l'interopérabilité et du multicloud, baisse du coût de changement de fournisseur)
- Ce dernier facteur pourrait à lui seul permettre une **croissance relative des fournisseurs de cloud** européens face à leurs homologues internationaux

Rôle dans la transition vers le scénario



Légende : Rôle mineur Rôle majeur

Efficacité du scénario et impacts associés sur les indicateurs économiques des acteurs européens



Légende Faible impact Fort impact

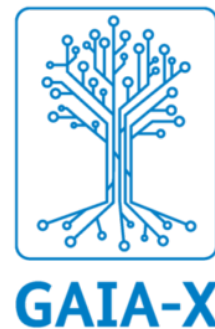
ILLUSTRATION

Ce scénario pourrait se concrétiser grâce à l'initiative européenne Gaia-X, qui vise à favoriser l'échange de données dans un environnement protégé par les lois européennes

#1

Gaia-X est un label de conformité ; ce label ne sera attribué qu'aux solutions répondant exclusivement à un ensemble de critères définis par le conseil d'administration et fondés sur les travaux du comité technique et du comité réglementaire. Les entreprises qui s'appuient sur un service conforme GAIA-X auront l'assurance que les solutions sont **conformes au droit européen**, qu'elles offrent la **portabilité des données**, les **critères les plus élevés de sécurité des données**, une **transparence sur l'utilisation des données** et la **réglementation applicable**, la **garantie de la réversibilité** et **tous les critères pertinents qui reflètent l'objectif de GAIA-X**. Ce label pourra être accordé aussi bien aux membres qu'aux non-membres de l'association GAIA-X.

Toute entreprise cloud (y compris les acteurs non-européens) **peut rejoindre le projet Gaia-X à condition de respecter le corpus de principes et les politiques directrices de l'initiative, qui sont les suivantes :**



Protection des données européennes : adhésion à la législation européenne et capacité à appliquer différents niveaux de protection en fonction du type de données et du cas d'usage

Infrastructure de données ouverte promouvant la transparence et la standardisation des contrats et des procédures, afin de réduire la complexité et les coûts

Libre accès au marché pour que les entreprises des différentes industries puissent échanger facilement les données ce qui stimulerait la collaboration entre les secteurs

Modularité et interopérabilité permises par le rattachement et l'intégration des données des différentes plateformes cloud, éliminant les barrières à l'accès et permettant aux petits services cloud spécialisés de concourir

Scénario 2 : montée en puissance des acteurs européens

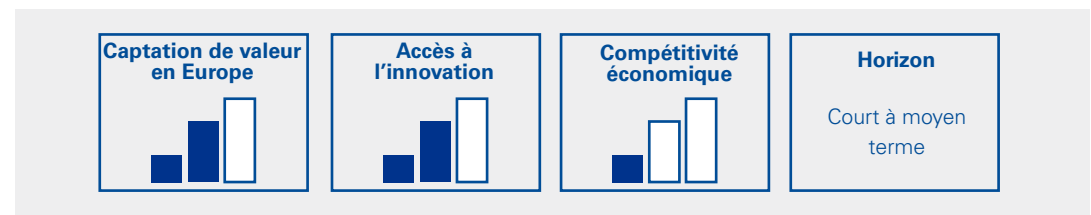


Rôle dans la transition vers le scénario



Légende : Rôle mineur Rôle majeur

Efficacité du scénario et impacts associés sur les indicateurs économiques des acteurs européens



Légende Faible impact Fort impact

ILLUSTRATION

La montée en puissance des fournisseurs européens du cloud pourrait se faire sur différents nouveaux marchés, où un cloud local pourrait être préféré, avec des objectifs associés des autorités européennes

#2

Tendance de marché favorisant la montée en puissance des acteurs européens

Des marchés sous-exploités...



Edge computing

... aux besoins spécifiques...

- Data centers locaux avec de **fortes capacités de calcul** pour un traitement **local** des données générées
- **Infrastructure sécurisée et souveraine** adaptée à l'**hébergement de données industrielles**



Intelligence artificielle pour données industrielles

- Data centers à forte capacité de calcul capables d'exécuter de **puissants algorithmes d'Intelligence Artificielle et de Machine Learning**
- **Écosystème cloud sécurisé et souverain** nécessaire au traitement des données industrielles critiques



Offres souveraines

- **Environnements cloud souverains, sécurisés et certifiés** permettant aux entreprises européennes de **faire migrer leurs données critiques vers le cloud**

... pour lesquels les acteurs européens sont plus pertinents

Pour les données européennes (notamment industrielles critiques), les prestataires européens pourraient mettre en place des **capacités de calcul et de stockage locales et sécurisées** dans un environnement souverain

“Nous vivons le début d'une nouvelle phase marquée par l'essor des données industrielles. Parce qu'elle est le continent le plus industriel, l'Europe doit se positionner en leader dans ce domaine. L'avenir de l'AI est intrinsèquement lié à l'utilisation intense des données : il n'y a pas d'AI sans données”, (T. Breton, oct. 2020)

Proposition de la Commission

Ces tendances de marchés se retrouvent dans l'objectif de la **Commission européenne de créer un Marché unique de la donnée, où les fournisseurs cloud européens** seraient la pierre angulaire.

L'instauration d'un tel marché peut être facilitée par les mesures suivantes :

- **Soutien technologique et financier** pour créer une infrastructure cloud européenne sécurisée et souveraine apte à **héberger et calculer les données industrielles**
- Création d'une **chaîne de valeur de manipulation des données 100 % européenne** et souveraine grâce à une alliance de sous-traitants européens
- Développement de normes et standards d'autorégulations par les acteurs du secteur en Europe, sous la forme d'un **Guide de Réglementation Cloud traitant du système de certification de la cybersécurité, les sujets de concurrence loyale et le code de conduite sur l'efficacité énergétique des data centers**
- D'autres projets, tels que l'**Important Project of Common European Interest (IPCEI)**¹ sur les prochaines générations d'infrastructures et services cloud, devraient contribuer à renforcer efficacement le leadership et la souveraineté des données européennes²

Notes : (1). Dans le cadre IPCEI, les États membres de l'UE ont la possibilité d'élaborer des projets importants d'intérêt européen commun reposant sur une aide d'État autorisée et apportant une contribution majeure à la croissance, à l'emploi et à la compétitivité de l'industrie européenne (2). Projet mentionné en particulier dans la Déclaration conjointe des États membres d'octobre 2020 sur la construction de la prochaine génération de cloud

Sources : Entretiens clients et experts ; KPMG Avocats, Recherches et Analyses GSG ; Commission spéciale « Artificial Intelligence in a Digital Age »

Scénario 3 : puissante vague réglementaire

Leviers

Réglementation ex ante avec autorité dédiée au cloud

- Création d'une **Autorité de Régulation du Cloud** (au niveau européen et/ou national) indépendante, chargée de réglementer le marché du cloud et ses acteurs, d'assurer une protection adéquate des consommateurs, et de préserver la compétitivité économique

Réglementation des pratiques commerciales et des prix

- Réglementation plus stricte** concernant les pratiques commerciales actuelles des hyperscalers, dans l'**objectif de réduire le lock-in / les ventes liées** (p. ex., l'incontournable SaaS + IaaS)
- Réglementation des prix pour prévenir les pratiques d'acquisition client déloyales** (p. ex., migration gratuite) et permettre une **concurrence plus saine**

Interopérabilité « forcée »

- Interopérabilité** entre fournisseurs de cloud, **imposée par le régulateur** avec la mise en place de lois spécifiques (vs. engagement volontaire des participants au marché), en particulier au niveau PaaS / SaaS, grâce notamment à des **APIs ouvertes et documentées**

Réglementation de l'innovation et de la Propriété Intellectuelle

- Réglementation** accrue de l'**innovation basée sur le cloud ou dérivée du cloud** (p. ex., Intelligence Artificielle) pour mieux protéger les compétences européennes en la matière
- Niveau accru de protection en ce qui concerne la Propriété Intellectuelle** pour les entreprises européennes stockant leurs données dans les clouds d'hyperscalers (p. ex., interdiction de réutilisation de certaines données propriétaires)

Implications

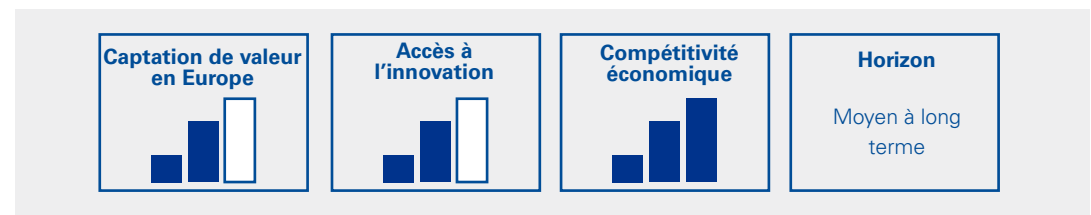
- Ce scénario devrait permettre une **concurrence plus saine** entre les fournisseurs de cloud, et favoriser la croissance des acteurs cloud locaux, grâce à :
 - la diminution des obstacles au changement de fournisseur** pour les consommateurs de cloud, et l'augmentation probable de l'attrition pour les hyperscalers américains suite à la réduction des pratiques de lock-in
 - la redistribution des capacités d'innovation**, par exemple: par l'interopérabilité et la réglementation de l'innovation cloud
- ... mais aussi **accélérer la migration cloud des entreprises européennes** grâce à l'amélioration de la protection des données et l'interopérabilité
- Ce scénario serait **aligné sur le Digital Markets Act** (qui vise à mettre fin aux pratiques d'auto-préférence), à condition qu'il s'applique aux « contrôleurs d'accès » B2C mais également B2B

Rôle dans la transition vers le scénario



Légende : Rôle mineur Rôle majeur

Efficacité du scénario et impacts associés sur les indicateurs économiques des acteurs européens



Légende Faible impact Fort impact

ILLUSTRATIVE

L'Allemagne, l'un des premiers pays de l'UE à adopter de nouvelles lois conformes au RGPD, se montre volontariste avec des premières initiatives



Le Digital Care Act allemand entend réglementer l'usage des données de santé en interdisant leur stockage par des prestataires américains

Une réglementation dédiée aux données de santé...

- En Allemagne, depuis 2020, les applications de santé numérique sont régies par la **Digital Health Applications Regulation**

produisant des règles spécifiques en matière de cloud computing

- Aucunes données de santé collectées par des applications de santé **ne peuvent être transférées hors de l'Union Européenne**
- Le Federal Institute for Drugs and Medical Devices **n'autorise pas les applications stockant des données de santé sur un service cloud appartenant à une entreprise américaine**, même avec des filiales et des serveurs européens



Le 10e amendement du German Competition Act vise à créer un « cadre réglementaire de concurrence numérique »

Une loi contre les restrictions à la concurrence...

- En 2021, mise en œuvre du **10e amendement de la loi contre les restrictions à la concurrence** (Digital Competition Act), traduisant l'intention du gouvernement de créer un « cadre réglementaire de concurrence numérique »

... visant à limiter fortement la dominance sur le marché des géants du numérique

- Une approche réglementaire inédite ciblant un nombre limité de grands « contrôleurs d'accès et intermédiaires » sur les marchés numériques
- Grands principes :**
 - L'**Office fédéral de lutte contre les cartels allemand** (FCO) peut délivrer une ordonnance déclaratoire constatant qu'une entreprise exerce une « **pré-éminence sur les marchés** » compte tenu de plusieurs facteurs (domination des marchés, intégration verticale, puissance financière, accès aux données ou à d'autres ressources)
 - Le FCO obtient **le pouvoir d'interdire préalablement un certain nombre de pratiques répertoriées**, même sur les marchés où l'entreprise n'est pas dominante
 - L'**entreprise supporte la charge de la preuve** pour se défendre
- Type de conduites** que le FCO peut désormais interdire :
 - Auto-préférence lors de la fourniture d'un accès au marché d'approvisionnement et de vente (p. ex., offres pré-installées exclusives)
 - **Obstacle à l'interopérabilité** des produits, services ou données

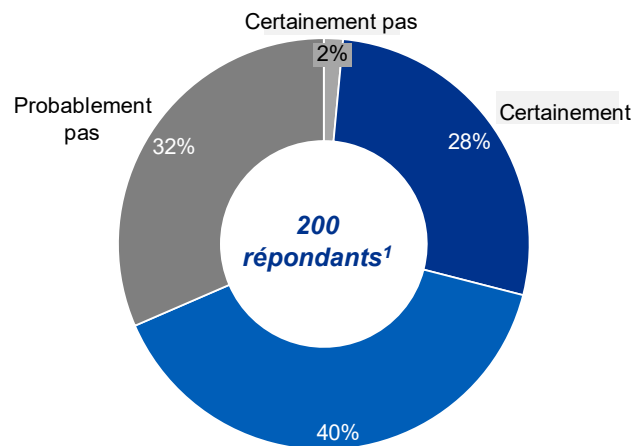
Les résultats de l'enquête montrent que les décideurs s'attendent à un renforcement de la réglementation, qui pourrait les faire basculer vers les prestataires cloud européens



Les attentes des décideurs européen du cloud computing en matière de réglementation et leur choix de fournisseur cloud



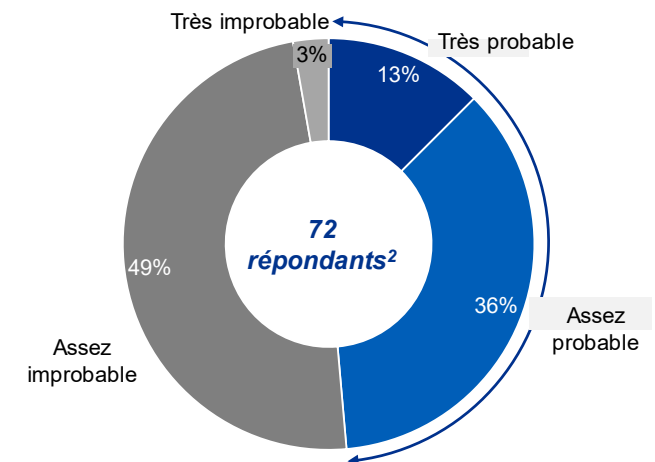
Vous attendez-vous à un renforcement de **la réglementation européenne** dans les 3 à 5 prochaines années ?



68% des interrogés anticipent un renforcement de la réglementation européenne dans un futur proche



Votre entreprise est-elle susceptible de **faire évoluer son choix en faveur de fournisseur de cloud européens** dans les 3 prochaines années, pour des raisons juridiques et/ou marketing ?



49% des interrogés pourraient privilégier un fournisseur cloud européen pour des raisons juridiques ou marketing

Scénario 4 : européanisation des opérations des prestataires cloud

Leviers

« Européanisation » des opérations des hyperscalers

- Dans ce scénario, les fournisseurs cloud non-européens seraient soumis à des réglementations assurant à l'Europe une plus grande part des bénéfices économiques du cloud (p. ex., investissements, capacités R&D locales) et donnant un contrôle accru aux Européens...
- ... qui pourraient prendre la forme d'obligations / incitations locales (dépenses de R&D, présence de la direction générale des hyperscalers, comme cela se fait déjà pour les banques européennes, et chaîne d'approvisionnement (par exemple, composants des data centers), avec un suivi approprié des autorités européennes pour assurer l'efficacité de la création de valeur locale et l'absence d'« UE washing » dans les activités des hyperscalers

Contrôle européen effectif des filiales locales d'hyperscalers

- **Les filiales européennes des fournisseurs cloud internationaux devraient légalement appartenir et être effectivement contrôlées par des entreprises européennes locales** (p. ex., à travers des joint ventures), notamment pour assurer une conformité effective au RGPD...
- **... comme cela se passe en Chine ou dans d'autres pays (p. ex., Russie, États-Unis)**
 - exemple : en Chine, Microsoft Azure et AWS fournissent des services locaux de cloud computing via une joint venture mise en place avec des acteurs locaux

Implications

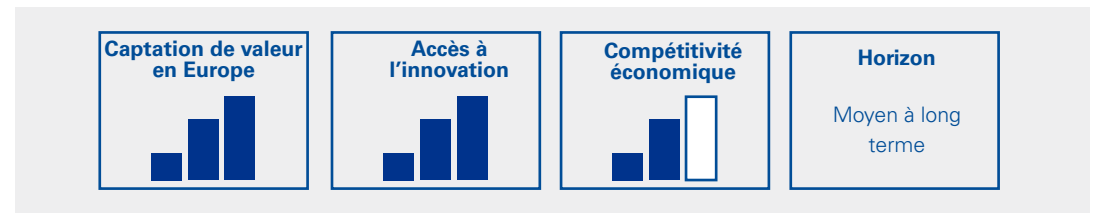
- **La composition des investissements des prestataires non-européens en Europe devrait évoluer**, avec une part croissante de R&D par rapport aux dépenses de capital dans les data centers (qui constituent le gros des investissements des hyperscalers à date)
- **La montée en puissance de l'écosystème cloud européen s'accélérerait** grâce à la porosité de la R&D locale des prestataires non-européens et à la détention des opérations locales des hyperscalers par les européens, **qui garantirait le maintien et la croissance d'un vivier de talents spécialisés dans les technologies du cloud computing en Europe**

Rôle dans la transition vers le scénario



Légende : Rôle mineur Rôle majeur

Efficacité du scénario et impacts associés sur les indicateurs économiques des acteurs européens



Légende Faible impact Fort impact

ILLUSTRATION

Les gouvernements de certains pays (Chine, États-Unis) ont déjà imposé le contrôle par des acteurs locaux d'une partie des activités des fournisseurs de cloud étrangers

#4

La Loi chinoise sur la cybersécurité impose aux prestataires cloud étrangers d'établir un partenariat avec des entreprises locales pour fournir des services aux clients chinois

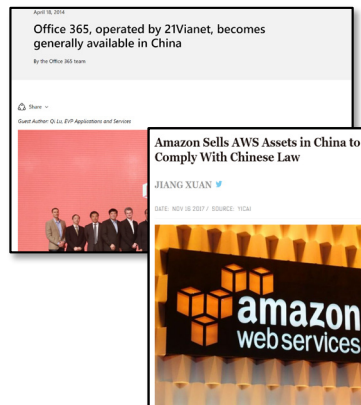
- **La Loi chinoise sur la cybersécurité** adoptée en 2017 et progressivement appliquée et améliorée impose des exigences strictes aux fournisseurs cloud étrangers, notamment :



Localisation des données : toutes les entreprises exerçant des activités en Chine doivent stocker leurs données sur le territoire chinois



Data Centers Internet : les entreprises étrangères ne sont pas autorisées à demander directement des Licences pour des Data Centers, mais peuvent le faire au titre de JV ou de partenariats avec des opérateurs locaux chinois



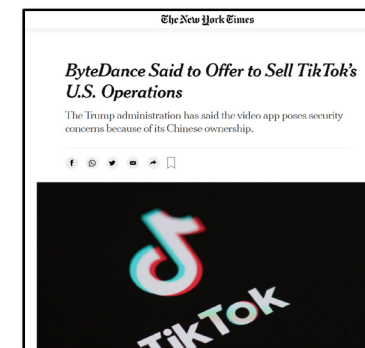
“Dans le cadre d'un contrat de partenariat stratégique, **Microsoft cédera sous licence ses technologies à 21Vianet**, qui devient le fournisseur de services officiel de Microsoft Azure, Office 365 et Dynamics 365 en Chine”

“Pour pouvoir respecter le droit chinois, **AWS a vendu certaines infrastructures physiques à Sinnet**”

Les États-Unis, inquiets du traitement de données par des applications étrangères, envisagent souvent des cessions en faveur d'entreprises américaines

Les États-Unis surveillent de plus en plus près **les applications étrangères pour les données à caractère personnel qu'elles traitent**, en les menaçant de sanctions ou d'interdiction :

- En 2020, **Trump a menacé d'interdire TikTok si elle n'était pas vendue à un acteur américain**, à cause des problèmes de sécurité nationale posés par cette application. ByteDance, propriétaire chinois de TikTok, a ainsi envisagé la cession de sa branche américaine, mais la vente a été mise en pause suite à l'élection de Joe Biden
- En 2020, **l'entreprise de gaming chinoise Beijing Kunlun Tech a vendu Grindr**, un site de rencontres qu'ils avaient acheté en 2016, **après avoir été ordonnée** de le faire par le Comité pour l'investissement étranger aux États-Unis (CFIUS)



“Quelle est la bonne réponse ? Faire racheter TikTok par une entreprise américaine comme Microsoft. C'est du gagnant-gagnant. Cela permet de préserver la concurrence et d'éviter que les données ne tombent entre les mains du Parti communiste chinois,”
(L. Graham, Sénateur républicain)

Scénario 5 : séparation (fonctionnelle ou structurelle) des activités cloud

Leviers

Séparation fonctionnelle des activités cloud

- **Séparation « fonctionnelle » entre les activités cloud des hyperscalers et leurs autres activités** (p. ex., GCP vs la publicité, cœur de métier de Google), avec distinction très nette des effectifs, bureaux, Propriété Intellectuelle, etc., sans changement de propriétaire, ...
- ... Perçue comme un **moyen réglementaire d'améliorer la conformité des pratiques commerciales** (p. ex., interdiction des ventes liées ou du subventionnement de l'activité cloud par le cœur de métier), grâce à une **transparence accrue** sur les liens existant entre les différentes activités des hyperscalers

Séparation structurelle des activités cloud

- Similaire à la **séparation fonctionnelle des activités cloud**, mais avec cette fois un isolement de la branche cloud au sein d'une **entité légale** distincte (en Europe ou au niveau mondial, si jamais ce levier était actionné par un régulateur américain), donc avec un changement possible d'actionnaire pour l'activité cloud...
 - Le levier global peut être envisagé dans le contexte d'une joint venture (voir le scénario 4)
- ... Dans l'esprit d'un certain nombre de propositions formulées par des candidats politiques aux États-Unis (p. ex., E. Warren)

Implications

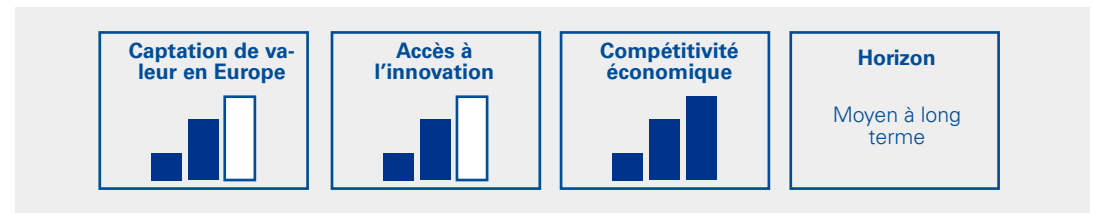
- **Plus grande équité concurrentielle** entre les fournisseurs cloud européens et les hyperscalers, du fait de la perte par ces derniers d'un avantage concurrentiel hérité de leur cœur de métier (p. ex., O365 + Azure pour Microsoft)
- **Les consommateurs de cloud** devraient quant à eux bénéficier d'un **déclin du lock-in** (amélioration de l'environnement du point de vue des pratiques commerciales)

Rôle dans la transition vers le scénario



Légende : Rôle mineur Rôle majeur

Efficacité du scénario et impacts associés sur les indicateurs économiques des acteurs européens



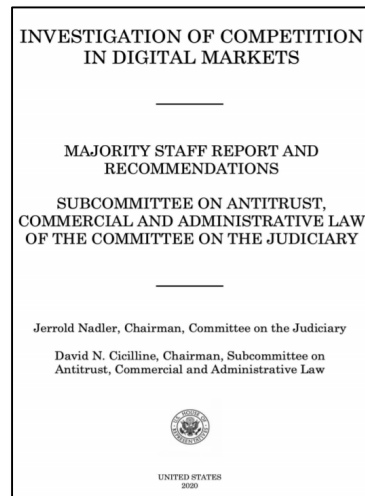
Légende Faible impact Fort impact

ILLUSTRATION

Aux États-Unis, les appels au démantèlement des Big Tech se multiplient, et le besoin s'accroît d'en réduire le pouvoir sur l'économie et la société



Les rapports parlementaires sur la concurrence sur les marchés numériques, axés sur la nécessité d'une réforme antitrust...



Recommandations:

- **Réduction des conflits d'intérêts** grâce à des **séparations structurelles** et des **limitations des lignes de métier**
- Promotion de l'innovation **par l'interopérabilité et l'accès libre** (portabilité des données)
- **Réduction de la dominance sur le marché** par la présomption de fusion

... sont soutenus par un nombre croissant de politiques et de citoyens favorables à un démantèlement



« Ces entreprises seraient **interdites de posséder** à la fois le service de plateforme et les participants de cette plateforme. Les services de plateforme devraient respecter des règles assurant des **relations équitables, raisonnables et non-discriminatoires avec les utilisateurs**. Les services de plateforme **ne seraient pas autorisés à transférer ou partager des données avec les tiers**. » (Sénatrice E. Warren, mars 2019)

« Slack **veut simplement une concurrence loyale et une égalité de traitement**. [...] Slack demande à la Commission européenne d'agir rapidement **pour que Microsoft ne puisse plus continuer à user illégalement de son pouvoir d'un marché à l'autre** en groupant ou en liant des produits. » Extrait de la plainte antitrust déposée par Slack contre Microsoft devant l'Union européenne (juillet 2020)



The New York Times A Leading Critic of Big Tech Will Join the White House

Tim Wu's appointment to the National Economic Council signals a confrontational approach by the Biden administration.



« Ce que fait le gouvernement fédéral, c'est rappeler une règle fondamentale pour toute entreprise : **on n'éteint pas la concurrence avec de l'argent** » T. Wu, nouveau conseiller à la Maison-Blanche et ardent défenseur d'une lutte antitrust agressive contre les géants technologiques américains (mars 2021)

En conclusion, l'avenir du cloud européen pourrait être la combinaison de plusieurs scénarios, chacun procurant ses avantages, à des horizons variés

	Rôle dans la transition vers le scénario				Efficacité du scénario et impacts associés sur les indicateurs économiques des acteurs européens				
	Régl. & gouv. UE	Fourn. cloud UE	Clients indust. UE	Commentaires	Valeur captée en Europe	Accès à l'innovation	Compétitivité économique	Horizon	Commentaires
#1. Le cloud comme bien commun				Rôle clé des prestataires cloud (notamment. européens) pour créer un écosystème répondant aux besoins de l'industrie (par exemple: interopérable)				Court à moyen terme	Captation de valeur locale limitée (tout prestataire peut proposer ces offres), mais bénéfices en matière de compétitivité globale de l'UE
#2. Montée en puissance des acteurs européens				Les prestataires européens s'implantent sur de nouveaux marchés sous-exploités, où les industriels européens ont des exigences fortes				Court à moyen terme	Captation de valeur en Europe, car les besoins industriels (AI, cloud sécurisé) ne peuvent être remplis pour l'essentiel que par des prestataires UE
#3. Puissante vague réglementaire				Changements induits surtout par la création d'une autorité de régulation et l'application d'une réglementation ex ante				Moyen à long terme	Le marché doit s'ouvrir à une concurrence plus saine (fin du lock-in, prix réglementés), avec des avantages en matière de compétitivité
#4. Européanisation des opérations des prestataires cloud				Nécessité d'une réglementation plus stricte en Europe pour améliorer le contrôle de la localisation des données (cf. lois chinoises)				Moyen à long terme	Les fournisseurs internationaux doivent respecter la législation européenne imposant des activités locales assurant le maintien de la création de valeur en Europe
#5. Séparation des activités cloud				Séparation fonctionnelle ou structurelle imposée par le régulateur européen pour instaurer une plus grande équité concurrentielle				Long terme	Des changements structurels doivent promouvoir la concurrence, assurant un meilleur accès à l'innovation et une création de valeur accrue dans l'UE

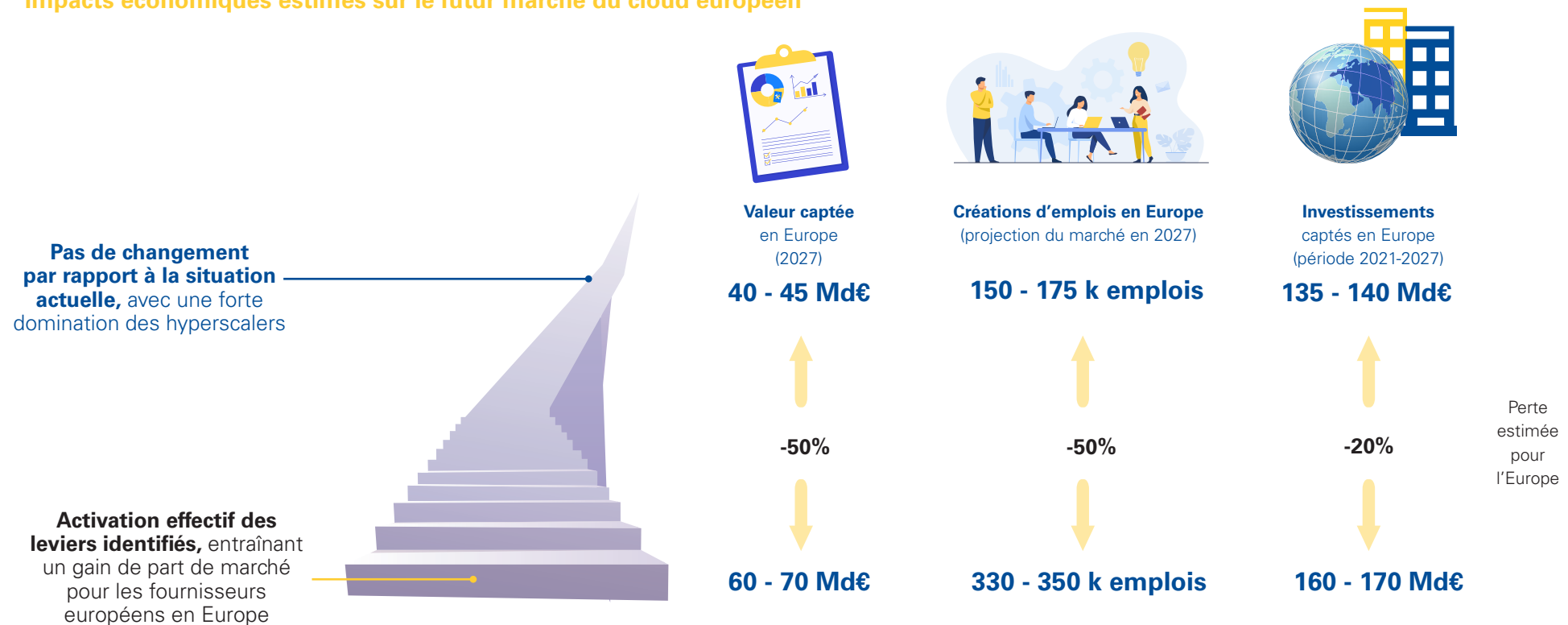
Légende Rôle mineur Rôle majeur

Légende Impact limité Impact marqué

ESTIMATIONS GÉNÉRALES

Si les leviers identifiés n'étaient pas suffisamment actionnés, l'Europe pourrait perdre 20 à 50 % de l'impact économique estimé sur le marché du cloud computing

Impacts économiques estimés sur le futur marché du cloud européen



Les impacts économiques du cloud en Europe (notamment valeur captée, emplois créés et investissements) **pourraient varier** en fonction du ou des scénarios éventuellement mis en place et des leviers activés

5



Pour aller plus loin : bonnes pratiques et initiatives à mettre en place pour les parties prenantes du secteur privé et public

Les défis actuels, conjugués aux incertitudes entourant le futur du cloud européen, représentent des risques pour les parties prenantes clés du marché...

Incertitudes concernant le futur du cloud européen



Répercussions potentielles pour les parties prenantes clés du marché

Pour
les DSI,
Directeurs
Techniques
& Sécurité

Risques associés aux technologies de l'informations :

- Stratégies IT et métier non alignées
- Dépassement des coûts cloud, et perte de l'avantage concurrentiel procuré par le cloud
- Manque d'interopérabilité, lock-in
- Configuration inefficace de l'infrastructure, avec potentielles failles de sécurité associées

Pour
les
Directeurs
Juridiques

Risques juridiques et réglementaires :

- Manquement aux règles du RGPD
- Nécessité de se soumettre aux lois extraterritoriales
- Perte du contrôle sur les données stratégiques

Pour
les
Directeurs
Marketing

Risques associés au marketing et à la relation client :

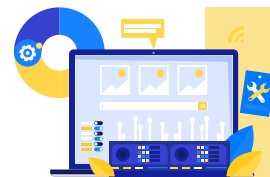
- Utilisation d'applications obsolètes (ventes et marketing), facteur de dégradation de l'expérience client / d'érosion de la réputation
- Perte de clients

Pour
les décideurs
publics

Risques associés à la gestion des données publiques :

- Gestion des données sensibles, avec un soutien des pouvoirs publics et des moyens financiers associés limités
- Sous-exploitation de la valeur créée par l'agrégation des données

...qui peuvent être atténués par des initiatives que les Directeurs SI, Directeurs Juridiques, Directeurs Marketing et décideurs publics doivent mettre en place



**DSI,
Directeurs
Techniques
& Sécurité**

**Maîtrisez l'utilisation réelle
de votre IT**
(données et charge de travail
IT)

**Amorcez un changement
culturel vers une stratégie
cloud plus proactive**

**Réalisez un choix et une
gestion avisés de vos
plateformes cloud**



**Directeurs
Juridiques**

**Identifiez les transferts
de données et évaluez les
outils de transfert**

**Réalisez une évaluation
des risques en cas de non-
conformité au RGPD**

**Vérifier les conditions
de chiffrement
des données**



**Directeurs
Marketing**

**Formulez une promesse
client responsable et
durable**

**Valorisez les certifications
cloud**

**Différenciez-vous
de la concurrence**



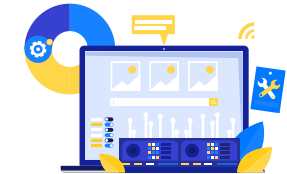
**Décideurs
publics**

**Uniformisez
les politiques
publiques cloud**

**Définissez une politique de
dépenses publiques dédiée
au cloud computing**

**Informez et formez
les décideurs IT
des collectivités locales**

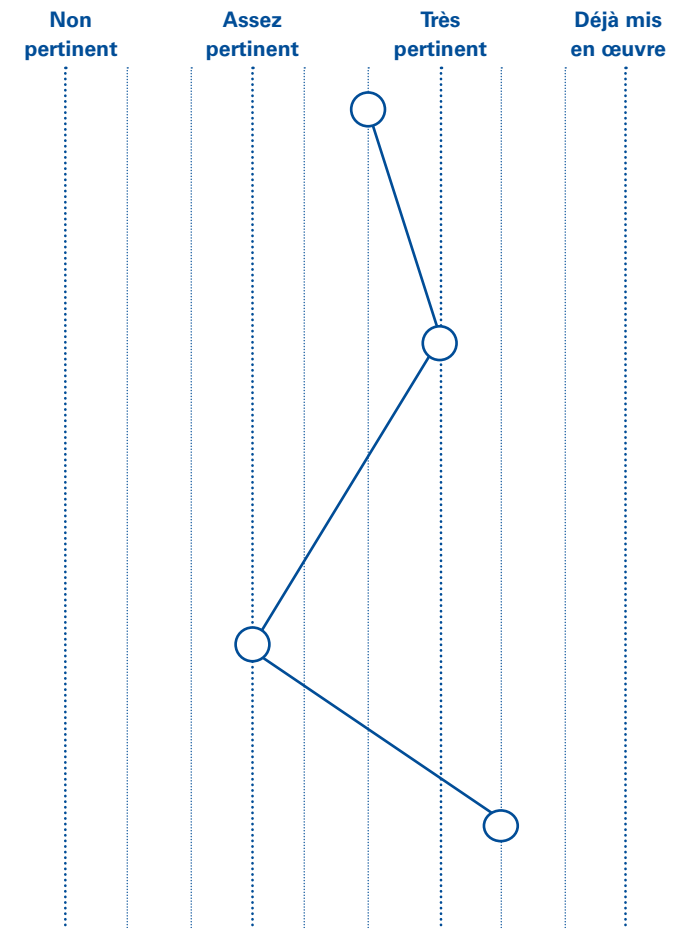
Les DSI, Directeurs Techniques et Directeurs Cybersécurité cherchant à exploiter le potentiel permis par le cloud doivent envisager certaines bonnes pratiques pour opérer une migration conforme et sécurisée



Bonnes pratiques et initiatives à mettre en place par les DSI et autres décideurs IT

Bonnes pratiques	Initiatives
Maîtrisez l'utilisation réelle de votre IT, dont les données	• Classement des données par degré de confidentialité (C1 à C4), avec une attention particulière pour les données à caractère personnel et/ou sensibles • Mise en place de la bonne gouvernance pour l'ensemble du cycle de vie des données par niveau et par type (par exemple: lieu et durée de stockage, accès et autorisation, finalité)
Maîtrisez l'utilisation réelle de votre IT, dont la charge de travail IT	• Évaluation de la charge de travail IT, en étroite collaboration avec les parties prenantes métiers, notamment en ce qui concerne : • Le volume et le type de calcul (CPU, GPU, HPC)² requis • L'évolutivité de la charge de travail (VM, conteneur, non évolutif) • La nature de la charge de travail (fréquence, personnes impliquées, durée, motif, données d'entrée, données de sortie)
Amorcez un changement culturel vers une stratégie cloud plus proactive	• Initiation de plusieurs changements culturels à différents niveaux : • Au niveau RH, avec un recrutement adapté (évolution des postes qui était plus manuels et hardware vers des postes de développement software) • Au niveau IT, avec la nécessité de mettre en place une gestion proactive de la sécurité et d'assurer la résilience cloud dans le déploiement de l'infrastructure
Réalisez un choix et une gestion avisés de vos plateformes cloud	• Réalisation d'une évaluation des prestataires cloud (par exemple: SLA pour situation de crise, souveraineté des données, transferts de données et garanties d'accès) et examen d'une stratégie multicloud permettant de prévenir tout lock-in potentiel • Exploitation des meilleures pratiques de développement software pour traiter votre infrastructure as code (Devops, CI/CD)

Pertinence des initiatives¹



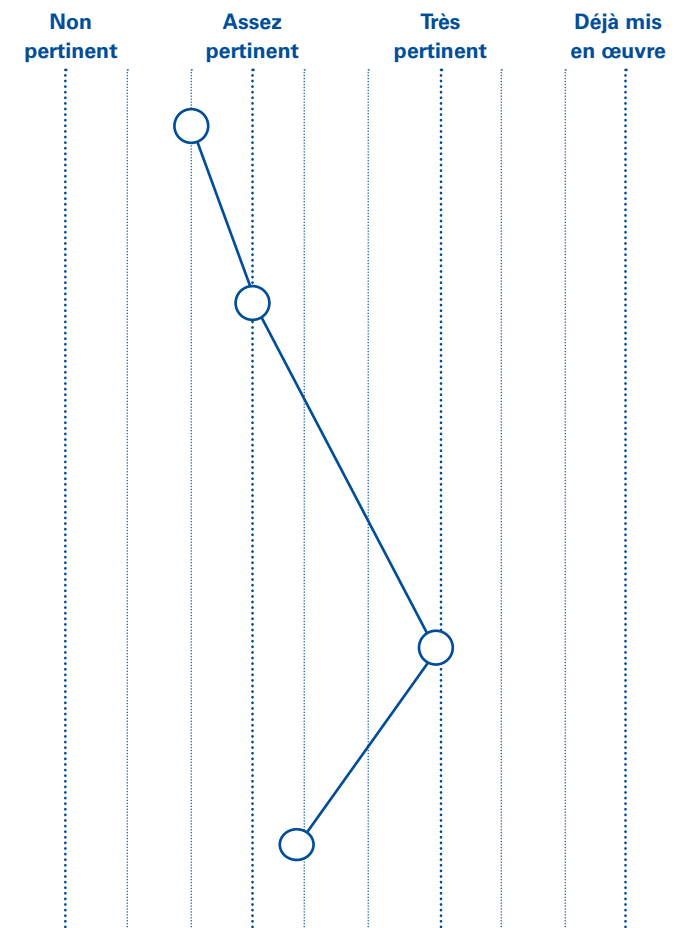
Pour s'aligner sur une réglementation des données changeante et complexe, les Directeurs Juridiques doivent cartographier les transferts de données, évaluer le rapatriement des données et réaliser une évaluation des risques



Bonnes pratiques et initiatives à mettre en place² par les Directeurs Juridiques

Best practices	Initiatives
Identifiez les transferts de données	• Identification des fournisseurs de services établis hors UE ou susceptibles de réaliser des transferts en dehors de l'UE (concernant les processus les plus risqués) • Identification du traitement de données à caractère personnel confié à ces fournisseurs et de la base juridique correspondante (consentement, intérêt légitime, etc.)
Evaluez vos outils de transfert	• Identification des outils de transfert mis en place (décisions d'adéquation, règles d'entreprise contraignantes, codes de conduite, clauses contractuelles ad hoc, mécanismes de certification, etc.) • Analyse des réglementations locales pour savoir si l'outil de transfert RGPD utilisé est efficace en toutes circonstances
Réalisez une évaluation des risques en cas de non-conformité avec le RGPD	• Dans les cas de transferts ou outils non-conformes, évaluation du risque associé (cas d'usage autorisés ou interdits) et de la nécessité de mettre en place des mesures supplémentaires - Cas d'usage autorisés : renforcement de votre contrat (par exemple: clauses de protection des données, règles d'entreprise contraignantes, clauses contractuelles) - Cas d'usage interdits (les plus courants) : rapatriement de vos données dans un pays respectant le RGPD (y compris, évaluations des coûts, du temps requis et des restrictions) • Réaliser régulièrement cette évaluation de risques
Vérifier les conditions de chiffrement des données	• Évaluation des conditions de chiffrement des données (souvent considéré comme un moyen rapide et efficace d'être conforme au RGPD), y compris modalités, pertinence, efficacité et volume de données chiffrées

Pertinence des initiatives¹



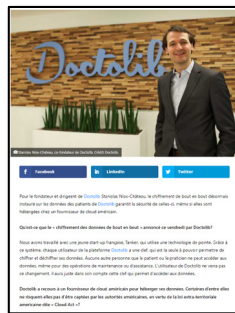
ILLUSTRATION

Au-delà de la conformité réglementaire, le chiffrement peut, dans des conditions très strictes de mise en place, garantir la souveraineté numérique aux entreprises



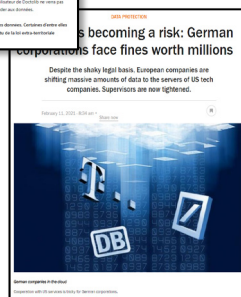
Même si le chiffrement des données fait partie des mécanismes les plus efficaces pour la protection des accès aux données...

- Les technologies de chiffrement, tant algorithmiques (TLS, flux, disques, bases de données...) qu'infrastructures (Key Management Service – KMS, KMS as a service) sont accessibles et s'ajoutent aux couches de sécurité déjà fournies par les technologies et l'infrastructure cloud, **pour protéger les données des atteintes externes et des actes malveillants**



“La protection des **données personnelles** de nos utilisateurs est notre premier devoir. La décision prise aujourd'hui de **généraliser le chiffrement** de bout en bout sur Doctolib en est le meilleur exemple. A partir du moment où vous chiffrez les **données avec des clés** de chiffrement chez un autre hébergeur, l'identité de notre hébergeur de nos données a peu d'importance.”

Directeur général de Doctolib



“Deutsche Bahn a bâti un **concept de chiffrement global très innovant**, permettant une protection complète de nos données sur le cloud.”

Porte-parole de Deutsche Bahn

... sa bonne mise en œuvre est nécessaire pour se prémunir contre l'extraterritorialité des réglementations étrangères

Facteurs clés à prendre en considération pour le chiffrement des données



Notamment s'assurer d'avoir **un stockage et un management des clés de chiffrement indépendant géré par un fournisseur tiers** (deux fournisseurs de services distincts pour le cloud et le KMS), sachant que le KMS proposé par les fournisseurs de cloud **permet la sécurité des données mais n'en garantit généralement pas la souveraineté**



Dédier la mise en œuvre du **chiffrement à des équipes dédiées composées d'experts qualifiés** en mesure de mettre en place une approche approfondie par les risques et une politique de sécurité orientée sur la réduction des risques liés aux accès extraterritoriaux



Gérer le chiffrement des données comme **un projet complexe** avec une **feuille de route de déploiement** précise qui tient compte des **spécificités du système IT de l'entreprise** et des potentiels **coûts élevés associés**

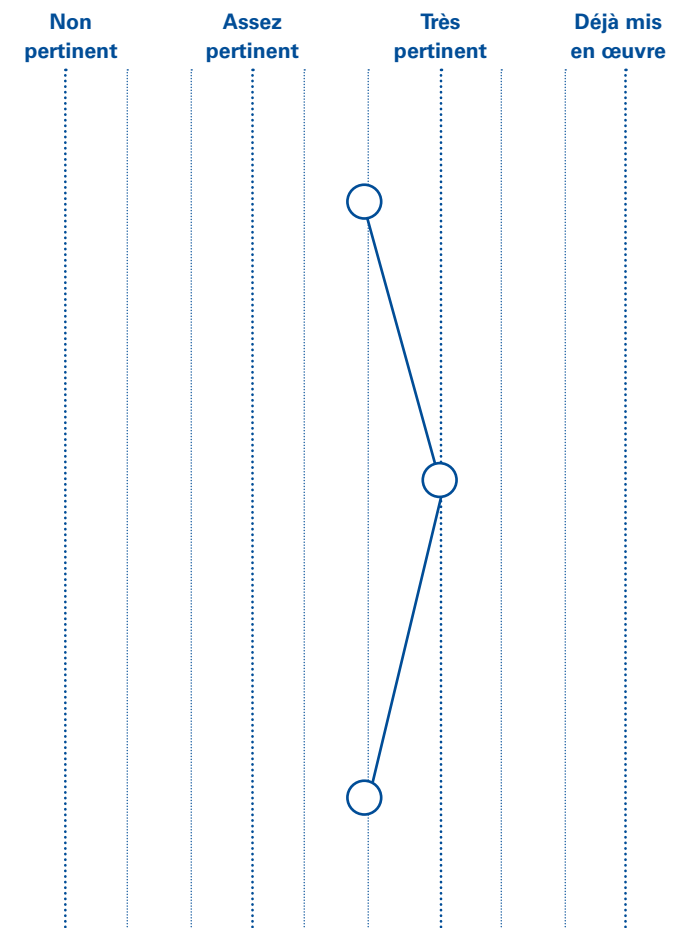
Les Directeurs Marketing ont également un rôle à jouer, notamment en alignant leur proposition de valeur client sur les choix IT en ce qui concerne la protection et la souveraineté des données



Bonnes pratiques et initiatives à mettre en place par les Directeurs Marketing

Bonnes pratiques	Initiatives
Proposez une promesse client responsable et durable en termes de protection des données	• Prise en compte de l'importance croissante de la confidentialité, de la protection et de la souveraineté des données pour les clients et des risques associés si ce n'est pas encore le cas (p. ex., désabonnement client) • Intégration de ces besoins clients dans les choix de politique cloud de l'entreprise (par exemple: critère de souveraineté dans la sélection d'un fournisseur cloud, mise en place de processus adéquats) • Rattachement des choix de protection des données de l'entreprise à la proposition de valeur globale, démontrant aux clients et prospects la valeur accordée par l'entreprise à leurs données... • ... et augmentant les chances de prévenir toute dégradation de l'image de marque, par exemple: en cas de fuite de données à caractère personnel hors UE
Mettez en avant les certifications cloud comme argument commercial	• Pour preuve de l'engagement de l'entreprise, garantie de la sélection par l'entreprise de fournisseurs disposant des certifications adéquates... • ... et communication autour de ces certifications pour démontrer l'engagement de l'entreprise en ce qui concerne les sujets de protection et de souveraineté des données
Différenciez-vous de la concurrence grâce à la stratégie cloud	• Garantie de la conformité effective au RGPD (p. ex., par la conclusion d'un contrat avec un prestataire cloud européen) : moyen de se différencier de la concurrence et de renforcer ainsi la proposition de valeur client • Communication des choix de politique cloud de l'entreprise et valorisation de ces choix comme argument de vente • Identification d'applications cloud native sophistiquées pour le marketing (p. ex., gestion des campagnes marketing) et les ventes (par exemple: CRM)

Pertinence des initiatives¹



Notes : (1). Réponses recueillies auprès de 76 DSI français et allemands invités à répondre à la question suivante : « D'après vous, serait-il pertinent pour votre entreprise de mettre en œuvre l'une de ces actions ? »

Sources : Entretiens experts ; Sondage GSG ; Analyses GSG

Les décideurs publics peuvent encourager la digitalisation et la migration cloud, notamment à travers la standardisation des politiques publiques en termes de cloud



Bonnes pratiques et initiatives à mettre en place par les décideurs publics¹

Bonnes pratiques	Initiatives
Uniformisez les politiques publiques cloud	• Définition de directives pour les politiques cloud au niveau national et local, et élaboration d'une feuille de route associée, afin de : - Accompagner les décideurs publics locaux dans l'identification de leurs données sensibles, notamment en fournissant des exemples concrets (e.g. données de santé, données RH à caractère personnel) - Mutualiser les besoins locaux concernant la migration vers le cloud, pour assurer une approche cohérente et limiter les coûts
Définissez une politique de dépenses publiques dédiée au cloud computing	• Allocation de dépenses publiques massives sur le long-terme pour soutenir la montée en puissance de fournisseur de cloud européens (p. ex., migration de toutes les archives publiques numérisées vers des fournisseurs cloud européens)
Informez et formez les décideurs IT des collectivités locales	• Information des décideurs IT locaux / décentralisés sur les options souveraines et locales possibles pour la migration cloud avec des fournisseurs européens pour : - limiter les inquiétudes portant sur la migration cloud - assurer une migration cloud locale / européenne vers des clouds publics souverains • Formation des décideurs IT locaux à la nécessité de classer leurs données et à la possibilité d'engager une migration cloud (pour des raisons de coût, de sécurité et de flexibilité) pour les données qui ne sont pas qualifiées de sensibles

Exemple : smart cities et données publiques

- **Les données forment l'un des prérequis majeurs à l'émergence des smart cities**, pour lesquelles il convient de clarifier :
 - **qui détient** les données produites
 - **qui peut y accéder**
- Le principal défi des smart cities consiste à **agréger des données provenant de sources variées** : différents réseaux (eau, gaz, électricité), dispositifs connectés (IOT) au sein du mobilier urbain, etc.
- À ce titre, **la gouvernance des données est clé**
 - **L'open data et le cloud computing**, s'ils sont bien appréhendés, peuvent être considérés comme de réels catalyseurs



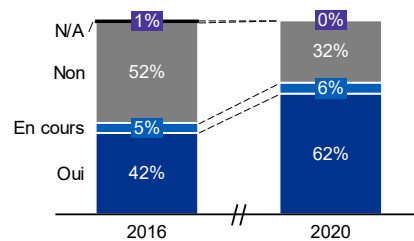
Note : (1). Par exemple, collectivités locales et régionales
Sources : Entretiens experts ; Sondage GSG ; Analyses GSG

ILLUSTRATION

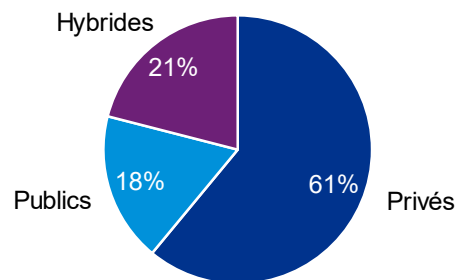
L'adoption lente du cloud par les collectivités locales, notamment due à des freins juridiques et fiscaux, souligne le fort potentiel des fournisseurs cloud locaux, et plus globalement, de l'edge computing

Un rythme d'adoption qui reste lent...

Utilisation de services cloud (au moins un) par les collectivités locales / régionales en France
- 2016-2020, % -



Décomposition des services cloud utilisés par les collectivités locales / régionales en France
- 2020, % -



... du fait de différentes barrières

- **Barrières juridiques**, levées seulement récemment⁽¹⁾, qui interdisaient jusqu'alors l'hébergement de données publiques dans des data centers implantés en dehors du territoire français
- Préférence des collectivités locales / régionales pour l'investissement dans des data centers propres plutôt que dans le IaaS, pour deux raisons :
 - **Sensibilité des données** à héberger (p. ex., données des citoyens)
 - **Vision à long-terme de la politique publique**, renforçant la pertinence des investissements par rapport à la location cloud

« Notre organisation comptable actuelle favorise les budgets d'investissement (CapEx) à ceux d'exploitation (OpEx) »
Responsable du département Infrastructure technique d'un organisme public français

- Bien que l'usage du IaaS soit très limité, **le recours au SaaS s'est répandu** pour les applications ne faisant pas partie des missions essentielles des collectivités

... que les acteurs du cloud doivent adresser

- Même si les collectivités locales vont probablement conserver une partie de leur infrastructure on-premise, la **levée des obstacles juridiques offre la possibilité aux acteurs du cloud de prendre des parts de marché** sur l'on-premise
- La sensibilité des données devrait également rester une préoccupation forte, à laquelle répond en partie le recours à des **fournisseurs cloud locaux**, parfois perçus comme plus fiables par les collectivités locales
- Il est néanmoins possible que les collectivités locales veuillent privilégier une **mutualisation des investissements dans des installations cloud locales**
- Ces éléments s'inscrivent dans la **récente stratégie cloud de l'administration française (mars 2021)**, qui souligne l'importance de la sécurité des données, de la souveraineté numérique, du choix de fournisseurs cloud compétents, ainsi que la nécessité pour l'État de soutenir le secteur du cloud

6



Annexes -chapitre 1

Abréviations et terminologie employées

Terminologie	Définition
API	Application Programming Interface : technologie permettant de faire communiquer différents softwares entre eux.
Baremetal cloud	Serveur physique mis à la disposition d'un client unique, disposant d'une stabilité et des performances de calcul élevées.
BYOL	Bring Your Own License : pratique permettant à des applications SaaS de fonctionner sur des environnements cloud autres que ceux du fournisseur SaaS.
Cloud computing	Hébergement de données et d'applications sur des serveurs physiques, accessibles par Internet.
Cloud hybride	Coordination des services cloud de fournisseurs de cloud public et privé en vue de la création d'un nouvel environnement cloud.
CRM	Customer Relationship Management : software dédié à la gestion des relations et des interactions avec les clients.
ERP	Enterprise Resource Planning : software dédié à la gestion des principaux business process des entreprises (ex., achats, distribution, comptabilité, ressources humaines).
Hosted private cloud	Infrastructure privée hébergée et gérée par le fournisseur cloud.
Cloud hybride	Coordination des services cloud de fournisseurs de cloud public et privé en vue de la création d'un nouvel environnement cloud.
IaaS	Infrastructure as a Service: modèle de service de cloud computing basé sur la location d'un accès à la capacité de stockage et de calcul sur des serveurs physiques.
IOT	Internet Of Things: objets physiques connectés à Internet via des capteurs embarqués.
PaaS	Platform as a Service: modèle de service de cloud computing basé sur la location d'accès à des plates-formes de développement de logiciels.
Cloud privé	Environnements cloud dédiés à un client / propriétaire disposant d'un accès totalement isolé.
Cloud public	Environnements cloud au sein de serveurs appartenant à un fournisseur de cloud et partagés entre différents clients/entreprises.
SaaS	Software as a Service : modèle de service de cloud computing basé sur la location d'un accès à une application en ligne (ainsi qu'aux plateformes et infrastructures sous-jacentes).
Virtual Networking	Technologie permettant la création d'une infrastructure privée complexe en connectant plusieurs réseaux privés sécurisés.
Virtual private server	Serveurs virtuels destinés à héberger des sites web et des applications, basés sur un stockage des données sur des machines virtuelles dédiées aux utilisateurs.

Abréviations et terminologie employées - Courbe Gartner Hype cycle (1/2)

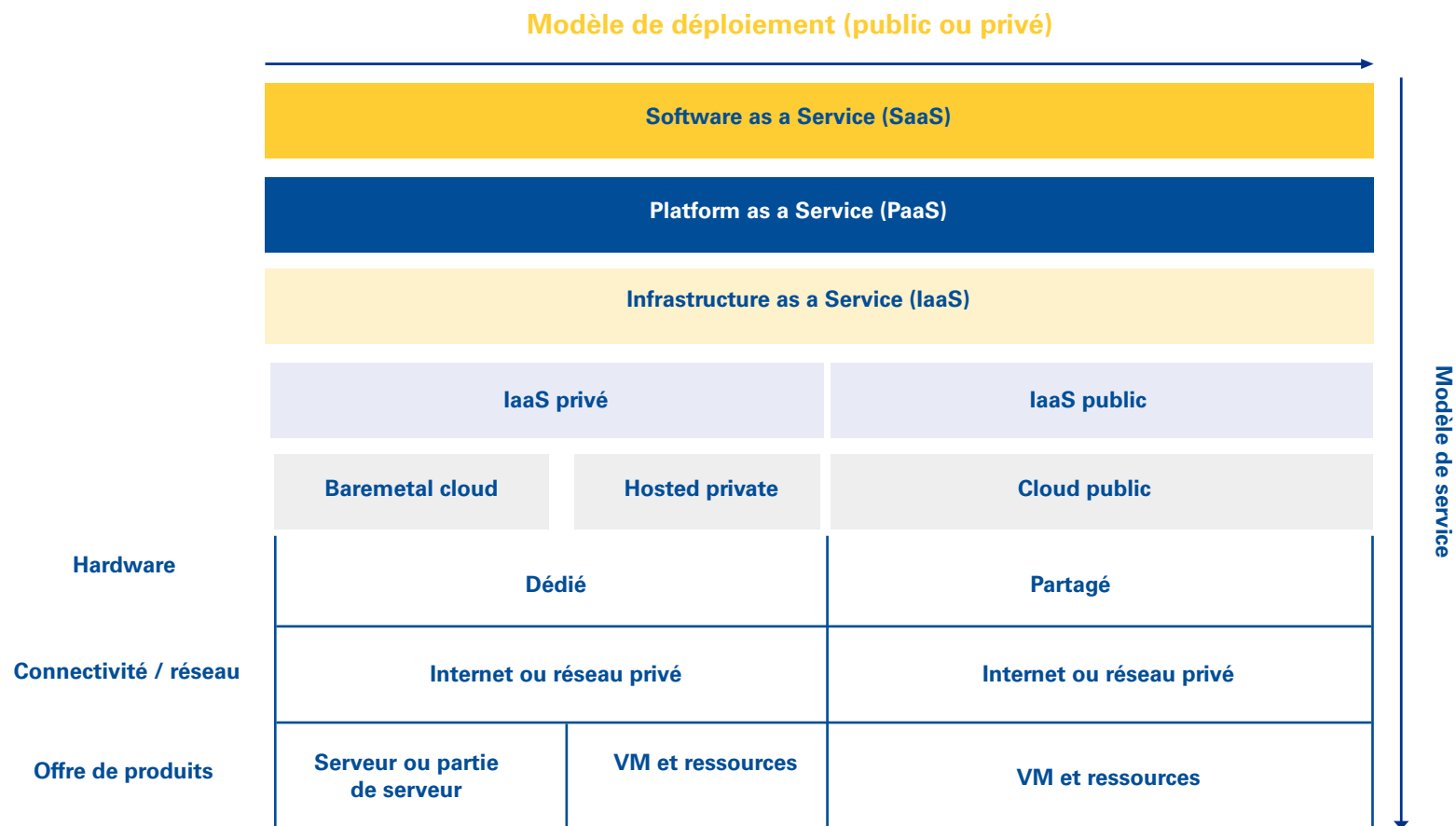
Terminologie	Définition
API Gateway	Plateforme de centralisation d'API chargée d'acheminer les appels vers le microservice approprié avec routage des demandes, composition et traduction des protocoles.
Application PaaS	Service de plateforme cloud fournissant des environnements de développement et de déploiement d'applications.
Blockchain PaaS	Ensemble de services de plateforme logicielle blockchain proposés dans le cloud par un fournisseur cloud pour des souscripteurs
Cloud management platforms	Plateforme permettant à une entreprise de gérer des services et ressources de cloud privé, cloud public ou multicloud.
Cloud marketplaces	Boutiques en ligne dans lesquelles les clients peuvent rechercher et souscrire à des offres de services cloud, notamment IaaS, PaaS et SaaS.
Cloud migration	Processus consistant à préparer et exécuter la migration d'applications ou de charges de travail d'une infrastructure on-premise vers des services cloud externes, ou entre différents services cloud externes.
Cloud Networking	Service proposé par les fournisseurs de services cloud pour connecter des environnements cloud IT hybrides désagrégés, assurant une interconnectivité robuste entre les data centers cloud externes et les data centers on-premise du client.
Cloud office	Collection des suites d'outils SaaS de productivité personnelle, de collaboration et de communication (ex., emails, partage de fichiers, gestion et édition de documents).
Cloud Security assessment	Évaluation de sécurité formelle réalisée par un évaluateur indépendant.
Cloud Tethering	Un modèle de déploiement d'applications dans lequel une application déployée sur un appareil est liée au service cloud du fournisseur pour l'octroi de licences.
Cloud to Edge Development Support	Décrit l'élargissement des modèles de programmation des fournisseurs cloud et leur utilisation sur des dispositifs de Edge, tels que pour les objets IOT.
Cloudbursting	Utilisation alternée de différents services de cloud public ou privé afin d'augmenter et de gérer les pics d'utilisation des systèmes IT au démarrage ou en cours d'exécution.
Cloud-testing tools & services	Technologie cloud destinée à prendre en charge les tests effectués depuis ou dans le cloud (y compris la gestion de laboratoire basée sur le cloud, la virtualisation des services, les outils de test fournis à la demande et les clouds de terminaux).

Abréviations et terminologie employées - Courbe Gartner Hype cycle (2/2)

Terminologie	Définition
Container Management services	Software prenant en charge la gestion de conteneurs à grande échelle dans des environnements de production.
Edge Computing	Topologie informatique distribuée dans laquelle le traitement des données s'effectue à proximité des objets ou des personnes les produisant / consommant.
Expense management	Pratique consistant à examiner et à rapprocher les coûts de services fournis par les fournisseurs de cloud à l'aide d'un outil de suivi.
Hyperscale Computing	Ensemble de modèles architecturaux permettant de livrer des capacités IT évolutives à une échelle industrialisée massive.
Immutable Infrastructure	Modèle architectural dans lequel le système et l'infrastructure d'applications, une fois instanciés, ne sont jamais actualisés sur place.
IOT Platform	Software permettant le développement, le déploiement et la gestion de solutions qui se connectent et traitent les données des points finaux IOT.
Machine Learning	Discipline qui vise à résoudre des problèmes opérationnels en appliquant des modèles mathématiques capables d'extraire des renseignements et des tendances / pattern à partir des données.
Multicloud	Utilisation de services cloud provenant de plusieurs fournisseurs de cloud public.
Private PaaS	Un type de PaaS qui offre un accès exclusif à une entreprise cliente. Le PaaS privé peut être établi, par l'entreprise cliente, on-premise ou hébergé sur un IaaS public.
Public Cloud Storage	IaaS fournissant des services de stockage de blocs, de fichiers et/ou d'objets via différents protocoles.
SaaS Administrative ERP	ERP administratif spécialisé dans la gestion financière, la gestion du capital humain (HCM) et les achats indirects. (Sont exclus l'hébergement distant, où la propriété revient au client, ou le cloud privé).
Serverless PaaS	PaaS fourni avec des caractéristiques sans serveur. Le «serverless» est une manière de fournir un service informatique dont les ressources sous-jacentes sont opaques, ne nécessitent aucun préprovisionnement et sont facturées à l'usage.
Software-defined infrastructure	Englobe un large éventail de composants d'infrastructure software-defined (ex., Software-defined data center SDDC IP, SD-edge des adaptateurs, moniteurs, passerelles, appareils et machines basée sur le Edge).

Les offres cloud disponibles sur le marché se différencient selon deux dimensions distinctes : les modèles de déploiement et les modèles de service

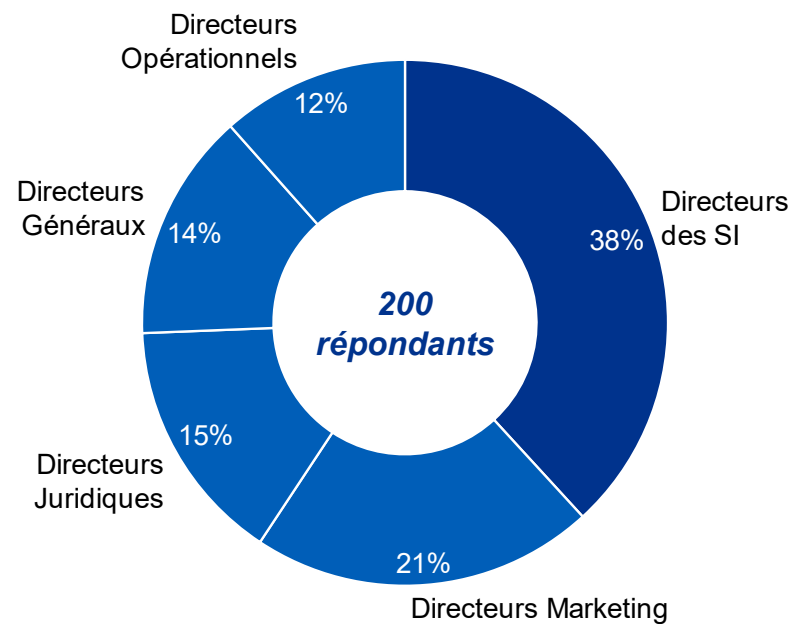
Principales caractéristiques du cloud



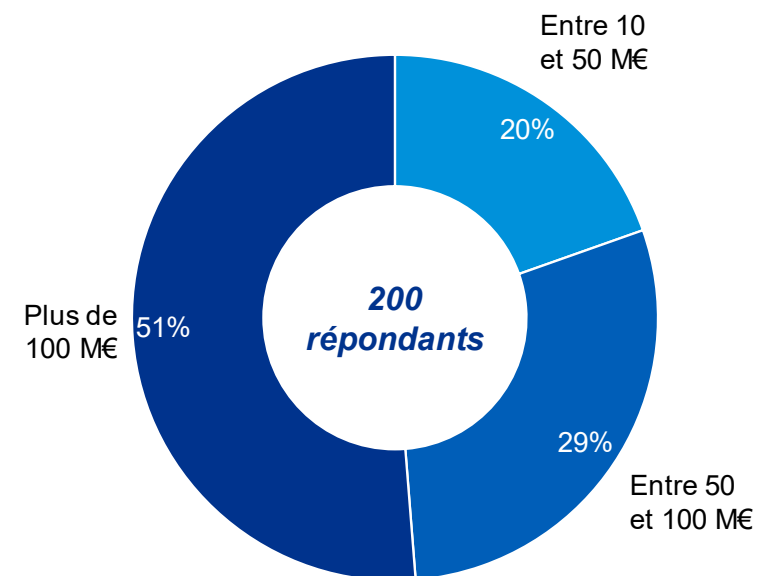
Lors de notre enquête, nous avons récolté les réponses de 200 participants, couvrant un large spectre d'acteurs, en terme de taille d'entreprise...

Profil des répondants au sondage

Par fonction au sein de l'entreprise



Par taille d'entreprise (exprimée en CA annuel)



Dont



50 % de répondants français

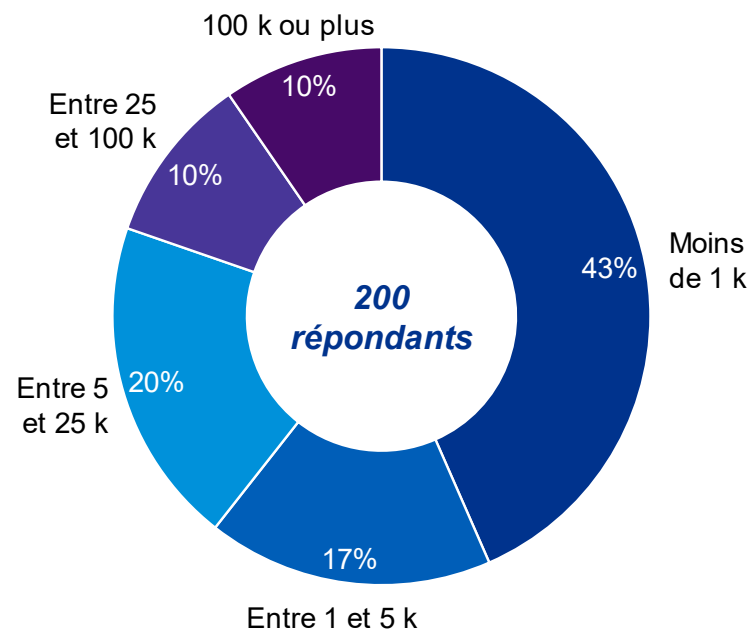


50 % de répondants allemands

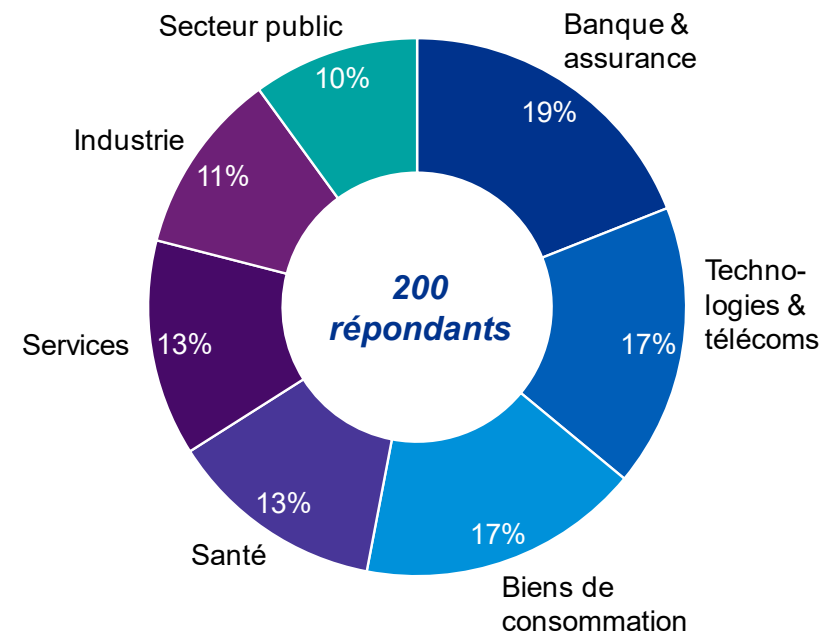
... mais également en ce qui concerne le nombre d'employés au sein de l'entreprise et le secteur d'activité

Profil des répondants au sondage

Par nombre d'employés



Par secteur d'activité de l'entreprise

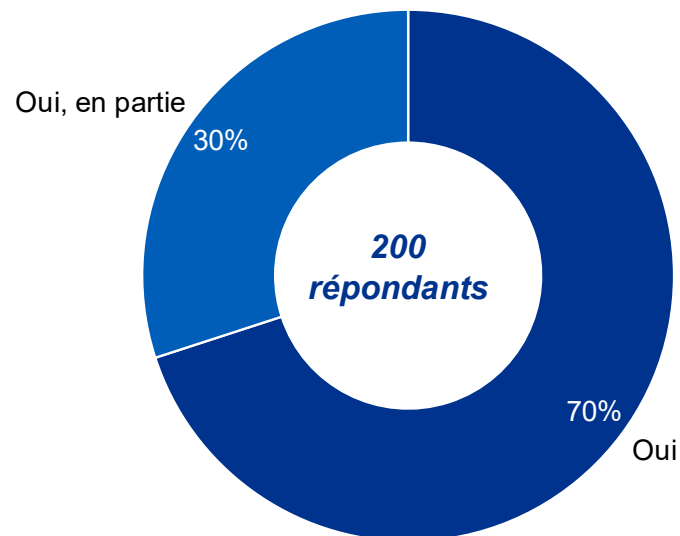


Toutes les personnes interrogées sont impliquées dans les choix liés au cloud computing et disposent en majorité d'une stratégie cloud formalisée

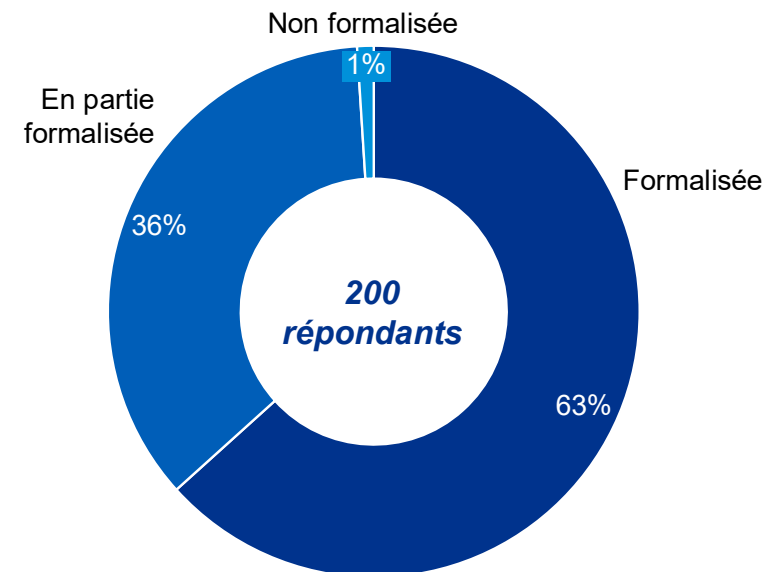
Profil des répondants au sondage



Prenez-vous part au processus décisionnel concernant le cloud computing dans votre entreprise ?



Comment décririez-vous votre stratégie cloud ?



6



Annexes -chapitre 3

Le RGPD a mis en place une « zone d'échange de données » réglementée au sein de l'Union européenne et instauré des règles strictes de traitement des données hors UE



Le Règlement général sur la protection des données (RGPD) détermine un niveau particulier de protection des données à caractère personnel, et permet donc la libre circulation des données à caractère personnel à l'intérieur et en dehors de l'UE



Qui est concerné ?

Toute organisation, publique ou privée, indépendamment de la taille, du pays d'implantation et de l'activité

Le Règlement général sur la protection des données :

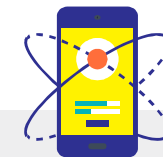
- impose **davantage d'obligations** aux sous-traitants et responsables du traitement
- renforce les **droits des personnes** dont les données sont traitées
- nécessite la mise en œuvre de **mesures techniques et organisationnelles spécifiques**



Données à caractère personnel

Toute information liée à une personne physique identifiée ou identifiable

Article 4.1 du RGPD : « une personne physique identifiable est **une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale** »



Traitement des données

Toute opération, ou ensemble d'opérations, se rattachant à des données à caractère personnel

Article 4.2 du RGPD : « 'traitement' désigne toute opération ou tout ensemble d'opérations **effectuées ou non à l'aide de procédés automatisés et appliquées à des données** ou des ensembles **de données à caractère personnel**, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »

Le RGPD forme un cadre cohérent pour la protection des données à caractère personnel dans l'Union européenne, permettant la libre circulation interne des données



- Afin d'assurer un **niveau élevé et cohérent** de protection des personnes physiques, et de lever les obstacles à la circulation des données à caractère personnel à l'intérieur de l'Union, le niveau de protection des droits et libertés des personnes physiques en ce qui concerne le traitement de ces données doit être **équivalent dans tous les États membres⁽¹⁾**

C'est parce que le RGPD est un règlement homogène dans l'ensemble des États membres que cette protection cohérente peut être assurée dans toute l'Union

Les flux de données sortant de l'UE vers un pays étranger sont une nécessité économique, et ne sont autorisés par le RGPD que sous certaines conditions

Principes directeurs

“ Considérant 101 du RGPD ”

Les **flux** de données à caractère personnel **à destination et en provenance de** pays en dehors de l'Union et d'organisations internationales **sont nécessaires au développement du commerce international et de la coopération internationale**



- Le RGPD n'interdit pas les flux internationaux. Il établit cependant que, lorsque des responsables du traitement ou des sous-traitants effectuent des transferts dans des pays tiers ou vers une organisation internationale, ils doivent veiller à ce que « **le niveau de protection des personnes physiques garanti dans l'UE par le RGPD ne soit pas compromis** »
- Afin d'assurer un **niveau élevé et cohérent** de protection des personnes physiques et de **lever les obstacles à la circulation** des données à caractère personnel **en dehors de l'Union**, le niveau de protection des droits et libertés des personnes physiques en ce qui concerne le traitement de ces données doit être **fondamentalement équivalent à celui garanti à l'intérieur de l'UE**

Le RGPD assure **un seuil minimum** à respecter, indépendamment de l'origine du responsable du traitement ou du sous-traitant

Trois grands outils ont été créés par le RGPD pour faciliter la conformité dans les cas de flux de données sortants

Boîte à outils

Les **transferts de données à caractère personnel en dehors de l'UE étant inévitables**, le RGPD a créé une boîte à outils pour faire en sorte que ces transferts respectent le **seuil minimum établi**

1 Premier outil : la décision d'adéquation

La Commission peut décider **avec effet dans l'ensemble de l'UE** qu'un pays tiers, un territoire ou un secteur spécifié dans un pays tiers, ou une organisation internationale **offre un niveau adéquat de protection des données**, assurant ainsi une sécurité juridique et une uniformité dans l'ensemble de l'Union en ce qui concerne le pays tiers ou l'organisation internationale en question⁽¹⁾



2 Deuxième outil : Clauses Contractuelles Types

Les Clauses Contractuelles Types (CCT) adoptées par la Commission peuvent être appliquées entre les responsables du traitement et les fournisseurs afin **d'assurer des garanties suffisantes** pour la protection des données transférées à l'international

3 Troisième outil : règles d'entreprise contraignantes (REC)

En cas de **transferts intra-groupe** de données à caractère personnel en dehors de l'UE, les règles d'entreprise contraignantes peuvent et doivent être **établies au sein du même groupe** lorsque des entités du groupe situées en dehors de l'UE sont impliquées dans des transferts de données personnelles

Le Privacy Shield de 2016 visait à permettre le transfert de données et l'accès aux données entre les États-Unis et l'UE... mais a été invalidé en 2020



2016

Le **Privacy Shield** est un cadre défini par les États-Unis et l'Union européenne (décision d'adéquation), dont l'objet est de **protéger les droits fondamentaux des utilisateurs en ligne de l'UE** dont les données à caractère personnel seraient traitées par des entreprises et organisations américaines. Il permet aux responsables du traitement et aux sous-traitants de **transférer librement les données à caractère personnel** de ressortissants de l'UE **tout en respectant leurs droits personnels**.

2020



Privacy Shield Invalidation du Privacy Shield (Schrems II)

Suite à une plainte du militant pour la protection des données M. Schrems, la Cour de justice de l'UE a invalidé l'accord Privacy Shield, considérant que les programmes de surveillance américains **n'étaient pas compatibles** avec les principes du RGPD.



Le Foreign Intelligence Surveillance Act (FISA) et l'Executive Order 12333 permettent aux autorités publiques américaines d'accéder à toutes données à caractère personnel transitant sur le sol américain



En conséquence de l'invalidation du Privacy Shield, les entreprises transférant des données à caractère personnel sur des serveurs en dehors de l'UE **n'ont plus de base juridique** pour le faire et sont donc passibles de poursuites judiciaires

De fait, le Cloud Act assure aujourd'hui au gouvernement américain un accès relativement large aux données à caractère personnel, au sein ou en dehors du territoire des États-Unis, en contradiction avec le RGPD



Le Clarifying Lawful Overseas Use of Data (Cloud) Act est une loi fédérale américaine contraignant les fournisseurs de services de communications électroniques ou d'informatique à distance à divulguer au gouvernement américain les données personnelles des utilisateurs, que les informations se trouvent sur ou en dehors du territoire des États-Unis



Qui est concerné ?

Tous les fournisseurs soumis au droit américain, c'est-à-dire toute entité implantée aux États-Unis, notamment :

- **Entreprises américaines**
- Entités étrangères ayant des **filiales américaines**



Conditions de communication des données

Les autorités peuvent contraindre les prestataires de services à fournir des données, en vertu des dispositions légales strictes d'un **mandat émis par un tribunal américain**

Nombre de demandes gouvernementales d'informations d'utilisateur reçues (2019)



81 785 demandes au total pour Google, dont **282** concernant des entreprises, **152** demandes relatives à des clients G Suite Enterprise Cloud, et **0** demandes relatives à des clients Google Cloud Platform Enterprise

Résultat de l'invalidation du Privacy Shield, la boîte à outils du RGPD est devenue obsolète, soulevant des interrogations de fond pour les entreprises américaines et européennes

Une boîte à outils RGPD inefficace



L'affaire Schrems II a imposé le **réexamen** de l'ensemble de la boîte à outils créée par le RGPD dans la mesure où il n'est plus possible, indépendamment de l'outil, d'assurer un niveau adéquat de protection des données à caractère personnel transférées aux États-Unis.



La législation nationale prévaut sur les différents outils prévus par le RGPD, puisque les autres moyens visant à assurer un niveau adéquat de protection des données à caractère personnel transférées en dehors de l'UE sont des outils contractuels

Le réexamen de la boîte à outils pose de nouvelles questions

- Lorsque vous êtes une entreprise **d'hébergement américaine**, vous ne pouvez traiter des données à caractère personnel de l'UE que sur la base d'une décision d'adéquation (Safe Harbor, puis Privacy Shield). Que se passe-t-il si cette décision d'adéquation est annulée ?
- Si vous êtes une entreprise d'hébergement, **établie dans l'UE mais affiliée à et contrôlée par une entreprise américaine**, que se passe-t-il si la décision d'adéquation en vertu de laquelle les données à caractère personnel sont traitées est annulée ?

Compte tenu de l'invalidation du Privacy Shield, le Comité européen de la protection des données (CEPD) propose une nouvelle boîte à outils prévoyant 6 grandes étapes

Nouvelle boîte à outils du CEPD¹



Compte tenu de l'invalidation du Privacy Shield, le Comité européen de la protection des données propose une **nouvelle boîte à outils : la feuille de route de redevabilité prévoit 6 étapes à suivre** permettant aux exportateurs d'évaluer les pays tiers et d'identifier des mesures supplémentaires appropriées au besoin



Le CEPD remédie à l'invalidation du Privacy Shield dans un certain nombre de cas impliquant des données à caractère personnel



Cas d'usage autorisés

- ✓ Cas d'usage 1 : stockage de données aux fins de sauvegarde ou autres ne nécessitant pas d'accès aux données en clair
- ✓ Cas d'usage 2 : transfert de données pseudonymisées
- ✓ Cas d'usage 3 : données chiffrées transitant simplement vers des pays tiers

✓ Cas d'usage 4 : destinataire protégé

✓ Cas d'usage 5 : traitement fractionné ou multipartite

Implique de prévoir contractuellement des mesures techniques de sécurité pour les transferts de données à caractère personnel

Le CEPD donne l'exemple d'un exportateur de données transférant des données à caractère personnel à un importateur de données d'un pays tiers expressément protégé par la loi de ce pays, par exemple aux fins de fournir conjointement un traitement médical à un patient ou un service juridique à un client.

Ce cas d'usage est autorisé si, entre autres, le droit du pays tiers exempte un importateur de données résident de toute violation potentielle d'accès aux données détenues par ce destinataire pour la finalité considérée (secret professionnel) et que des mesures techniques sont prises pour garantir ces informations privilégiées (clés cryptographiques, mots de passe, etc.)



Le CEPD donne l'exemple d'un exportateur de données souhaitant traiter des données à caractère personnel conjointement avec deux sous-traitants indépendants (ou plus), situés dans des juridictions différentes, sans leur communiquer le contenu des données. Avant la transmission, l'exportateur de données fractionne les données de sorte qu'aucune partie reçue par un sous-traitant individuel ne suffise à reconstruire les données à caractère personnel en tout ou en partie.

Ce cas d'usage est autorisé si, entre autres, l'exportateur de données traite des données à caractère personnel de telle manière qu'elles soient fractionnées en deux parties ou plus, chacune d'elles ne pouvant plus être interprétée ou attribuée à une personne concernée spécifique sans l'utilisation d'informations supplémentaires et étant transférée à un sous-traitant distinct situé dans une juridiction différente



Pourtant, deux des cas d'usage les plus courants semblent toujours interdits malgré les efforts du CEPD pour atténuer les conséquences de l'invalidation du Privacy Shield



Cas d'usage interdits



Cas d'usage 6 : transfert à des fournisseurs de services cloud ou à d'autres fournisseurs nécessitant un accès aux données en clair



Cas d'usage 7 : accès à distance aux données à des fins commerciales

Le remède apporté par le CEPD n'est que partiel, puisque les cas d'usage les plus courants sont prohibés

Le CEPD donne l'exemple d'un exportateur de données recourant à un fournisseur de services cloud ou à un autre fournisseur pour faire traiter des données à caractère personnel selon ses instructions dans un pays tiers.

➤ Ce cas est interdit puisque le fournisseur de services cloud a besoin d'accéder aux données en clair pour exécuter la tâche assignée, dans l'hypothèse où le pays tiers des destinataires donne pouvoir aux autorités publiques pour accéder aux données transférées d'une manière allant au-delà de ce qui est nécessaire et proportionné dans une société démocratique



Le CEPD donne l'exemple d'un exportateur de données mettant à disposition d'entités d'un pays tiers des données à caractère personnel à utiliser à des fins commerciales partagées. Il peut s'agir d'un responsable du traitement ou d'un sous-traitant établi sur le territoire d'un État membre de l'UE et transférant des données à caractère personnel à un responsable du traitement ou un sous-traitant d'un pays tiers appartenant au même groupe d'entreprises ou à un groupe d'entreprises engagées dans une activité économique conjointe.

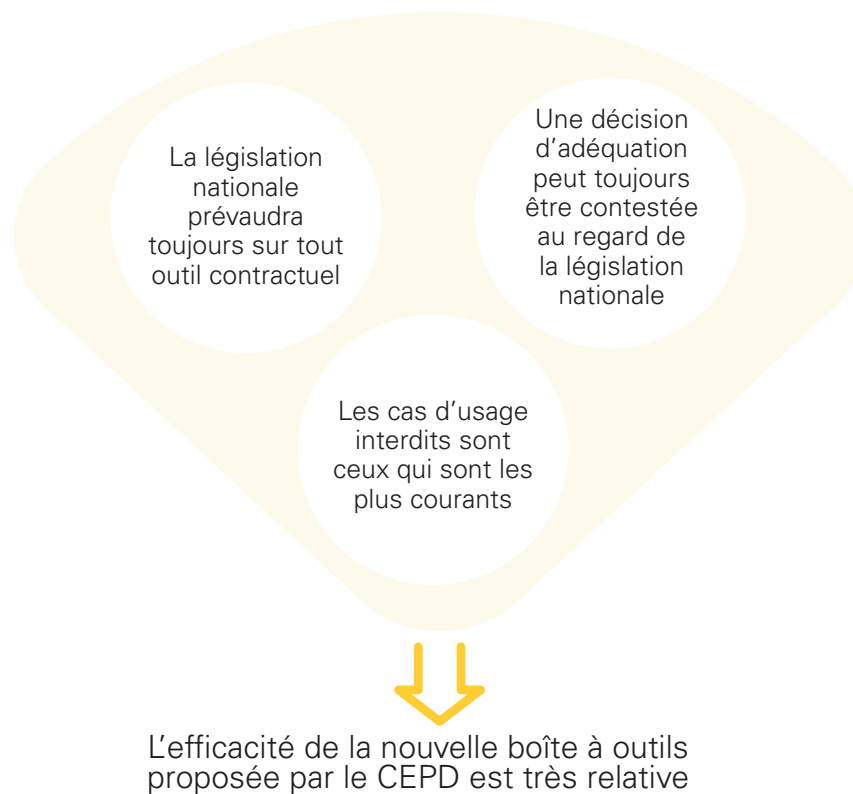
➤ Ce cas est interdit puisque l'exportateur de données permet à l'importateur d'accéder directement aux données de son choix en les transférant directement au moyen d'un service de communication pour que l'importateur les utilise en clair à ses fins, en particulier si le pays tiers de l'importateur donne pouvoir aux autorités publiques pour accéder aux données transférées d'une manière allant au-delà de ce qui est nécessaire et proportionné dans une société démocratique



Dans les deux scénarios, même le chiffrement en transit et le chiffrement des données au repos ne peuvent constituer ensemble une mesure supplémentaire assurant un niveau fondamentalement équivalent de protection des données à caractère personnel

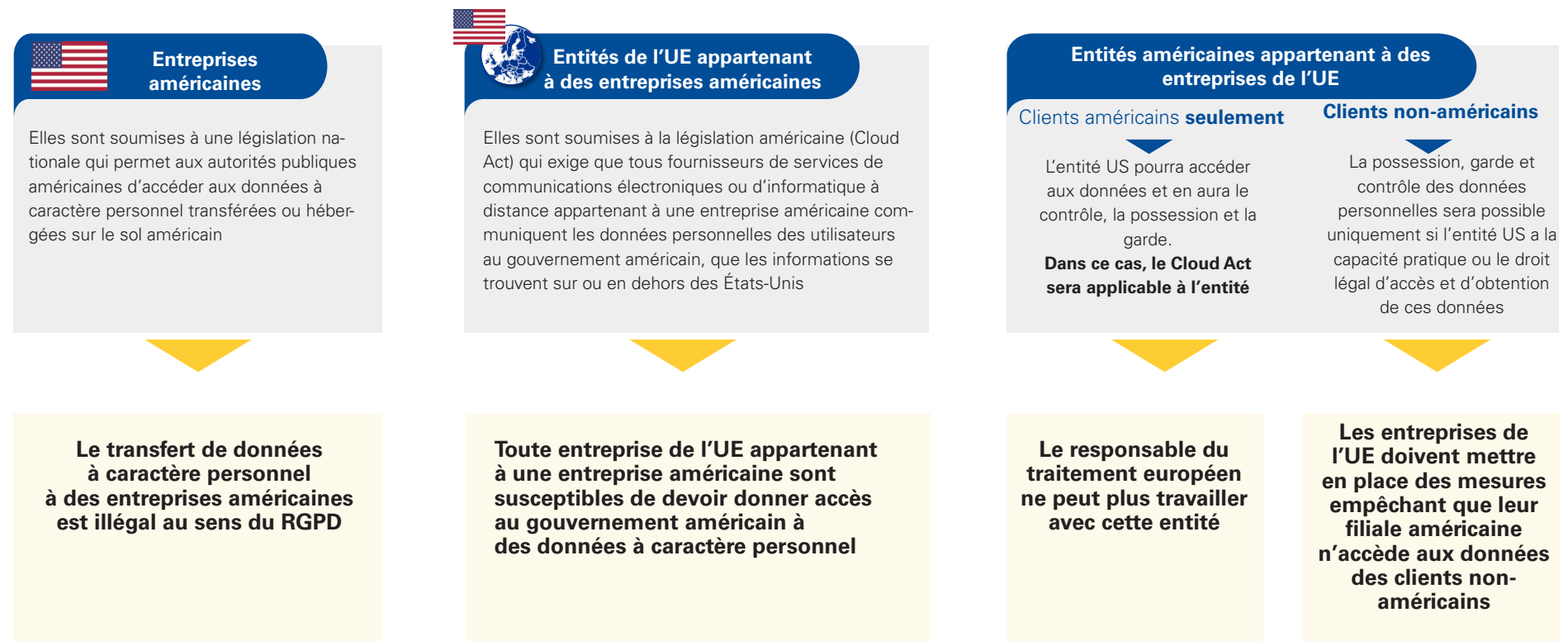
En conclusion, le succès des efforts menés par le CEPD avec sa boîte à outils semble très relatif, car les cas d'usage les plus courants sont interdits

Synthèse des problématiques relatives à l'utilisation de la boîte à outils du CEPD



- Le réexamen de la boîte à outils créée par le CEPD **pose la question de son efficacité** au regard des obstacles ci-contre
- Ces obstacles s'appliquent à **tous les transferts de données à caractère personnel en dehors de l'UE**, non seulement vers les États-Unis, mais aussi vers d'autres pays tiers, comme par exemple, le Royaume-Uni depuis le Brexit

En conclusion, les entreprises de l'UE soumises au RGPD en tant que responsables du traitement ne peuvent plus travailler avec les entreprises américaines ou les entreprises européennes appartenant à des entreprises américaines



- **Les entreprises européennes soumises au RGPD, en qualité de responsables du traitement, ne peuvent plus travailler avec les entreprises américaines, les entreprises européennes appartenant à des entreprises américaines, ou les entités américaines appartenant à des entreprises européennes avec des clients américains seulement**, dans la mesure où la législation américaine enfreint le principe de protection adéquate posé par le RGPD, et ce que les informations se situent au sein ou en dehors du territoire des États-Unis



Jean-Charles Ferreri

Partner

Global Strategy Group KPMG France

Tel: +33 (0)6 60 07 08 99
jferreri@kpmg.fr



Bertrand Grau

Partner

Global Strategy Group KPMG France

Tel: +33 (1) 55 68 25 10
bertrandgrau@kpmg.fr



Sébastien Ropartz

Partner

KPMG Technology Transformation

Tel: +33 (1) 55 68 38 83
sropartz@kpmg.fr



Patrick Amouzou

Partner

Global Strategy Group KPMG France

Tel: +33 (1) 55 68 51 19
pamouzou@kpmgavocats.fr