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

Description

Une profonde incohérence entre les réglementations américaine et européenne fausse le marché du cloud européen

En avril 2021, le cabinet d'audit KPMG a remis à Talan SAS, InfraNum, OVHcloud et Linkt le présent rapport dont l'objectif fut *« d'étudier la conjoncture et les défis du marché européen du cloud »*, presque entièrement aux mains de fournisseurs en dehors de l'Europe. Au premier semestre 2020, 68 % des dépenses d'infrastructures cloud des entreprises européennes sont captées par Amazon Web Services (53 %), Microsoft Azure (9 %) et Google (6 %) alors que le Français OVHcloud, leader européen du cloud privé, n'en détient que 4 %. Dans un marché en pleine croissance, qui passerait de 53 milliards d'euros en 2020 à 560 milliards en 2030, le cabinet estime que les enjeux pour l'Europe représentent *« environ 550 000 emplois et près de 200 milliards d'euros d'investissements sur la période 2021-2027, dans la configuration où les opérateurs de Cloud localisent leurs opérations et leurs investissements en Europe »*.

Élaboré grâce à 250 entretiens auprès de décideurs privés et publics, dont la Commission européenne, le document explique notamment *« l'incompatibilité réglementaire »* entre les législations européenne et américaine. En 2016, lors de l'élaboration du Règlement général pour la protection des données personnelles (RGPD) en Europe (voir *La rem* n°42-43, p.21), les États-Unis ont adopté le *Privacy Shield* (bouclier de confidentialité), pour encadrer le transfert de données à caractère personnel d'Européens vers les États-Unis. Les États-Unis ont ensuite voté, en mars 2018, le Clarifying Lawful Overseas Use of Data Act, dit « CLOUD Act », leur permettant de contraindre n'importe quel fournisseur de services cloud établi sur le territoire américain à fournir les données personnelles de quiconque, stockées sur des serveurs situés aux États-Unis comme dans des pays étrangers. Or, cette législation et les programmes de surveillance américains ne sont pas compatibles avec les principes du RGPD, en vigueur depuis mai 2020 en Europe, ce qu'a confirmé la Cour de justice de l'Union européenne (CJUE) le 16 juillet 2020 dans son désormais célèbre arrêt « Schrems II » (voir *La rem* n°54bis-55, p.5). Cette incompatibilité réglementaire aboutit à ce que *« les entreprises transférant des données à caractère personnel d'Européens à des serveurs d'entreprises noneuropéennes n'ont plus de fondement juridique lié au Privacy Shield et sont ainsi passibles de poursuites judiciaires »*. 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 »* ou encore *« 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 »*.

Cette profonde incompatibilité pourrait cependant devenir bénéfique au marché du cloud européen, si la législation suivait. *« 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 »*, explique ainsi le rapport.

Parmi les scénarios envisagés par le cabinet, celui permettant la plus grande captation de valeur en Europe et favorisant plus que les autres l'innovation serait celui de *« l'européanisation des opérations des prestataires cloud »* assorti d'un *« contrôle européen effectif des filiales locales d'*hyperscalers *»*. Les *hyperscalers*, qui désignent les offres cloud les plus performantes au monde – celles d'Amazon, Microsoft et Google –, pourraient être contraints d'assurer à l'Europe *« une plus grande part des bénéfices économiques du cloud »*, notamment par des obligations d'investissement et de localisation en Europe de leur R&D (Recherche et Développement). Dans ce scénario, KPMG suggère également que les filiales européennes des *hyperscalers* appartiennent légalement à des entreprises européennes, sous la forme de joint-ventures, afin de s'assurer d'une réelle conformité de leur activité à la réglementation européenne en matière d'exploitation et de transfert des données personnelles. Ce scénario n'est pas irréaliste puisque la Chine et les États-Unis font précisément de même. Selon le rapport, *« en Chine, Microsoft Azure et Amazon Web Service fournissent des services locaux de cloud computing via une joint-venture mise en place avec des acteurs locaux »*. La loi chinoise sur la cybersécurité impose purement et simplement *« aux prestataires cloud étrangers d'établir un partenariat avec des entreprises locales pour fournir des services aux clients chinois »*. Aux États-Unis, en 2020, *« l'entreprise de gaming chinoise Beijing KunlunTech 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) »*

.

Selon le cabinet d'audit, l'absence de prise de position protectrice de l'Europe pourrait mener à une perte de 20 à 50 % de l'impact économique attendu, tant en termes de valeur captée que de nombre d'emplois créés ou d'investissements nouveaux.

Le Cloud européen : de grands enjeux pour l'Europe et cinq scénarios avec des impacts majeurs d'ici 2027-2030, KPMG Global Strategy Group, avril 2021.

Categorie

1. A lire en ligne

date créée
7 octobre 2021
Auteur
jacquesandrefines