



CLOUD SOUVERAIN

L'ÉMERGENCE DE LA « CONFIANCE » DANS LE CLOUD

A défaut d'une définition de Cloud souverain tout à fait explicite et arrêtée, l'écosystème semble s'organiser autour d'une notion de « Cloud de confiance ». « Nous sommes sur un marché où beaucoup de choses sont dites et écrites et qui sont souvent fausses. Notre fonctionnement est donc principalement de faire ce que l'on dit, et de le prouver », avance Rémi Grivel, DSI du groupe Ciril, qui ajoute qu'il voit, souvent, des clients arriver « avec des contrats sans clause de réversibilité, pas de droit français, etc. ». Cette nouvelle approche prend toutefois différentes formes selon le prestataire, mais ils sont nombreux à s'y reconnaître voire à s'en revendiquer. « Nous ne l'avons pas libellé de la sorte mais cela fait partie de nos engagements et de la solution apportée. Par exemple, nous proposons des images de VM qui ont déjà

passé l'ensemble des étapes de qualité. Les niveaux de services répondent pour nous à une notion de confiance », explique quant à lui David Chassan, directeur de la stratégie d'Outscale.

La confiance par tous les côtés

Autre approche de la confiance : le semi-public. « Nous proposons un Cloud privé mais aussi un Cloud semi-public sur lequel il faut signer une charte et un contrat pour entrer dans cet environnement mutualisé », souligne Georges Lotigier du Français Scalair. Par ailleurs « ceux qui étaient réticents au Cloud sont rassurés par la proximité que nous leur apportons. Le client doit désormais comprendre où se trouvent les zones étanches, publiques, etc., et demander pour cela des analyses d'architecture de sécurité », ajoute-t-il. Directeur de l'hébergeur Alfa Safety, Christophe Lejeune tempère toutefois : « Le niveau

de confiance dans les grands Clouds professionnels – Azure, Salesforce, etc. – a beaucoup augmenté depuis deux ans. On voit désormais de l'hébergement SAP sur AWS, ou même des outils CRM chez Salesforce. Certaines banques passent elles aussi certaines parties de leurs applications dans des Clouds publics. » Enfin, la notion de confiance est également perçue de manière plus pragmatique par un certain nombre de prestataires, en se basant principalement sur le respect des certifications, normes, labels, etc. « Nous proposons des mécanismes de protection applicative pour minimiser les risques de fuite de données, mais cela reste cher », rappelle Laurent Perriault chez Claranet France. « La confiance revient de plus en plus souvent », ajoute Édouard de Rémur, co-fondateur d'Oodrive. « D'où l'intérêt des différentes certifications comme Cloud Confidence ou des labels que propose l'Anssi notamment ». ☺

Cispe : l'amorce d'une harmonisation européenne par la profession

À défaut d'une loi au niveau européen, une vingtaine de fournisseurs d'infrastructures en provenance d'une quinzaine de pays réunis au sein du Cispe (Cloud Infrastructure Services Providers in Europe) a décidé de prendre les devants à la fin 2016. Ce faisant, ils prennent de l'avance sur le futur Règlement général sur la protection des données (RGPD ou GDPR) de l'UE qui verra le jour en 2018. Les Français OVH, [IkoULA](#), Outscale sont de la partie. Globalement, ils souhaitent « redonner aux citoyens le contrôle sur leurs données personnelles », mais aussi « simplifier l'environnement réglementaire pour le commerce international, en harmonisant les réglementations au sein de l'UE ». Sorte de « Label Rouge » de la donnée, le code de conduite doit permettre une utilisation maîtrisée des données. Tout d'abord, il s'agit du traitement et du stockage, pour lesquels les fournisseurs du CISPE s'engagent à en garantir l'exécution en Europe uniquement. « Les services appropriés seront clairement identifiables au moyen d'une marque de confiance, que les fournisseurs d'infrastructures cloud pourront utiliser afin d'indiquer leur conformité au code de conduite »,

écrivent les principaux concernés. De plus, les adhérents au code de conduite s'engagent à ne pas traiter les données personnelles de leurs clients, que ce soit pour leur propre compte ou pour celui d'un tiers. Cela concerne donc le profilage, l'exploration de données ou autre, dans un but marketing par exemple. Pour le moment l'initiative du Cispe est aussi perçue comme un outil de conformité pour les entreprises, qui comble un manque actuel en aidant à l'identification des fournisseurs engagés. Elle remporte déjà de nombreux suffrages auprès des autorités. La conférence de presse à Bruxelles a été organisée avec le concours de l'eurodéputée Eva Paunova, membre de la Commission du marché intérieur et de la protection des consommateurs. De son côté, Axelle Lemaire, secrétaire d'État chargée du Numérique et de l'Innovation, a ajouté que « le code de conduite de l'association Cispe confirme que le secteur du Cloud Computing européen est capable de fournir des services conformes et sécurisés pour l'ensemble des données personnelles et techniques et d'améliorer la confiance dans les services numériques ».