

Qu’est-ce que la souveraineté des données et comment s’applique-t-elle dans le cloud public ?

PAIEMENT
CONNECTIVITÉ
CONTRÔLE D’ACCÈS
IDENTITÉ
VOYAGE
JUSTICE ET SÉCURITÉ PUBLIQUE

POSTÉ LE 21.03.23

En termes simples, la souveraineté des données consiste à contrôler ce qui est important, du point de vue des lois et des réglementations relatives à la protection des données d’une organisation, à toutes les phases du cycle de vie de ces données. Il s’agit d’un terme très large mais néanmoins important à bien appréhender lorsqu’il est appliqué à un environnement de cloud public. Pourquoi ? Parce que les données dans le cloud public sont hébergées sur le site d’un tiers et que diverses exigences définissent ce que signifie réellement la souveraineté des données dans ce contexte.

Il est important de noter que si la **protection des données personnelles** est au centre du débat public et constitue un aspect non négligeable de la souveraineté des données, ce n’est pas le seul : la souveraineté des données porte également sur la **sécurisation des infrastructures critiques**. Les pays ont, par exemple, des données sensibles qu’ils souhaitent conserver sur leur territoire et donc sous leur contrôle. Il peut s’agir d’informations essentielles au fonctionnement et à la gestion d’infrastructures critiques, telles qu’un réseau électrique, un réseau de télécommunications ou un système de soins de santé.

Compte tenu de la variété des services qui peuvent bénéficier d’un hébergement dans un environnement de cloud public et des différents niveaux de sensibilité des données associées, il existe **de nombreuses façons d’envisager la souveraineté des données**. Elle peut être abordée sous trois angles principaux : la résidence des données, le contrôle opérationnel et le contrôle juridique.

La résidence des données : la façon la plus courante d’envisager la souveraineté des données

La majorité des entreprises et des pays utilisent indifféremment les termes de souveraineté et de résidence des données. La résidence des données concerne **le lieu (c’est-à-dire l’emplacement physique réel) où les données sensibles sont stockées ou traitées**. Il s’agit généralement un pays ou une région, ou bien de l’emplacement physique d’un groupe de centres de données où une application est déployée. Le « où » est important car l’emplacement détermine la juridiction applicable et a une incidence sur le degré de contrôle qu’un pays exerce sur les données, leur traitement et les activités qui y sont associées.

La résidence des données est **une attente répandue** dans tous les secteurs et il est généralement **facile d’y répondre**

pour les principaux fournisseurs de services de cloud public étant donné l'étendue de leurs réseaux mondiaux de centres de données. Sur ce point, un environnement de cloud public est aussi clairement un avantage pour les entreprises opérant dans plusieurs juridictions, car il leur permet de stocker des données sensibles dans plusieurs centres de données situés dans plusieurs régions géographiques à travers le monde, afin de **se conformer aux réglementations locales** en matière de protection des données.

Contrôle opérationnel : la souveraineté des données au niveau de l'infrastructure

Le deuxième aspect le plus courant de la souveraineté des données est le contrôle opérationnel, qui concerne **la gestion de l'infrastructure sous-jacente** qui stocke, traite et protège les données sensibles et les applications correspondantes. Il s'agit de définir des contrôles et des politiques pour déterminer **qui peut accéder à l'information** et de mettre en place des équipes auxquelles on peut faire confiance pour sécuriser les données sensibles. Les entreprises peuvent mettre en œuvre divers contrôles pour vérifier « qui a les mains sur le clavier ». Il peut s'agir de :

- la mise en place d'un **audit** pour produire des éléments de preuve de conformité ;
- l'obtention de **certifications** pour prouver le contrôle opérationnel ou, plus récemment ;
- la mise en œuvre de **solutions technologiques** telles que le confidential computing (ou « informatique confidentielle » en français), qui consiste à crypter les données sensibles lorsqu'elles sont traitées par une machine virtuelle, afin de s'assurer que personne, pas même « ceux qui ont les mains sur le clavier », ne puisse accéder aux données en clair.

Le contrôle juridique : la façon la plus stricte d'envisager la souveraineté des données

La troisième exigence en matière de souveraineté des données est celle du contrôle juridique. Il s'agit de l'exigence la plus compliquée à mettre en œuvre, mais c'est aussi la moins courante. **Lorsqu'un État exige le contrôle juridique sur les données, il demande à ce que le fournisseur de services cloud se trouve dans sa propre juridiction**, autrement dit en dehors de la juridiction de toute puissance étrangère. Dans ce cas de figure, le fournisseur de services cloud, qui possède et gère les actifs, n'est soumis à aucune influence étrangère et ne peut en aucun cas être contraint de se conformer aux exigences d'une autorité étrangère.

Si l'on considère que quelques entreprises basées aux États-Unis représentent actuellement plus de 70% des parts de marché des fournisseurs de services de cloud public, il est manifestement **difficile pour une entreprise ou un gouvernement non américain** de s'attendre à un tel contrôle juridique tout en bénéficiant de tous les avantages d'un environnement de cloud public. Cela dit, très peu d'organisations ont besoin d'un tel contrôle juridique à ce jour, et lorsqu'elles en ont besoin, **cela ne concerne que des tâches bien spécifiques**.