

Qu'est-ce que la souveraineté des données ?

3 juin 2024

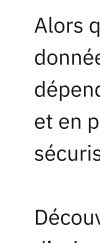
Aperçu

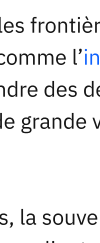
Pourquoi la souveraineté des données est-elle importante ?

Comment la souveraineté des données est-elle déterminée ?

Comment fonctionne la souveraineté des données ?

Auteurs

Mesh Flinders
Author, IBM Think

Ian Smalley
Senior Editorial Strategist

Qu'est-ce que la souveraineté des données ?

La **souveraineté des données** est le concept selon lequel les données sont soumises aux lois du pays où de la région où elles ont été générées.

Parfois appelée résidence des données, la souveraineté des données est rapidement en train de devenir un élément central des stratégies juridiques, de confidentialité, de sécurité et de **gouvernance** pour les entreprises qui gèrent le stockage, le traitement et le transfert de données. En adoptant une approche solide de la **gestion des données** et des flux de données internationaux, un élément clé de la souveraineté des données, les entreprises sont mieux à même de protéger leurs informations les plus sensibles contre les **les cyberattaques** et autres menaces.

Souveraineté, résidence et localisation des données sont des termes étroitement liés. En fait, les termes de souveraineté des données et de résidence des données sont si étroitement liés qu'ils sont parfois employés de manière interchangeable. Cependant, il existe certaines différences importantes que les organisations qui souhaitent utiliser les capacités de **cloud computing** dans le cadre de leur **transformation numérique** doivent comprendre.

Souveraineté des données : les données sont stockées et traitées dans le pays où elles ont été générées.

Localisation des données : données stockées dans un pays différent de celui où elles ont été générées.

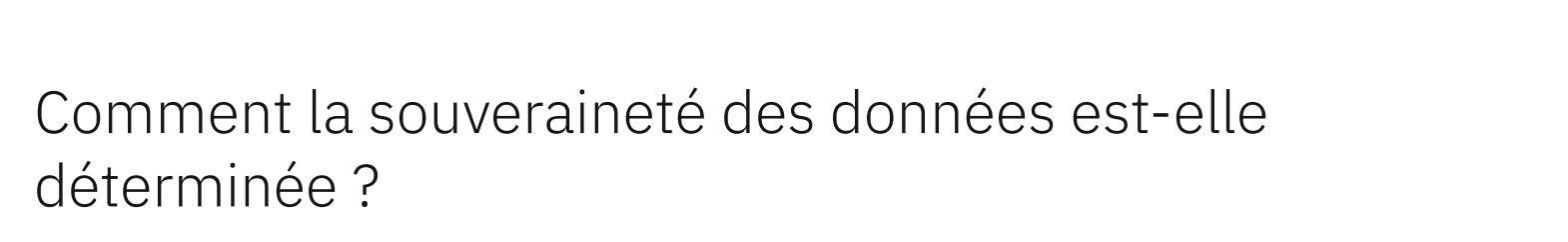
Residence des données : se rapporte au respect de la conformité avec toutes les lois et exigences applicables concernant l'hébergement des données.

Qu'est-ce que le cloud souverain ?

La souveraineté, la résidence et la localisation des données sont toutes des éléments essentiels d'un concept dénommé **cloud souverain**, un type de cloud computing qui aide les organisations à se conformer aux lois sur la protection de la vie privée en vigueur dans les régions et pays où elles collectent, traitent et stockent les données de leurs clients.

Alors que le stockage dans le cloud poursuit une expansion dans le monde entier, les frontières géographiques traditionnelles ne suffisent plus à protéger les données sensibles. De plus, l'essor des technologies à forte intensité de données comme **l'intelligence artificielle (IA)** et le **machine learning (ML)** qui dépendent d'un accès rapide et sécurisé aux données obligent les entreprises à prendre des décisions plus stratégiques en matière de sécurité du cloud, l'IA, et en particulier **l'IA générative**, a le potentiel d'alimenter des innovations métier de grande valeur, mais elle a besoin d'une infrastructure cloud rapide et sécurisée pour fonctionner.

Découvrez le cloud souverain, un concept qui englobe la souveraineté des données, la souveraineté opérationnelle et la souveraineté numérique. Les cadres d'exigences du cloud souverain aident les entreprises à renforcer la confiance de leur clients et à **développer leurs activités** tout en respectant les lois sur la collecte, le stockage et la **confidentialité des données** dans les régions où elles opèrent.



What is Sovereign Cloud? (9:50 min)

Pourquoi la souveraineté des données est-elle importante ?

L'importance de la souveraineté des données est étroitement liée à la place croissante qu'occupent les environnements de cloud computing dans les stratégies de croissance globales de nombreuses entreprises.

Alors que de plus en plus d'applications d'entreprise migrent vers le cloud, l'environnement cloud devient une **infrastructure critique**, tout aussi importante pour la santé d'une entreprise qu'une usine, un immeuble de bureaux ou une propriété intellectuelle précieuse.

Les exigences en matière de souveraineté des données sont généralement liées aux réglementations sur la confidentialité des données applicables dans un pays ou une région spécifique. Les principales préoccupations des organisations cherchant à se conformer aux lois locales portent généralement sur la **cybersécurité**, la **sécurité** et la confidentialité des données, la protection des données sensibles contre les **violations** et les **logiciels malveillants**, et le contrôle de l'accès des individus, des entités et des applications aux données.

Par exemple, l'Union européenne (UE) dispose d'un **Règlement général sur la protection des données (RGPD)** qui oblige les entreprises opérant sur le territoire de l'UE et traitant les données des citoyens de l'UE à engager une personne dénommée « Délégué à la protection des données » (DPO ou Data Protection Officer), afin de s'assurer que les organisations respectent strictement la confidentialité, l'intégrité et l'accessibilité des données qu'elles génèrent, traitent et stockent.

Renforcez vos renseignements de sécurité

Gardez une longueur d'avance sur les menaces grâce à l'actualité et aux réflexions sur la sécurité, l'IA et bien plus encore, dans la newsletter hebdomadaire Think.

S'abonner dès maintenant

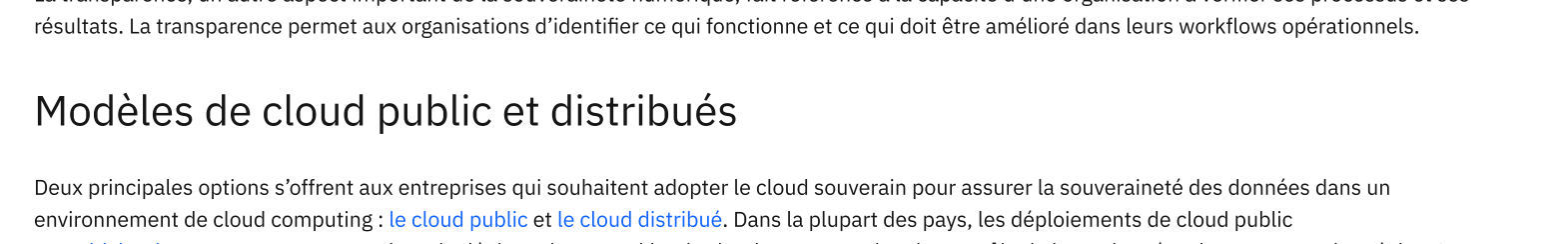
Comment la souveraineté des données est-elle déterminée ?

La souveraineté des données est déterminée par les lois et réglementations particulières qui régissent la région ou le pays où les données ont été générées.

Ces lois varient d'un territoire à l'autre, mais en règle générale, lorsqu'un pays est dit « souverain » sur un élément de données, cela signifie qu'il détient la juridiction et l'autorité sur la manière dont ces données peuvent être utilisées et les personnes autorisées à y accéder. Cependant, les données sont souvent soumises aux législations de plusieurs pays (résidence des données et localisation des données), si bien que leur gestion, leur stockage et leur traitement deviennent de plus en plus complexes.

Lorsque les données sont générées dans un pays ou une région, mais stockées et/ou traitées ailleurs, l'entreprise responsable des données doit s'assurer qu'elle respecte toutes les exigences légales relatives au traitement des ensembles de données dans les deux emplacements. Par exemple, les entreprises peuvent être amenées à établir des accords particuliers de protection des données ou à concevoir et mettre en œuvre des protocoles de transfert de données spécifiques pour maintenir la conformité et éviter les conflits potentiels sur un ou plusieurs territoires. De plus, les entreprises qui stockent et traitent des données dans plusieurs régions ou pays doivent connaître les **lois applicables en matière de protection des données**, les restrictions transfrontalières et autres obligations à respecter afin de préserver la confidentialité et l'intégrité des données.

Mixture of Experts | 25 avril, épisode 52



Décryptage de l'IA : Tour d'horizon hebdomadaire

Rejoignez notre panel d'ingénieurs, de chercheurs, de chefs de produits et autres spécialistes de premier plan pour connaître l'essentiel de l'actualité et des dernières tendances dans le domaine de l'IA.

Écouter les derniers épisodes de podcast →

Comment fonctionne la souveraineté des données ?

Pour être efficace, l'approche d'une organisation en matière de souveraineté des données doit également inclure deux autres composantes essentielles : la souveraineté opérationnelle et la souveraineté numérique. La souveraineté des données, la souveraineté opérationnelle et la souveraineté numérique sont les trois composantes les plus importantes d'une infrastructure de cloud souverain. La souveraineté opérationnelle garantit que les infrastructures critiques sont toujours disponibles pour les personnes, les entités et les applications qui en ont besoin, tandis que la souveraineté numérique garantit qu'une entreprise a toujours le contrôle de ses actifs numériques. Examinons de plus près ces deux concepts et pourquoi ils sont importants.

Souveraineté opérationnelle

La souveraineté opérationnelle garantit que l'infrastructure critique associée aux applications enrichies en données est active en permanence et accessible. En outre, la souveraineté opérationnelle aide les entreprises à assurer la transparence et le contrôle sur leurs processus opérationnels et à repérer les inefficacités.

Avec une approche solide de la souveraineté opérationnelle, une entreprise est en mesure de garantir la résilience de son infrastructure critique, même lorsqu'une région particulière est touchée par une catastrophe. Pour ce faire, de nombreuses approches de souveraineté opérationnelle prévoient un plan de **continuité des activités et de reprise après sinistre (BCDR)** et de **reprise après sinistre en tant que service (DRaaS)**. Enfin, la souveraineté opérationnelle aide les entreprises à se conformer aux réglementations locales régissant l'infrastructure nécessaire pour prendre en charge les environnements cloud dans une région donnée.

Souveraineté numérique

La souveraineté numérique décrit le niveau de contrôle d'une organisation sur ses actifs numériques, tels que les données, les logiciels, le contenu et l'infrastructure numérique. C'est un élément important du concept de cloud souverain, principalement du point de vue de la gouvernance et de la transparence. Les entreprises qui appliquent un contrôle des accès à leurs actifs numériques doivent définir des règles qui déterminent les autorisations d'accès à accorder en fonction des différents utilisateurs. Ces règles doivent être mises en place de façon à être facilement applicables, par exemple à l'aide de « règles en tant que code », un processus qui permet aux organisations de gérer leur infrastructure et leurs procédures de manière reproductible.

La transparence, un autre aspect important de la souveraineté numérique, fait référence à la capacité d'une organisation à vérifier ses processus et ses résultats. La transparence permet aux organisations d'identifier ce qui fonctionne et ce qui doit être amélioré dans leurs workflows opérationnels.

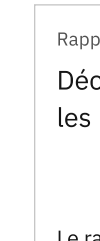
Modèles de cloud public et distribués

Deux principales options s'offrent aux entreprises qui souhaitent adopter le cloud souverain pour assurer la souveraineté des données dans un environnement de cloud computing : **le cloud public** et **le cloud distribué**. Dans la plupart des pays, les déploiements de cloud public et **multicloud** permettent aux entreprises de déployer leurs workloads cloud tout en gardant le contrôle de leurs données dans une certaine région. Les architectures de cloud public comportent généralement une couche de plateforme cloud, comme une **plateforme de cloud hybride**, pour assurer un déploiement cloud stable et cohérent.

La seconde option est le modèle de déploiement cloud distribué, par exemple un fournisseur d'infrastructure local ou un **centre de données** sur site. Ces solutions sont intéressantes pour les entreprises qui souhaitent mieux contrôler leurs données. Fondamentalement, un modèle de déploiement cloud distribué vous permet de déployer des workloads et des plateformes dans l'infrastructure de votre choix.

L'approche en trois étapes de la souveraineté des données d'entreprise

Pour commencer à mettre en œuvre une approche efficace en matière de souveraineté des données, les organisations doivent prendre les mesures suivantes :

- **Connaître les lois et réglementations applicables**
Les entreprises qui cherchent à développer des fonctionnalités de données sur site ou basées sur le cloud dans plusieurs régions ou pays doivent d'abord se familiariser avec les lois et réglementations régissant la souveraineté des données dans ces territoires.
- **Établir un canal de communication avec les autorités compétentes**
Il est important de contacter les autorités chargées de l'application des lois sur la souveraineté des données dans les pays ou les régions où vous souhaitez exercer vos activités. Communiquez sur vos projets de stockage, de traitement et de transfert de données pour vous assurer d'être en conformité avec les lois que ces organismes sont chargés d'appliquer.
- **Partenariat avec des experts locaux**
Dans de nombreuses régions où le cloud computing est largement utilisé, les lois sur la conformité peuvent changer rapidement. C'est pourquoi il est toujours utile d'être en relation avec un spécialiste des accords réglementaires dans le pays où la région où vous stockez et traitez des données. À ce titre, les fournisseurs de services cloud (CSP) qui opèrent sur un territoire ont généralement déjà conclu des accords avec les autorités locales.

Remarques importantes pour les entreprises souhaitant établir une souveraineté des données

Alors que le sujet de la souveraineté des données continue de préoccuper les citoyens et les organismes de réglementation du monde entier, les approches de cloud souverain aident les entreprises à garantir l'intégrité de leurs données, quel que soit l'endroit où elles sont stockées et traitées.

Dans les années à venir, la manière dont les entreprises collectent, sécurisent, stockent et contrôlent l'accès à leurs données aura des répercussions considérables sur la croissance et la sécurité, en particulier si elles souhaitent exploiter de nouvelles technologies riches en données telles que l'IA et le ML. La souveraineté des données est donc un enjeu majeur, et le choix d'un fournisseur de cloud qui maîtrise parfaitement le sujet les aidera à mettre en œuvre une approche solide du cloud souverain et à atteindre leurs objectifs de transformation numérique. Les partenaires dans les régions et les pays où les entreprises cherchent à établir un environnement cloud doivent disposer de stratégies pour atténuer les risques courants tels que les cyberattaques, les catastrophes naturelles et les temps d'arrêt.

Enfin, les entreprises qui cherchent à élaborer une approche solide en matière de souveraineté des données et de cloud souverain doivent s'assurer que leur fournisseur de cloud dispose d'une stratégie cloud globale robuste qui respecte les législations des pays ou des régions dans lesquels ils opèrent. Voici quelques-uns des éléments les plus importants à prendre en compte par les entreprises qui envisagent de faire appel à des CSP et à d'autres partenaires potentiels pour élaborer une approche rigoureuse de la souveraineté des données.

Fonctionnalités de gouvernance des données : l'approche d'un CSP en matière de gouvernance des données doit démontrer qu'il dispose des règles et procédures adéquates pour gérer correctement les données sensibles et appliquer les restrictions d'accès nécessaires. Il doit également fournir des audits réguliers, prouvant que les directives qu'il a mises en place sont respectées.

Contrats de niveau de service (SLA) : lorsqu'il s'agit d'établir un SLA pour la souveraineté des données dans un environnement cloud souverain, les trois domaines les plus importants à couvrir sont le contrôle (cloud management), la disponibilité et les performances.

Conformité : les CSP et autres partenaires qui aident les entreprises à se conformer aux exigences en matière de souveraineté des données doivent posséder une connaissance approfondie des différentes législations de protection des données en vigueur dans les régions où ils opèrent. Idéalement, les entreprises et les CSP devraient partager la responsabilité de se tenir informés des nouvelles réglementations et d'élaborer des stratégies pour y faire face.

Chiffrement des données : il est essentiel que les CSP dans l'espace cloud souverain disposent de solides capacités de chiffrement des données, telles que les clés cryptographiques, afin de garantir la sécurité et l'accessibilité des données sensibles. Ces clés transforment les données en un algorithme de chiffrement qui ne peut être déchiffré que par une personne disposant des autorisations nécessaires (c.-à-d. une clé). Les entreprises bénéficient ainsi d'une assurance et d'un contrôle techniques complets sur qui peut accéder à leurs données et quand.

Résilience : une approche rigoureuse de la souveraineté des données et des environnements de cloud souverain doit comprendre de solides fonctionnalités de résilience. Les entreprises ne devraient s'adresser qu'aux CSP ayant fait leurs preuves en matière d'aide aux clients dans leurs efforts de résilience et de reprise dans les pays ou régions concernés. Dans le cas d'un environnement cloud souverain, tous les déploiements cloud doivent disposer de capacités de récupération et de basculement intégrées adaptées à chaque domaine de conformité pour la région dans laquelle les données sont stockées.

Rapport

Découvrez pourquoi KuppingCole classe IBM parmi les leaders

Le rapport KuppingCole sur les plateformes de sécurité des données offre des conseils et des recommandations pour trouver les produits de protection et de gouvernance des données sensibles qui répondent le mieux aux besoins des clients.

[Lire le rapport](#) →

Webinaire

Explorer le paysage réglementaire et l'impact sur la protection et le stockage des données

Découvrez des stratégies pour simplifier et accélérer votre feuille de route de résilience des données tout en répondant aux dernières exigences de conformité réglementaire.

[Regarder le webinaire](#) 

Ressources

Rapport

L'impact économique total (TEI) de Guardium Data Protection

Découvrez les avantages et le retour sur investissement de IBM Security Guardium Data Protection dans cette étude TEI de Forrester.

[Lire le rapport](#) →

Webinaire

Explorer le paysage réglementaire et l'impact sur la protection et le stockage des données

Découvrez des stratégies pour simplifier et accélérer votre feuille de route de résilience des données tout en répondant aux dernières exigences de conformité réglementaire.

[Regarder le webinaire](#) 

**Solutions de sécurité et de protection des données**
Protéger les données dans chaque environnement, assurez votre conformité aux réglementations en matière de confidentialité et réduisez la complexité opérationnelle.

**IBM Guardium**
Découvrez IBM Guardium, une gamme de logiciels de sécurité des données qui protège les données sensibles sur site et dans le cloud.

[Découvrir les solutions de sécurité des données](#) →

[Découvrir IBM Guardium](#) →

**Services de sécurité des données**
IBM fournit des services complets de sécurité des données pour protéger les données, les applications et l'IA de votre entreprise.

[Explorez les services de sécurité des données](#) →

Passez à l'étape suivante

Protégez les données de votre entreprise dans les clouds hybrides et simplifiez les exigences de conformité grâce à des solutions de sécurité des données.

Découvrir les solutions de sécurité des données

[Réserver une démo en direct](#) →