Localisation des données

Perspectives de la stratégie AWS

Juillet 2018

aws

[Perspectives de la stratégie]

© 2018, Amazon Web Services, Inc. ou ses sociétés apparentées. Tous droits réservés.

Mentions légales

Ce document est fourni à titre informatif uniquement. Il présente l'offre de produits et les pratiques actuelles d'AWS à la date de publication de ce document, des informations qui sont susceptibles d'être modifiées sans avis préalable. Il incombe aux clients de procéder à leur propre évaluation indépendante des informations contenues dans ce document et chaque client est responsable de son utilisation des produits ou services AWS, chacun étant fourni « en l'état », sans garantie d'aucune sorte, qu'elle soit explicite ou implicite. Ce document ne crée pas de garanties, représentations, engagements contractuels, conditions ou assurances à l'encontre d'AWS, de ses affiliés, fournisseurs ou concédants de licence. Les responsabilités et obligations d'AWS vis-à-vis de ses clients sont régies par les contrats AWS. Le présent document ne fait partie d'aucun contrat et ne modifie aucun contrat entre AWS et ses clients.

Sommaire

Introduction

Dans l'environnement informatique complexe actuel, les organisations du secteur public continuent à exprimer des inquiétudes légitimes quant à la sécurité de leurs données. En conséquence, certains gouvernements ont déterminé que rendre obligatoire la localisation des données, l'exigence que tous les contenus client traités et stockés dans un système informatique demeurent au sein des frontières d'un pays spécifique, offre une couche supplémentaire de sécurité. La localisation des données reflète une combinaison de problèmes principalement associés aux risques de sécurité perçus (et dans certains cas réels) quant à l'accès des parties tierces aux données, agences étrangères du maintien de l'ordre incluses. Les clients du secteur public veulent l'assurance que leurs données sont protégées contre les accès indésirables d'agresseurs malveillants, mais également d'autres États.

Le cas d'une localisation stricte des données restreint parfois l'utilisation de fournisseurs de services de cloud (CSP, cloud service providers) à grande échelle et multinationaux, souvent appelés CSP à grande échelle. Les inquiétudes relatives à la cybersécurité générale, ainsi que celles concernant l'excès potentiel de la surveillance gouvernementale par certains pays, ont contribué au souci constant de conserver les données à l'intérieur du pays. Cependant, cette restriction est contreproductive par rapport à l'objectif de sécuriser efficacement les données du secteur public. Comme expliqué ci-dessous, un opérateur cloud à très grande échelle, qui peut se trouver en dehors du pays, fournit à la totalité de sa base de clients la possibilité d'atteindre de hauts niveaux de protection des données à travers les protections de leur propre plateforme et d'outils clé en main pour leurs clients Les opérateurs cloud procèdent ainsi tout en préservant en même temps la souveraineté régulatrice de l'État-nation.

Les services de cloud à grande échelle représentent une disruption transformationnelle dans la technologie, en raison du haut degré d'efficacité, d'agilité et d'innovation afin de fournir une sécurité d'envergure internationale pour soutenir leurs clients. Les opérateurs cloud à très grande échelle conçoivent, conduisent et gèrent les offres afin de permettre aux clients des différents secteurs (commercial, public, réglementé) de faire face à quelques-unes des failles et quelques-uns des risques de sécurité les plus courants. Les clients s'appuient sur les offres d'un opérateur cloud à grande échelle pour intégrer les pratiques de sécurité qui sont dynamiques et sensibles aux menaces en temps réel, améliorant de façon spectaculaire la posture de sécurité de chaque client. Les opérateurs cloud, pour leur part, ont tous la juste motivation de préserver une cybersécurité de classe internationale, car ils seraient confrontés à d'importantes conséquences à long terme, y compris les impacts associés à la mise en danger d'un système, la perte de la confiance des clients et les dommages causés à la marque. Autrement dit, une sécurité optimale (la meilleure sécurité de sa catégorie) est obligatoire pour la réussite d'un opérateur cloud. La sécurité doit être pleinement intégrée à la conception, au développement et aux opérations de services de cloud à grande échelle.

Le présent document aborde les points suivants :

- Risques réels et perçus pour la sécurité exprimés par les gouvernements quand ils exigent la localisation des données dans le pays.
- Impact sur le commerce, le secteur public et l'économie de stratégies de localisation de données dans le pays, avec l'accent mis sur les données gouvernementales.
- Remarques à l'attention des gouvernements à évaluer avant d'appliquer les exigences qui peuvent de façon non intentionnelle limiter les objectifs de transformation numérique du secteur public et conduire à une augmentation du risque de cybersécurité.

Pourquoi la localisation des données n'offre-t-elle pas une meilleure sécurité ?

La propriété et l'emplacement géographique des données sont devenus un thème majeur en matière de cybersécurité et des politiques d'usage du cloud autour du globe. Historiquement, la commande et le contrôle des données d'entreprise sensibles impliquaient l'hébergement des informations en local sur site ou dans les installations propriété de l'entrepreneur et facilement accessibles dans le pays. Être pleinement propriétaire de la totalité de la « pile » du sol au plafond jusqu'aux logiciels installés sur les serveurs donnait aux individus le sentiment réconfortant que leurs données étaient aussi sécurisées que possible. Ces raisons continuent d'exister pour de nombreux gouvernements.

Au fur et à mesure de l'évolution de la technologie, trois réalités fondamentales ont perturbé le modèle traditionnel de « contrôle de la totalité de la pile » :

Quel que soit l'emplacement physique, si les systèmes informatiques sont d'une façon ou d'une autre connectés à Internet (ou à d'autres réseaux multi-parties), même indirectement, ils sont exposés à un risque considérable.

1. **La plupart des menaces sont orchestrées à distance.** L'emplacement physique des données n'a qu'un faible impact, voire aucun, sur les menaces propagées via Internet. Les systèmes connectés à Internet exposent une organisation à un vaste ensemble de menaces, toutes susceptibles de se propager à partir de n'importe quel emplacement. Par exemple, le récent logiciel « ransomware » Petya a affecté les services de santé, en paralysant leurs opérations et leur capacité à prendre en charge des patients. Il s'agissait là du résultat d'un logiciel malveillant affectant la disponibilité de leurs centres de données locaux connectés à Internet. En dépit d'un effort massif pour sécuriser les systèmes interconnectés via des pare-feux et autres dispositifs anti-intrusion, l'expérience a montré que la sécurité d'un périmètre était une très petite part d'un système protégé. Quel que soit l'emplacement physique, si les systèmes informatiques sont d'une façon ou d'une autre connectés à Internet (ou à d'autres réseaux multi-parties), même indirectement, ils sont exposés à un risque considérable et susceptibles d'être l'objet d'un large éventail de menaces d'accès logiques.
2. **Les processus manuels présentent des risques d'erreur humaine.** L'échec des processus humains joue un rôle dans la cause première (si ce n'est dans la totalité de la cause) de la défaille de la plupart des systèmes de cybersécurité. Un exemple fréquent est l'échec de la correction des systèmes vulnérables avec les mises à jour logicielles publiées de nombreux mois avant une attaque. Le processus manuel de mise à jour des systèmes avec les derniers correctifs est difficile et n'est pas faisable régulièrement sans automatisation.
3. **Les menaces internes prévalent en tant que risque significatif.** L'immense majorité des principaux accès non autorisés à des données se sont produits au travers d'erreurs non intentionnelles ou d'un comportement malveillant par des personnes utilisant des comptes autorisés qui avaient le droit d'accéder à ces données. Les pirates ou les accès non autorisés à des données sensibles de ces dernières années étaient largement attribuées à de médiocres pratiques en matière de cybersécurité. Les scénarios de compromission de compte d'accès les plus courants sont les suivants :
    - Par inadvertance : les informations d'identification sont perdues ou mal gérées et un hacker peut donc agir au sein du système en tant qu'utilisateur valide.
    - Ingénierie sociale : les piratages par phishing et par ingénierie sociale qui dupent les utilisateurs ou les administrateurs, et les conduisent à divulguer les informations d'identification à des pirates.

- Malveillance : menace interne classique, avec des acteurs au sein de l'organisation animés d'une intention malveillante.

L'emplacement physique n'a pas d'influence sur les scénarios répertoriés ci-dessus.

Dans le climat actuel, la gestion des risques constitue une tâche encore plus importante si l'on considère les technologies mobiles, ainsi que les inter-relations entre les entités externes et les entités internes. Tout système connecté à Internet, directement ou indirectement, représente un vecteur d'attaque crédible, indépendamment de l'emplacement physique de l'infrastructure ou du système. Au fur et à mesure que la technologie progresse et modifie les vecteurs et vulnérabilités qui menacent les clients, les gouvernements doivent réévaluer la façon dont ils modélisent leurs stratégies et leur tolérance aux risques. Des exemples concrets ont montré que le stockage des données sur vos propres serveurs, dans votre propre centre de données et dans votre propre pays ne constituait nullement une base appropriée pour sécuriser vos données.

Par exemple, un accès non autorisé à des données sensibles d'une agence gouvernementale américaine affectant plus de 20 millions d'employés fédéraux s'est produite dans un environnement sur site, à la suite de l'exposition d'informations d'identification d'un utilisateur. Celles-ci étaient compromises et utilisées sur Internet depuis différents emplacements, ignorant toutes les protections que l'environnement sur site proposait. La compromission de cette agence gouvernementale est un bon exemple des menaces venant d'Internet n'ayant aucun rapport avec l'emplacement géographique des données.

Ce problème ne s'applique pas uniquement aux systèmes connectés à Internet. Les systèmes sans connexion directe à Internet peuvent offrir aux utilisateurs un accès via une connexion VPN (Virtual Private Network, réseau privé virtuel) à partir d'un ordinateur portable, d'un ordinateur familial ou d'un appareil mobile. Les accès non autorisés à des données ne requièrent pas l'accès physique à un serveur, mais exploitent à la place un manque de contrôles de sécurité logiques implantés efficacement. Ce manque illustre que les exigences en matière de localisation de données n'apportent pas de niveau de sécurité supplémentaire par rapport aux menaces les plus répandues. Les exigences de localisation géographique, par conséquent, offrent peu de pertinence pour protéger les informations contre les menaces les plus répandues. À la place, les meilleurs mécanismes de protection, détection, réponse et récupération consistent à utiliser la sécurité transformationnelle qu'offre un opérateur cloud à grande échelle au travers de la modernisation et de l'automatisation. Les opérateurs cloud à grande échelle, comme AWS, réfléchissent aux bonnes pratiques de sécurité techniques et opérationnelles et investissent dans celles-ci, car elles sont au cœur de leurs opérations et de leurs offres. Les clients en récoltent les fruits quand ils mettent à profit un opérateur cloud tel que les offres de cloud et d'infrastructure d'AWS.

Gartner[1] et IDC[2], deux organisations majeures de recherche informatique, ont établi que la posture sécurité des principaux opérateurs cloud était égale ou supérieure aux meilleurs centres de données professionnels et que cette sécurité ne devait plus être envisagée comme un inhibiteur fondamental à l'adoption des services de cloud publics. De ce fait, les entreprises profitent réellement de la sécurité native du cloud.

1 http://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

2 Pete Lindstrom, « Assessing the Risk: Yes, the Cloud Can Be More Secure Than Your On-Premises Environment », International Data Corporation (juillet 2015).

Pourquoi le cloud n'a-t-il pas d'effet sur le risque de divulgation forcée des données ?

Pour certains gouvernements, les exigences en matière de localisation des données sont destinées à atténuer les risques associés à l'accès d'une autre entité à leurs données. Cette section a pour objectif d'aborder le risque perçu de la capacité d'une entité à « forcer la divulgation » des données d'une entité souveraine quand celles-ci sont stockées au sein d'un opérateur cloud à grande échelle. Le concept de divulgation forcée ou d'accès forcé fait référence aux droits d'accès aux données par les gouvernements ou leurs agents à l'aide de moyens légaux. Le résultat de ces types de droits d'accès peut impliquer que les entreprises soient soumises à des lois et réglementations applicables aux niveaux national, régional et sectoriel d'un pays donné, et qu'elles soient contraintes d'autoriser l'accès ou de transmettre les données en conformité avec de telles lois ou réglementations. La difficulté ressentie est qu'une divulgation forcée peut potentiellement laisser le propriétaire sans aucune capacité d'empêcher l'accès à ses données par une entité prétendant invoquer la loi applicable. Cependant, l'accès légal aux données d'une nation souveraine n'est pas un problème propre au cloud.

La possession du système physique, que ce soit directement ou via un contrat externalisé, ne réduit pas le risque d'un accès forcé, car il existe déjà d'autres dispositifs légaux qui confèrent aux gouvernements d'une juridiction les moyens d'accéder aux données stockées dans une autre juridiction. Par exemple, les traités d'entraide mutuelle judiciaire (MLAT)[3] et les commissions rogatoires[4] ont été mis en place pour régir les demandes de données d'une nation souveraine bien avant l'apparition de la technologie du cloud.

En comparaison avec l'environnement local traditionnel, l'application de la loi doit généralement surmonter plusieurs obstacles lors de la tentative de forcer un opérateur cloud à divulguer les données d'un autre client. La force publique ne peut rechercher ou saisir les données stockées sur les serveurs d'un opérateur cloud sans respecter les infrastructures légales prenant en charge un ensemble étroitement ciblé d'objectifs de police. En outre, les opérateurs cloud peuvent relever le défi de demandes qui sont trop larges, dépassent l'autorité du demandeur ou ne respectent pas totalement la loi en vigueur.

Plus important encore, les opérateurs cloud comme AWS s'engagent totalement à fournir aux clients concernés la notification des demandes de divulgation des données ; le client peut alors coopérer avec les autorités et/ou prendre les mesures appropriées pour se prémunir contre toute divulgation inappropriée de ses données. Il importe de reconnaître que ce défi complexe n'est pas propre au gouvernement américain ou aux entreprises basées aux États-Unis, car toute entreprise multinationale est soumises aux lois et réglementations applicable aux niveaux national, régional et sectoriel d'un pays donné, quel que soit l'emplacement des données.

---

3 Les traités d'entraide mutuelle judiciaire (MLAT) autorisent généralement l'échange de preuves et d'informations dans les affaires pénales et associées. https://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm

4 Les commissions rogatoires sont des demandes adressées par le tribunal d'un pays à celui d'un autre pays. Elles sollicitent l'exécution d'un acte qui, s'il était accompli sans l'autorisation du tribunal étranger, pourrait constituer une violation de la souveraineté de ce pays. Les commissions rogatoires peuvent être utilisées pour permettre le service du processus ou pour obtenir des preuves si les lois du pays étranger l'autorisent. https://travel.state.gov/content/travel/en/legal/travel-legal-considerations/internl-judicial-asst/obtaining-evidence/Preparation-Letters-Rogatory.html

Limitation du risque de divulgation forcée

Depuis le 20e siècle, de nombreux pays ont mis en place des dispositifs légaux pour permettre l'accès aux informations stockées à l'étranger en réponse aux demandes légales appropriées d'informations relatives à des enquêtes et poursuites criminelles. Par exemple, une entreprise travaillant dans le pays X peut être soumise à une demande légale d'informations, même si les contenus sont stockés dans le pays Y selon une infrastructure juridique bilatérale et multilatérale bien établie. Dans la plupart des cas, le dispositif légal reconnu est un traité d'entraide mutuelle judiciaire (MLAT).

En plus des MLAT nationaux bilatéraux, il existe aussi des MLAT régionaux clés, comme le MLAT inter-Amériques, le MLAT Union européenne-États-Unis et le MLAT ASEAN. En l'absence d'un MLAT, les pays peuvent obtenir des commissions rogatoires pour obtenir de l'aide auprès de gouvernements étrangers. La loi de chaque juridiction contiendra les critères qui doivent être satisfaits pour que le représentant de la loi puisse établir une demande valide. Par exemple, l'agence gouvernementale demandant l'accès devra obtenir une décision judiciaire ou un mandat attestant qu'elle a une raison valide de demander l'accès au contenu. Bien que mécanismes légitimes, ces instruments légaux n'étaient pas destinés à aborder l'accès de la force publique aux données dans un monde numérique.

> Les lois régissant l'accès aux données stockées à l'étranger par les agences du maintien de l'ordre dans le cadre d'enquêtes sur des graves délits, comme le terrorisme, n'ont pas été écrites avec la technologie moderne à l'esprit. Il en a résulté des cas où des entreprises technologiques se conformant à une garantie judiciaire selon les lois d'un pays ont également été confrontées au risque de violer les lois d'un autre pays interdisant la divulgation. Le CLOUD Act fournit une nouvelle infrastructure pour relever le défi des demandes de la force publique lorsqu'il existe des accords cadres entre les États-Unis et un autre pays. Il confirme aussi, selon les principes de la courtoisie internationale, le droit des fournisseurs de service de s'opposer à la divulgation de données si cette dernière entrait alors en conflit avec les lois d'un autre pays, même en l'absence d'un contrat cadre. Il permet aussi aux fournisseurs de services de cloud de divulguer les données aux gouvernements émettant des ordres ou des mandats pour obtenir des informations à partir de faits démontrant la cause probable qu'un délit grave s'est produit et que les informations recherchées sont directement associées à ce délit.

Dans une tentative d'alignement des lois avec la technologie moderne, les États-Unis ont voté le Clarifying Lawful Overseas Use of Data (CLOUD) Act en mars 2018. Le CLOUD Act offre un troisième mécanisme international légal pour acquérir les données stockées à l'étranger au travers de demandes directes adressées au fournisseur de services.[5] Le CLOUD Act décrit les procédures pour que les États-Unis concluent des accords cadres avec d'autres pays. Ces accords cadres visent à lever les restrictions légales qui empêchent certaines nations étrangères de rechercher directement des données auprès des fournisseurs américains, sous réserve que les États-Unis aient déterminé que les lois de la nation étrangère protègent de façon adéquate la confidentialité et les libertés civiles. Conformément au CLOUD Act, les opérateurs cloud ont le droit de s'opposer à la divulgation des informations au cas où celle-ci entrerait en conflit avec les lois d'un autre pays. Le MLAT, les commissions rogatoires et les accords cadres selon le CLOUD fournissent tous des mécanismes légaux internationaux réciproques pour l'accès de la force publique aux données stockées à l'étranger.

5 Le CLOUD Act s'applique à la fois aux États-Unis et aux compagnies étrangères opérant aux États-Unis qui fournissent « des services de communications électroniques » et/ou « des services informatiques distants », tels que les entreprises qui proposent des services de courriel, de messagerie électronique ou de stockage dans le cloud au public.

Les lois nationales d'un pays s'appliquent généralement à toutes les sociétés exerçant des activités dans ce pays, peu importe où se trouve le siège de la société ou si ces informations sont stockées dans le cloud, dans un centre de données sur site ou dans des dossiers physiques. Tandis que les nations poursuivent la numérisation et évoluent vers des sociétés modernes fondées sur l'information, les régimes d'accès contraint légaux à l'appui d'enquêtes sur des délits graves impactant la sécurité nationale, comme le terrorisme, ont aussi évolué. La promulgation du CLOUD Act constitue une autre infrastructure visant à renforcer le processus légal pour les demandes de la force publique dans ce contexte moderne.

Restreindre les opérateurs cloud à une seule juridiction n'empêche pas davantage les gouvernements d'accéder aux données

Une analyse légale indépendante auprès des premiers utilisateurs à avoir adopté le cloud a évalué les lois propres à chaque pays régissant l'accès des forces de l'ordre aux données basées sur un cloud stocké à l'étranger. Après l'évaluation de dix juridictions internationales (Australie, Canada, Danemark, France, Allemagne, Irlande, Japon, Espagne, Royaume-Uni et États-Unis), cette étude a révélé que la restriction des opérateurs cloud à une seule juridiction n'empêche pas davantage les gouvernements d'accéder aux données.

En réalité, de tels accès forcés se produisent dans un nombre de cas très limité et, généralement, seulement s'il s'agit d'un besoin extrême d'informations (par exemple, pour éviter des événements liés au terrorisme). Pour atténuer encore plus ce faible risque, les organisations peuvent faire preuve de diligence raisonnable et créer leurs propres protections avec les services cloud disponibles. Dans AWS, des atténuations telles que le chiffrement des données au repos et en transit, la décomposition et la distribution de données, et des stratégies de création de jeton peuvent être employées, entraînant une charge minime sur les ressources par rapport à une solution sur site.

AWS est vigilant quant à la protection des contenus de ses clients, quelle que soit la provenance d'une demande de contenu ou l'identité du client. AWS ne divulguera pas les contenus de ses clients sauf en cas d'obligation face à un ordre légalement valable et exécutoire, tel qu'une assignation à comparaître ou une décision judiciaire. AWS examine attentivement chaque demande afin de vérifier son authenticité et s'assurer qu'elle respecte la loi en vigueur. AWS s'opposera aux demandes dont la portée est excessive, qui dépassent l'autorité du demandeur ou qui ne respectent pas totalement la loi en vigueur. Sauf si la loi l'interdit, AWS essaye également de rediriger la demande directement vers le client, ce qui offre à ce dernier la possibilité de prendre des mesures à l'encontre de la demande. Des informations supplémentaires sont disponibles dans notre dernier rapport sur la transparence et dans les Directives relatives à l'application de la loi d'Amazon.[6]

6 http://d0.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf

Pourquoi le risque d'accès non autorisé est-il moindre dans le cloud ?

Pour certains gouvernements, les exigences en matière de localisation des données sont destinées à atténuer les risques associés à l'accès d'une autre entité à leurs données. Cette section a pour objectif d'aborder la hausse perçue de risques d'accès non autorisés lorsque vous utilisez un opérateur cloud à grande échelle. L'accès non autorisé est la menace la plus courante que tentent les adversaires essayant d'accéder aux données des clients par différents moyens. Un accès non autorisé peut inclure les problèmes liés à l'accès de tiers, y compris la possibilité de menaces d'initiés ou de personnes extérieures mal intentionnées.

Les exigences de localisation des données ne parviennent pas à contrer les outils couramment utilisés par les attaquants pour y accéder. L'exploitation de ces vecteurs résulte pratiquement toujours d'un échec des disciplines de cyber-hygiène de base, telles que la gestion des stocks d'un système, la gestion de la configuration, le chiffrement des données et la gestion des accès privilégiés.

Réduction du risque d'accès non autorisé

Empêcher les accès non autorisés nécessite la pratique d'une bonne hygiène de sécurité et l'implémentation de solides capacités de prévention et de détection. Par exemple, les systèmes doivent être conçus pour limiter le « rayon d'impact » de toute intrusion afin qu'un nœud compromis ait un impact minimal sur tout autre nœud dans l'entreprise. Les opérateurs cloud à grande échelle, comme AWS, fournissent un environnement complet d'outils de sécurité pour permettre aux clients de conserver des communications chiffrées et mettre en place des protections contre les falsifications pour atténuer le risque d'accès non autorisé. AWS n'a ni la visibilité ni la connaissance du contenu du compte client, et ignore donc si ce contenu contient ou non des informations personnelles. Les clients AWS sont habilités à utiliser différentes techniques telles que le chiffrement,[7] la création de jeton, la décomposition des données ou l'utilisation de techniques de leurres et la cyber tromperie pour que le contenu ne puisse pas être compris par AWS ou d'autres parties cherchant à accéder à leur contenu.

- Chiffrement - Un chiffrement approprié des données permet de les rendre illisibles. Cela signifie que le fait de stocker les données chiffrées dans le cloud, quel que soit leur emplacement, peut fournir une protection adéquate contre l'immense majorité des menaces d'exfiltration. Il est crucial que les clés de chiffrement soient soigneusement gérées afin de s'assurer de la présence de solides protections contre toute tentative d'interception par une partie tierce. AWS propose des services à même de fournir ces capacités au niveau de l'entreprise avec AWS CloudHSM ou AWS Key Management Service (KMS).[8] Le client décide du degré de contrôle dont il souhaite disposer sur la méthode de chiffrement, le stockage des clés cryptographiques et la gestion des clés cryptographiques utilisées avec ses données.[9]

---

7 AWS autorise les clients à utiliser leurs propres mécanismes de chiffrement pour la quasi-totalité des services AWS, y compris Amazon S3, Amazon EBS, Amazon DynamoDB et Amazon EC2. Les tunnels IPSec vers VPC sont également chiffrés. Amazon S3 propose également Server Side Encryption à ses clients. Les clients peuvent aussi utiliser des technologies de chiffrement tierces.

8 Le service AWS CloudHSM (Hardware Security Module) vous permet de protéger vos clés de chiffrement au sein des modules HSM conformes aux normes gouvernementales (FIPS 140-2 niveau 3) relatives à la gestion sécurisée des clés, y compris une solide protection contre toute falsification. AWS KMS, certifié FIPS 140-2 niveau 2, offre un service similaire, mais plus évolutif et plus étroitement intégré à un vaste ensemble de services AWS. Les protections sont ainsi fournies automatiquement à partir de simples modifications de la configuration du service. À l'aide de l'un de ces services, vous pouvez générer, stocker et gérer de manière sécurisée les clés de chiffrement utilisées pour le chiffrement des données de telle sorte que vous seul puissiez y accéder. Pour plus d'informations, consultez https://aws.amazon.com/cloudhsm/ et https://aws.amazon.com/kms/.

9 Les options de chiffrement AWS sont détaillées dans les liens suivants : 1) Sécurisation des données au repos avec le chiffrement, 2) Protection des données à l'aide d'un chiffrement dans Amazon S3, 3)Détails cryptographiques d'AWS Key Management Service, et 4) Présentation des processus de sécurité AWS.

- Création de jeton – La création de jeton est un processus qui vous permet de définir une séquence de données pour représenter une information sensible par ailleurs (par exemple, un jeton pour représenter le numéro de carte de crédit d'un client). Un jeton n'a pas de signification en lui-même et ne peut pas en retour être associé aux données qu'il représente sans que le système de création de jeton ne soit utilisé. Il est possible de construire des coffres de jetons dans les VPC afin de stocker les informations sensibles sous une forme chiffrée tout en partageant les jetons avec les services approuvés dans le but de transmettre des données brouillées. De plus, AWS collabore avec un certain nombre de partenaires spécialisés dans la fourniture de services de création de jeton qui s'intègrent aux bases de données les plus répandues et à d'autres services de stockage.

- Décomposition des données – Il s'agit d'un processus qui réduit les ensembles de données en éléments non identifiables qui n'ont aucune signification.[10] Ces éléments ou fragments sont ensuite stockés de manière distribuée de telle sorte que la mise en danger d'un nœud ne produise qu'un fragment de données insignifiant. L'un des avantages spécifiques de cette technique est qu'elle nécessite que le hacker mette en péril tous les nœuds, obtienne tous les fragments et connaisse l'algorithme (ou modèle de fragmentation) pour reconstituer les données d'une manière cohérente.

- Défense par cyber tromperie – Les architectures et solutions de cyber tromperie peuvent constituer un composant clé pour atténuer les attaques adverses avancées. Les solutions fondées sur la tromperie peuvent utiliser des pièges et des leurres sophistiqués pour offrir à l'agresseur le sentiment qu'il a pénétré le système, alors qu'en réalité il est dérouté vers un environnement hautement contrôlé. Les renseignements sur l'agresseur sont collectés afin d'atténuer les menaces futures et l'attaque est neutralisée.

Autre inquiétude associée à l'accès non autorisé, l'accès d'un tiers au contenu du client et l'adéquation des mesures de contrôle destinées à empêcher les accès non autorisés par le personnel de l'opérateur cloud. L'accès de parties tierces aux systèmes AWS est alloué sur la base du moindre privilège, approuvé par une personne agréée avant la mise à disposition de l'accès et supervisé par un employé d'AWS. Les obligations et zones de responsabilité (demande et approbation d'accès, demande et approbation de gestion des modifications, etc.) doivent être réparties entre différentes personnes afin de réduire le risque de modification non autorisée ou non intentionnelle, ou de mauvais usage des systèmes AWS. Le personnel AWS ayant besoin, pour des raisons professionnelles, d'accéder au niveau de gestion doit commencer par utiliser l'authentification MFA (Multi-Factor Authentication), distincte des informations d'identification Amazon standard, pour accéder aux hôtes d'administration conçus dans ce but. Ces hôtes d'administration sont des systèmes spécifiquement conçus, développés, configurés et renforcés pour protéger le niveau de gestion. Un tel accès est consigné et vérifié. Dès lors qu'un employé n'a plus de motif professionnel d'accéder au plan de gestion, les autorisations et l'accès à ces hôtes et aux systèmes concernés sont révoqués. AWS a implémenté une stratégie de verrouillage de gestion qui est systématiquement mise en œuvre. Le verrouillage de la session est maintenu jusqu'à l'exécution de procédures d'identification et d'authentification établies.

AWS surveille également la gestion distante non autorisée, et déconnecte ou désactive rapidement les accès distants non autorisés, une fois qu'ils ont été détectés. Toutes les tentatives d'accès administratif distant sont enregistrées. Les journaux eux-mêmes sont vérifiés, non seulement par des personnes afin de déceler toute activité suspecte, mais aussi par des systèmes automatiques de Machine Learning développés par l'équipe de sécurité d'AWS pour détecter tout modèle d'accès

10 Un tableau de recherche est disponible sur les techniques de décomposition des données. Dans le cadre de la rédaction du présent document, nous avons consulté une enquête menée par Kapusta et Memmi (20 juin 2017) et intitulée « Data protection by means of fragmentation in various different distributed storage systems » (Protection des données au moyen de la fragmentation dans les différents systèmes de stockage distribués).

inhabituel susceptible d'indiquer des tentatives non autorisées d'accès aux données. En cas de détection d'une activité suspecte, les procédures de réponse aux incidents sont déclenchées. De plus, AWS a instauré des procédures et stratégies formelles afin de définir des normes d'accès logique aux hôtes et à l'infrastructure AWS. Les politiques identifient également les responsabilités fonctionnelles pour l'administration de l'accès logique et de la sécurité. Sauf interdiction explicite par la loi, AWS requiert que tous les employés soient soumis à une enquête sur leurs antécédents, à la mesure de leur poste et de leur niveau d'accès.

Enfin, les instances virtuelles des clients sont exclusivement contrôlées par le client bénéficiant d'un accès racine complet ou d'un contrôle administratif sur les comptes, les services et les applications. Le personnel AWS n'a pas la possibilité de se connecter aux instances des clients.

Cloud à grande échelle: Approche transformationnelle de la sécurité

> Un autre corollaire imprévu des exigences de localisation des données nationales est que les hackers peuvent gagner en précision lorsqu'ils ciblent des systèmes en sachant que les données résident dans des emplacements spécifiques.

Les principaux fournisseurs de services de cloud (CSP), comme AWS, offrent aux clients la possibilité de développer pour leurs environnements une sécurité capable de s'adapter et hautement résiliente. Les opérations de restriction à des exigences nationales spécifiques réfrèneraient l'innovation en termes de services et entraveraient la capacité à contrebalancer les menaces, telles que celles qui ciblent la disponibilité. Le fait que les hackers puissent gagner en précision s'ils savent où résident les données au sein de zones spécifiques constitue un autre corollaire préjudiciable des contraintes géographiques dans le pays. Les opérateurs cloud à grande échelle proposent des offres et des architectures compatibles destinées à garantir des capacités de défense en[11] profondeur et enampleur[12]. La raison en est due à des mécanismes de sécurité intrinsèques à la conception et au fonctionnement des offres des opérateurs cloud à grande échelle.

Les six éléments suivants reflètent les principaux attributs de sécurité qui font partie intégrante d'un opérateur cloud à grande échelle comme AWS.

1. L'intégration en profondeur de la sécurité et de la conformité (rarement accomplie dans les systèmes traditionnels) signifie que la sécurité bénéficie directement de la conformité car les contrôles de sécurité sont constamment surveillés et mis à jour.
2. Les économies d'échelle ne s'appliquent pas seulement à la technologie, mais aussi au personnel et aux processus de sécurité. Il en résulte un retour sur investissement sans précédent par comparaison avec les systèmes traditionnels.
3. L'opérateur cloud prend en charge une part majeure de la « surface » de sécurité, et s'exécute avec une vigilance et une compétence professionnelles au-delà de pratiquement chaque client sur terre. Il en résulte que les clients peuvent recentrer leurs personnels et ressources de sécurité sur une plus petite part du défi, telle que la sécurité des applications.

---

11 La défense en profondeur désigne la pratique de mise en œuvre de plusieurs couches de contrôles de sécurité afin d'assurer l'indépendance et la redondance. En cas d'échec de l'une des couches de contrôle, la couche suivante est disponible pour atténuer les piratages ultérieures contre une ressource.

12 La défense en ampleur est l'approche qui consiste à utiliser les activités multidisciplinaires pour fournir de nombreux mécanismes de protection à chaque couche de défense identifiée. Généralement, cela signifie plus d'automatisation et plus de contrôles variés de sécurité à chaque couche.

4. Le cloud offre une visibilité, une homogénéité et une automatisation jamais rencontrées auparavant dans les systèmes traditionnels, et qui profitent massivement à la sécurité. Ces capacités incluent celles de l'audit et de la journalisation qui, par exemple, peuvent enregistrer les appels d'API qui consignent les actions prises par un opérateur cloud et susceptibles d'affecter le compte du client.

5. Les opérateurs cloud opèrent en quelque sorte comme un conteneur système qui offre bien plus de connaissances sur le fonctionnement et le comportement du système, y compris les opérations de sécurité, fournissant ainsi aux clients une couche supplémentaire de « défense approfondie ».

6. Grâce à un accès simple et économique aux nombreux comptes de stockage et à la capacité de traitement, les clients AWS « utilisent le cloud pour sécuriser le cloud » : ils exécutent l'analyse du Big Data sur les données de sécurité et les données des journaux, ce qui apporte plus de connaissances sur la posture de sécurité et se traduit par une correction beaucoup plus rapide des problèmes.

Avec la vitesse à laquelle se déroulent l'innovation et l'accroissement d'échelle, la sécurité du cloud ne peut que s'améliorer. Par exemple, au cours de la seule année écoulée, AWS a ajouté de puissantes fonctions de sécurité telles qu'Amazon GuardDuty[13], une gestion de détection des menaces qui surveille en permanence les comportements malveillants ou non autorisés ; Amazon Macie[14], une offre qui s'appuie sur l'apprentissage automatique pour protéger les données sensibles ; et AWS CloudHSM 2.0[15], une offre entièrement gérée qui utilise un équipement validé FIPS 140-2 Level 3[16] automatiquement déployé dans un cluster de zone de multi-disponibilité hautement disponible et redondante qui permet aux clients de générer, gérer et utiliser facilement leurs propres clés de chiffrement dans le cloud AWS, tout en fournissant à AWS zéro accès aux clés maîtres ou aux principales opérations de chiffrement.

Le chiffrement doit être considéré comme un service central car il peut agir comme moyen de protéger les données dans le cas où d'autres capacités échoueraient. Il ajoute une couche supplémentaire de sécurité, ainsi que l'assurance de la confidentialité et de l'intégrité des données en transit et au repos. L'association d'AWS KMS (AWS Key Management Service) et d'AWS CloudHSM se trouve au cœur d'une solution de chiffrement rigoureuse.[17] Les opérateurs cloud à grande échelle comme AWS offrent un chiffrement omniprésent qui peut être hors d'atteinte pour les opérations sur site. Par exemple, la validation AWS Key Management Service (KMS), FIPS 140-2 Level 2, propose une option BYOK (Bring Your Own Keys) qui permet aux clients d'utiliser leurs propres clés générées et stockées localement avec les services AWS. Les clients peuvent satisfaire à des exigences spécifiques de sécurité et de conformité par rapport à des charges de travail hautement sensibles grâce à la possibilité de conserver et gérer leurs clés en dehors d'AWS.

13 https://aws.amazon.com/guardduty/

14 https://aws.amazon.com/macie/

15 https://aws.amazon.com/cloudhsm/

16 FIPS 140-2, les exigences de sécurité pour les modules cryptographiques couvrent 11 domaines liés à la conception et à la mise en place d'un module de chiffrement.

17 https://d1.awsstatic.com/whitepapers/compliance/AWS_Logical_Separation_Handbook.pdf

Responsabilité d'un opérateur cloud : Sécurité native dans le cloud

L'infrastructure AWS est conçue et personnalisée pour le cloud, avec tous les éléments conçus pour intercommuniquer correctement et offrir la plus petite surface de piratage possible. En outre, les contrôles de sécurité physiques présents dans nos centres de données ont été conçus pour être parmi les plus contraignants au monde. L'architecture AWS a été examinée et validée en fonction de dizaines de cadres de conformité internationaux.[18] Nous recourons à des assesseurs et des auditeurs tiers indépendants pour évaluer et prouver notre adhésion à ces régimes, et fournir aux clients l'accès aux rapports obtenus et aux preuves à l'appui. Afin de satisfaire un large éventail d'exigences de sécurité, AWS développe ses centres de données et son architecture pour évoluer et avancer au rythme de l'innovation. Cette approche a conduit AWS à être approuvé par les gouvernements, les organisations militaires, les banques mondiales, les établissements de santé et autres organisations hautement sensibles.

Chez AWS, notre environnement unique a été une incitation à développer la plupart de nos propres outils de sécurité. Ceux-ci automatisent une grande partie des tâches quotidiennes et permettent à nos experts en sécurité de se concentrer sur les aspects essentiels de la protection de l'environnement. Nos outils se traduisent par des exigences de sécurité intégrées et respectées tout le long du cycle de vie du développement du système. Les préoccupations courantes de sécurité sont résolues dans les phases initiales de développement du système, ce qui permet à nos experts en sécurité de se concentrer sur l'atténuation des menaces avancées et complexes au niveau de la production.

Nos équipes de sécurité surveillent l'infrastructure 24 heures sur 24 et 7 jours sur 7, et sont parfaitement connectées à tous les principaux groupes et fournisseurs de sécurité pour identifier immédiatement les menaces potentielles. Elles procèdent ainsi à grande échelle, ce qui fait de l'organisation de la sécurité AWS quelque chose d'unique. Grâce à des algorithmes complexes pour parcourir des millions de comptes clients actifs exécutant pratiquement tous les types de charge de travail imaginables, nous rencontrons des problèmes qui ne se produisent qu'une seule fois par jour au cours de milliards d'opérations. Lorsque nous corrigeons ce problème, la correction s'applique à la totalité de la plateforme. Ce type de visibilité et de réponse n'est simplement pas atteignable pour l'immense majorité des organisations exploitant des centres de données sur site. La valeur qui provient d'une expertise privilégiée et d'une échelle massive explique pourquoi Gartner et IDC ont déterminé que les charges de travail Iaas (Infrastructure as a Service) du cloud public étaient confrontées à moins d'incidents de sécurité que celles des centres de données traditionnelles. Les études menées par Gartner estiment à au moins 60 % la réduction des incidents de sécurité.[19]

Responsabilité du client : Approche d'une architecture sécurisée

Les capacités de sécurité propres aux fournisseurs de cloud à grande échelle tels qu'AWS permettent aux clients de créer des architectures uniques pour atténuer les risques d'accès. Les installations sur site et similaires manquent de l'homogénéité, de l'économie d'échelle, de la visibilité et de l'automatisation que peuvent apporter les avancées majeures de la sécurité. Ces avancées sont nécessaires pour construire des systèmes hautement sécurisés qui peuvent parer les menaces en constante évolution que ce soit en interne ou en externe. Les installations sur site s'efforcent d'utiliser ces nouveaux concepts opératoires en raison des exigences de ressources pour le remaniement du réseau et l'acquisition de nouveaux systèmes, ainsi que la main-d'œuvre humaine en raison du manque d'infrastructures définies par logiciel. Les opérateurs cloud à grande échelle développent un niveau d'agilité et d'adaptabilité au sein de leur infrastructure afin de mettre en place organiquement

18 Consultez https://aws.amazon.com/compliance

19 https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

ces avancées de sécurité. Cela signifie que les clients peuvent utiliser plus rapidement les nouvelles avancées, car elles sont intégrées en mode natif aux offres des opérateurs cloud. Les clients peuvent ainsi élaborer des systèmes à l'aide d'architectures uniques telles que la micro-segmentation, les conceptions polymorphes[20] et les réseaux de duperie multiniveaux.

Par exemple, si nous regardons plus attentivement la conception basée sur la micro-segmentation dans AWS, un client peut utiliser un vaste ensemble de technologies dont Amazon Virtual Private Cloud (Amazon VPC), AWS Identity and Access Management (IAM), les groupes de sécurité, les listes de contrôle d'accès réseau, et les nombreux services de chiffrement et de journalisation, ainsi qu'AWS Certificate Manager pour former la base de construction d'un réseau « Zero Trust »[21] (Zero Trust Model ou ZTM). Par définition, le réseau ZTM peut offrir un réel avantage pour la diminution des menaces et la surveillance des performances. Les organisations ont un clair besoin d'implémenter un réseau ZTM ou une segmentation de sécurité similaire pour parer les menaces présentes, mais il est extrêmement difficile et onéreux de construire ce type d'architecture dans les environnements professionnels traditionnels. Le transfert vers un fournisseur de cloud public fournit aux organisations l'opportunité d'implémenter un réseau ZTM et concepts similaires sans la charge ressource et le coût importants associés à la construction/amélioration du réseau.

Rôles pour la protection des données

Il y a cinq concepts de base importants concernant la propriété et la gestion des données dans le modèle de responsabilité partagée :

1. Les clients restent les propriétaires de leurs données.
2. Les clients choisissent les zones géographiques dans lesquelles ils veulent stocker leurs données. Elles ne seront pas déplacées à moins que le client ne le souhaite.
3. Les clients peuvent télécharger ou supprimer leurs données à tout moment.
4. Les clients peuvent « crypto-supprimer » leurs données en supprimant les clés de chiffrement maîtres requises pour déchiffrer les clés des données, qui, à leur tour, sont requises pour déchiffrer les données.
5. Les clients doivent prendre en considération la sensibilité de leurs données et décider si et comment les chiffrer lorsqu'elles sont en phase de transition et au repos.

Les mesures de protection des données sont plus efficacement appliquées après que vous ayez défini les rôles de gestion des données pour déterminer les rôles et responsabilités des parties prenantes appropriées. La plupart des schémas de protection de données se différencient par le contrôleur des données (aussi appelé « utilisateur ») et le processeur de données et les obligations imposées basées sur ces rôles distincts. Par exemple, selon la Réglementation de l'Union européenne sur la protection générale des données, le contrôleur de données est responsable de la mise en place des mesures techniques et organisationnelles appropriées pour protéger les données personnelles contre la destruction accidentelle ou illégale, ou encore la perte accidentelle, l'altération, la divulgation ou l'accès non autorisé. Lorsque le traitement est effectué par un responsable de traitement de données pour le compte du contrôleur de données, ce dernier

20 En termes simples, la conception polymorphe permet la création de cibles mobiles, ce qui rend plus difficile les piratages réussis.

21 Le concept a été conçu à l'origine par Forrester Research. Il propose qu'il ne soit fait confiance à aucune entité sur le réseau. L'objectif est d'appliquer un accès sécurisé à toutes les ressources, qu'elles soient internes ou externes. Cela signifie qu'une organisation doit connaître et classer ses données, et tracer la carte de la façon dont ces données, et particulièrement les données sensibles, circulent entre le stockage, le traitement, le transit et les consommateurs. Puis, une fois que les données sont comprises, une organisation peut implémenter les mécanismes ZTM qui appliquent et automatisent le moindre privilège absolu, le chiffrement de bout en bout et l'inspection de la totalité du trafic.

est également responsable du choix d'un responsable du traitement offrant des mesures techniques et organisationnelles suffisantes pour régir le traitement à effectuer. Ces distinctions aident à délimiter les responsabilités entre les fournisseurs externalisés et leurs clients.

En tant que fournisseur d'infrastructure de service autonome entièrement placé sous le contrôle du client, concernant la façon dont les données sont traitées et si elles le sont, AWS fournit des services d'infrastructure aux clients qui souhaitent charger et traiter des contenus sur AWS. AWS n'a pas de visibilité ou de connaissance relative aux éléments que les clients téléchargent sur son réseau, et ignore par conséquent si ces contenus contiennent des données personnelles ou non. Les clients AWS peuvent également utiliser le chiffrement afin de rendre leurs contenus incompréhensibles pour AWS et toute partie tierce cherchant à accéder aux données.

Les services AWS ignorent les contenus, dans le sens où ils offrent le même niveau de sécurité élevé à tous les clients, quel que soit le type ou la région géographique des contenus traités ou stockés. En d'autres termes, AWS adopte le même niveau de sécurité à travers l'ensemble de nos offres. Cela signifie que nous adoptons le plus haut niveau de classification des données franchissant notre cloud commercial ou y étant stockées, et appliquons ces mêmes niveaux de protection à l'ensemble de nos offres et de nos clients. Ces offres sont ensuite mises en file d'attente par rapport à un haut niveau de sécurité et de conformité, qui a pour conséquence que les clients bénéficient de niveaux de protection élevés pour leurs données traitées et stockées dans le cloud. AWS Cloud a été certifié par rapport à de nombreux secteurs industriels réglementés (santé, finances, etc.), nationaux (par exemple, FedRAMP [États-Unis], C5 [Allemagne], IRAP [Australie]) et des accréditations mondiales (par exemple, ISO 27001,[22] ISO 27018,[23] la norme PCI [Payment Card Industry] relative à la sécurité des données [DSS][24] et les contrôles des organisations de services [SOC][25]), qui testent et valident la sécurité de nos systèmes par rapport aux normes les plus rigoureuses.

Le libre flux des données non personnelles proposé comme solution de facto pour l'UE et les régions transpacifiques

La Commission de l'Union européenne a récemment publié un projet de régulation du libre flux des données ***interdisant les règles de localisation des données nationales dans les États membres de l'UE*** et reconnaissant le principe de libre circulation des données non personnelles au sein de l'UE. Cette proposition établit la circulation transfrontalière de données comme la norme de fait, laissant la responsabilité aux États membres de justifier leur choix d'imposer des exigences de localisation des données en termes de sécurité publique. Bien qu'elle n'en soit qu'à ses premières phases de délibération, cette proposition reconnaît les avantages de la circulation transfrontalière des données en matière d'économie et de sécurité, avantages qui l'emportent sur les considérations relatives à l'application de stratégies de localisation de données. De plus, depuis début 2018, l'**Accord de partenariat transpacifique global et progressiste** conclu par 11 pays soutient également les ***flux de données transfrontaliers*** et n'impose pas aux entreprises d'établir des installations informatiques dans le pays comme condition pour exercer leur activité dans ce pays.

22 ISO 27001/27002 est une norme de sécurité mondialement reconnue qui établit des exigences et des bonnes pratiques pour une approche systématique de la gestion des informations de l'entreprise et de ses clients, basée sur des évaluations du risque périodiques appropriées à des scénarios de menaces en constante évolution.

23 ISO 27018 est un code de bonnes pratiques spécifique à la protection des données personnelles dans le cloud. Elle est basée sur la norme ISO 27002 portant sur la sécurité de l'information, et guide la mise en place des contrôles de la norme ISO 27002 liés aux informations personnelles identifiables (PII) dans le cloud public. Elle fournit également des contrôles et directives supplémentaires, visant à aborder les problèmes de protection des PII dans le cloud public ignorés par les mesures de la norme ISO 27002.

24 La norme de sécurité des données dans le secteur des cartes de paiement (également appelée PCI DSS) est une norme sur la sécurité des informations propriétaires administrée par le Conseil des normes de sécurité PCI (Payment Card Industry Security Standards Council) (https://www.pcisecuritystandards.org/), fondée par American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa Inc. La norme PCI DSS s'applique à toutes les entités qui stockent, traitent ou transmettent des données de cartes de paiement (CHD) et/ou des données d'authentification sensibles (SAD) dont les commerçants, les responsables de données, les acquéreurs, les émetteurs et les fournisseurs de services.

25 Les rapports SOC 1, 2 et 3 (Service Organization Controls) ont pour but de répondre à une grande variété de critères d'audits financiers exigés par les organismes d'audit américains et internationaux. L'audit réalisé pour ce rapport est effectué conformément à l'International Standards for Assurance Engagements n° 3402 (ISAE 3402) et l'AICPA (American Institute of Certified Public Accountants) : AT 801 (anciennement SSAE 16).

Alignement de la stratégie de sécurité, de la transformation numérique et de la croissance économique

Les stratégies doivent évoluer pour tenir compte des nouvelles réalités de la technologie et du monde qu'elle aide à créer. Sinon, les gouvernements continueront à être à la traîne par rapport à la mise à niveau de leurs opérations, au service de leurs citoyens et à l'adoption des solutions les plus modernes et les plus sécurisées. Cette section décrit comment AWS aborde les objectifs de sécurité sous-jacents aux exigences de localisation des données pour diminuer l'inquiétude des stratèges. Elle explore aussi les défis de la modernisation économique et informatique associés à la localisation des données, et propose une réflexion en faveur de l'adoption d'un cloud du secteur public sécurisé.

Défis du secteur commercial et du secteur public en matière de localisation des données

Les gouvernements doivent considérer comment leurs politiques nationales œuvrent pour favoriser ou accélérer la croissance économique et les opportunités de développement de la main-d'œuvre permises par les services de cloud à grande échelle. L'implémentation d'exigences de localisation des données peut se traduire par des impacts négatifs, tels que :

- **Effet contraire sur les efforts d'expansion commerciale multinationale des entreprises locales** - Tandis que les entreprises croissent et se développent en dehors des opérations régionales, il est vital qu'elles aient accès aux ressources qui ont une amplitude mondiale. La restriction de l'accès aux services des opérateurs cloud à grande échelle limite le niveau de l'expérience utilisateur qu'une entreprise peut fournir à sa base de clientèle mondiale.
- **Options de géo-redondance limitées par rapport aux régions CSP mondiales** - Pour les gouvernements et les entreprises, garantir la redondance dans l'hypothèse d'une défaillance opérationnelle due à un sinistre ou à d'autres circonstances est vital pour la stabilité. Le fait d'avoir des opérations en cluster dans un seul pays expose l'organisation à un niveau de risque qui peut être bien plus important que les préoccupations d'accès aux données.
- **Structures de coût onéreuses nécessaires pour répondre à des exigences rigoureuses** - Les environnements « cloud » conçus autour d'un seul propriétaire ou d'une communauté requièrent un niveau de tarification élevé pour garantir la durabilité opérationnelle qui peut réellement nuire à l'acquisition de capacités additionnelles nécessaires à l'obtention d'une défense en profondeur.

La technologie du cloud est l'activateur des évolutions commerciales et du secteur public, et jusqu'à quel point les gouvernements encouragent le principe de flux de données transfrontaliers ou s'y opposent impactent la force de leurs économies locales aussi bien que leur compétitivité sur le marché mondial.

Impact commercial

Permettre un libre flux des données entre les frontières a un impact positif net important sur l'économie mondiale. De récentes études conduites par différents organismes soulignent cet impact et insistent sur le coût que représente l'établissement de barrières contre les flux de données. Un rapport de février 2016 rédigé par le McKinsey Global Institute a estimé que les flux de données transfrontaliers ont pratiquement contribué à 2,8 milliards de dollars au sein de l'économie mondiale en 2014[26] grâce à l'autorisation des flux de biens, de services et d'autres ressources. Le rapport estime que ce

26 http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

chiffre pourrait atteindre $ 11 milliards en 2025. Les gouvernements qui exigent une localisation des données et limite les flux économiques transfrontaliers en paient un prix élevé. L'ECIPE (European Centre for International Political Economy), think tank indépendant, a publié une étude sur l'impact économique des exigences de localisation des données qui font de la discrimination contre les fournisseurs étrangers dans sept juridictions : Brésil, Chine, UE, Inde, Indonésie, Corée du Sud et Vietnam.[27] Leurs recherches ont conclu que les restrictions unilatérales sur les flux de données transfrontaliers et sur l'accès aux marchés étrangers impactent négativement la croissance et la reprise économiques, car elles limitent l'accès à une tarification compétitive, à la croissance de l'emploi dans de nombreux services et secteurs marchands, et aux opportunités d'investissement. L'étude a signalé que les exigences de localisation des données impactent non seulement le flux de données, mais également un ensemble plus large d'opportunités d'extension commerciale qui reposent sur les flux de données transfrontaliers.

Après avoir étudié six pays en développement et les 28 États membres de l'UE, une étude similaire de la Banque mondiale a révélé que les exigences de localisation des données peuvent réduire le PIB jusqu'à 1,7 %, les investissements jusqu'à 4,2 % et les exportations jusqu'à 1,7 %.[28] Cet impact est surtout ressenti par les petites entreprises et les start-ups. Grâce à l'utilisation du cloud, par exemple, les personnes et les petites et moyennes entreprises (PME) peuvent accéder à des ressources informatiques à un coût et à une échelle auparavant uniquement accessibles aux entités dotées d'une capitalisation beaucoup plus importante. Les PME sont les principaux moteurs de la création d'emplois. Le cloud computing réduit les obstacles à la création d'entreprise et facilite l'accès au marché. De cette façon, il favorise la création de nouvelles start-up et, en fin de compte, de plus d'emplois. Cependant, selon la Commission européenne, les entreprises technologiques à l'image des opérateurs cloud doivent supporter des coûts importants pour s'adapter aux diverses législations nationales. Ainsi, les coûts de la vente en ligne l'emportent sur les bénéfices. Plus récemment, en mai 2017, l'institut de recherche non partisan Information Technology and Innovation Foundation parvenait aux mêmes conclusions.[29]

27 Centre européen d'économie politique internationale (ECIPE) : « The Costs of Data Localization: A Friendly Fire on Economic Recovery », http://www2.itif.org/2015-cross-border-data-flows.pdf?_ga=1.8208626.1580578791.1473954628.

28 http://documents.worldbank.org/curated/en/961621467994698644/pdf/102724-WDR-WDR2016Overview-ENGLISH-WebResBox-394840B-OUO-9.pdf

29 Nigel Cory, « Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? » Information Technology and Innovation Foundation (Mai 2017) http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.243762501.1722557619.1508762047-1611916082.1508762047.

Le résultat principal de ces études indique qu'une interdiction des flux de données transfrontaliers sous forme d'exigences en matière de localisation des données peut impacter la croissance économique au niveau local et régional ainsi que la compétitivité sur le marché international, les PME étant les plus lourdement touchées. Un système sécurisé au sein de l'UE n'est ni plus ni moins sécurisé qu'un système à l'architecture similaire situé en Amérique du Sud. Les gouvernements peinent à comprendre que la protection des données ne dépend généralement pas de l'endroit où sont stockées les information, mais plutôt des mesures mises en place pour sécuriser les données. L'emplacement physique n'a généralement aucune incidence, car les centres de données sont quasiment toujours connectés à des réseaux largement accessibles. Ainsi, la sécurité réelle dépend des pratiques et des processus techniques, opérationnels et managériaux mis en place par les opérateurs cloud et le client.[30]

Coûts des centres de données fonctionnant exclusivement dans le pays

Une étude de 2015 réalisée par une entreprise spécialisée dans la sécurité des informations a évalué dans quelle mesure un modèle de centre de données dans le pays était bien plus onéreux que l'exploitation de CSP au niveau mondial. L'étude a démontré que le coût des services de cloud pouvait augmenter considérablement en raison de la localisation des données, selon la disponibilité des autres services. L'étude a révélé que :

- Si le Brésil avait adopté la localisation des données dans sa « charte pour les droits des internautes » de 2014, les entreprises auraient dû payer en moyenne 54 % de plus que le prix international le plus bas pour utiliser les services de cloud (quelle que soit la catégorie) des fournisseurs de cloud locaux.
- Si l'Union européenne avait adopté la localisation des données, les entreprises paieraient encore jusqu'à 36 % de plus pour utiliser des services semblables fournis pas des opérateurs cloud à grande échelle. À l'époque où a été réalisée l'étude, certains des centres de données à bas prix se trouvaient dans l'Union européenne.[29]

Impact sur le secteur public

Les pays qui dressent des barrières à l'encontre des flux de données peuvent empêcher leurs citoyens de profiter de services novateurs, capables d'améliorer leur qualité de vie, ainsi que de prestations de services gouvernementaux. Par exemple, les applications d'intelligence artificielle et d'apprentissage automatique exigent une infrastructure personnalisée pour fonctionner de manière optimale,[32] et tandis que les opérateurs cloud mondiaux agrandissent leurs centres de données, il est utopique de supposer que ces derniers s'implanteront dans chaque pays. Par conséquent, alors que l'intelligence artificielle et l'apprentissage automatique sont de plus en plus utilisés pour améliorer des services, tels que les pronostics de santé et les prévisions météorologiques pour la préparation aux situations d'urgence, les habitants des pays disposant d'exigences strictes en matière de localisation des données ne pourront pas accéder immédiatement aux avancées technologiques ou aux services axés sur les citoyens.

30 Ibid p. 4 Cet article en arrive indépendamment aux mêmes conclusions.

31 http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.51021357.566718019.1510350061-1611916082.1508762047

32 Par exemple, les systèmes dotés de capacités GPU générales et les circuits logiques programmables (FPGA).

À noter également la présence de coûts socio-économiques en cascade pour limiter les flux de données, notamment sur la compétitivité commerciales et le développement de la main-d'œuvre. L'omniprésence de la technologie cloud et son rapport étroit avec les progrès économiques permettent d'imposer le commerce numérique (et de réduire les obstacles qu'il rencontre) comme prioritaire aux yeux des gouvernements. Les pays autorisant les flux de données pourront accéder à une technologie de pointe qui à son tour modernisera les services commerciaux et publics, améliorera la productivité des travailleurs et augmentera le nombre d'emplois locaux et les compétences entre les secteurs. Les pays limitant les flux de données et le commerce numérique souffriront avec le temps d'un handicap concurrentiel. Par exemple, les nombreux avantages associés à l'IoT pour faciliter la fabrication, les villes ou l'élevage « intelligents » ne peuvent pas se concrétiser avec des stratégies restrictives qui limitent l'analyse du Big Data, l'apprentissage automatique ou d'autres fonctionnalités traitées par des mouvements de données gratuits mais sécurisés.

Il existe une forte demande continue concernant les compétences de cloud computing dans des secteurs clés tels que la sécurité des applications, le développement d'applications professionnelles dans le cloud, la migration d'entreprise dans le cloud et le Big Data. Le Bureau des statistiques du travail des États-Unis prévoit une augmentation de la demande pour les emplois liés à la sécurité des informations de l'ordre de 37 % pour la période 2012-2022. Afin de pourvoir ces nouveaux postes, les gouvernements devront investir et proposer des apprentissages et formations pour permettre aux individus d'acquérir des compétences technologiques.

Les limites empêchant d'accéder aux services informatiques perfectionnés fournis par les opérateurs cloud à grande échelle créeront un décalage persistant entre le développement et la préservation d'une main-d'œuvre hautement qualifiée et dotée d'une solide expertise technique. Cela s'explique par la corrélation entre les compétences de la main-d'œuvre et la sophistication technologique d'une organisation qui, à son tour, repose sur sa capacité à accéder à une technologie dernier cri. L'utilisation effective de la technologie moderne exige une main-d'œuvre dotée de compétences à sa mesure. L'écart connu entre les compétences s'élargit compte tenu de l'ampleur et du rythme de l'innovation grâce aux services cloud. Les gouvernements, notamment, se sont laissés distancer dans la course aux experts dont le rôle est essentiel pour moderniser les applications, tout en protégeant simultanément les informations et les systèmes du service public contre des adversaires hautement qualifiés et des failles toujours plus complexes dont la fréquence et les conséquences ne cessent de se multiplier.

Remarques relatives à la définition de stratégies de localisation des données

Comme indiqué plus haut, la souveraineté en matière de réglementation d'un État-nation sur les données peut encore être atteinte, tout en profitant du coût et des avantages sécuritaires des opérateurs cloud à grande échelle tels qu'AWS. Les mesures de sécurité déployées dans les services AWS et vérifiées grâce à nos audits tiers permettent d'assurer un degré élevé de sécurité pour prévenir et gérer les risques d'accès illégal aux données.

Nous encourageons les gouvernements à prendre en compte les stratégies suivantes pour respecter les objectifs de sécurité associés à la localisation des données.

1. Développer des stratégies et des exigences qui autorisent l'utilisation d'installations de traitement des données hors du pays si ces dernières sont traitées et stockées dans un environnement de cloud moderne, hautement sécurisé et à grande échelle. Les clients peuvent également choisir des emplacements disposant de lois relatives à la protection des données conformes à leurs propres législations et où des accords sur le transfert de données sont déjà en vigueur.

2. Aligner les stratégies nationales et les exigences réglementaires sur le principe de la libre circulation transfrontalière des données pour équilibrer efficacement les objectifs en termes de sécurité, d'économie et de modernisation informatique.

3. Évaluer les modèles de transfert des données, tels que le Bouclier de protection des données UE-USA, et les clauses contractuelles normalisées, telles que les Clauses types de l'UE, qui ont été approuvées par les autorités de protection de l'Union européenne et peuvent être utilisées dans les contrats entre les fournisseurs de services et leurs clients pour garantir que les données personnelles qui quittent l'Espace économique européen seront transférées conformément au Règlement général sur la protection des données (RGPD).[33] Ces types de contrats de transfert de données offrent l'assurance que les opérateurs cloud protègent les données de manière responsable, et fournissent des moyens préapprouvés pour protéger et soutenir le flux de données internationales de façon conforme et sécurisée..

4. S'assurer que les opérateurs cloud et les sous-traitants tiers démontrent des contrôles de sécurité efficaces pour traiter l'accès non autorisé de tiers aux données, aux systèmes et aux ressources via des accréditations tierces reconnues dans le monde entier (par exemple, ISO 27001, ISO 27018, SOC, PCI DSS, etc.).

Le RGPD de l'Union européenne, applicable depuis mai 2018, a pour but d'harmoniser les lois de protection des données à travers l'Union européenne (UE) en appliquant une même loi de protection des données qui lie chaque État membre. Le RGPD ne nécessite pas de lois sur la localisation des données au sein de l'Union européenne, mais soutient plutôt les infrastructures légales sous la forme de modèles de transfert des données et de clauses contractuelles normalisées (par exemple, les clauses du modèle de l'Union européenne) afin d'encourager les flux de données transrégionaux.

L'article 45 du RGPD établit le principe que les transferts de données vers un pays tiers ou une organisation internationale peuvent avoir lieu si le pays tiers, le territoire ou l'un des secteurs spécifiés au sein de ce pays, ou l'organisation internationale concernée, garantit un niveau adéquat de protection. Pour ce faire, les gouvernements peuvent :

- Modifier leur loi existante sur la protection des données et prendre part à des discussions conséquentes avec les autres pays. Par exemple, la Nouvelle-Zélande est en train d'obtenir une décision satisfaisante de la part de la Commission de l'Union européenne.
- Établir des infrastructures bilatérales telle que le bouclier de protection des données Union européenne - États-Unis.

5. Classer les données et définir les responsabilités et les rôles de gestion des données pour déterminer les obligations de protection des données appropriées pour chaque partie. Les gouvernements doivent penser à tirer profit de la norme ISO 2701 pour définir les rôles de contrôleur et de processeur de données. Les gouvernements peuvent travailler avec les opérateurs cloud pour la compréhension et l'application correctes des responsabilités de protection des données du contrôleur par rapport au processeur pour chaque modèle de services de cloud.

33 L'addenda sur le traitement des données du RGPD AWS, qui inclut les clauses du modèle de l'Union européenne, fait désormais partie de nos Conditions de service en ligne. Cela signifie que tous les clients AWS à travers le monde peuvent s'appuyer sur l'addendum chaque fois qu'ils utilisent les services AWS pour traiter les données personnelles conformément au RGPD. Pour plus d'informations sur l'approche d'AWS en matière de conformité au RGPD, consultez : https://aws.amazon.com/compliance/gdpr-center/.

6. S'assurer de la compréhension du client et de l'implémentation des services de sécurité pour chiffrer les données. AWS a lancé des services de chiffrement qui fournissent aux clients la possibilité de contrôler intégralement les clés de chiffrement. AWS offre aux clients la possibilité de chiffrer les données à l'aide de leurs propres clés qui peuvent être stockées en dehors d'AWS ou de manière sécurisée au sein des offres. Les clients peuvent ainsi contrôler leurs clés et leur accès aux données, tout en respectant les obligations strictes de sécurité et de conformité.
7. Prendre part à des efforts bilatéraux et multilatéraux pour mettre à jour le processus MLAT de telle sorte qu'il équilibre les besoins gouvernementaux et obtienne rapidement les preuves nécessaires dans les enquêtes et les poursuites avec le droit des individus à la confidentialité sur le contenu électronique en leur possession. Nous soutenons, aussi bien au niveau national qu'au niveau international, les législations qui mettent à jour les aspects relatifs à la confidentialité des communications électroniques et à leur accessibilité aux forces de l'ordre. Nous encourageons également les gouvernements à vérifier et à mettre à jour leurs lois nationales afin de faire face aux rôles, aux responsabilités et aux dispositifs régissant l'accès légal aux données conformément aux principes du processus MLAT.

Conclusion

Même si les gouvernements peuvent éprouver un sentiment plus important de sécurité lorsqu'ils imposent que les données traitées et stockées résident sur des sites informatiques locaux (offrant une proximité et un contrôle physique), une évaluation plus approfondie montre que la restriction des services informatiques à la juridiction locale seule ne garantit pas une meilleure sécurité globale des données. Du point de vue du rapport risque/bénéfice, les opérateurs cloud à grand échelle, comme AWS, peuvent mieux aider à gérer la cybersécurité tout en continuant à réduire le risque d'accès aux données de la part de gouvernements étrangers. Les gouvernements doivent aussi prendre en compte les compromis significatifs associés aux exigences en matière de localisation des données. Non seulement les gouvernements qui s'appuient sur les exigences restrictives de localisation des données perdront l'accès à quelques-uns des environnements informatiques les plus sécurisés sur terre, mais, au-delà de la sécurité, seront contraints d'affronter un décalage perpétuel en termes d'accès à une technologie économique et de pointe, indispensable à leur propre transformation numérique. Nous invitons les gouvernements à réévaluer les objectifs de sécurité qu'ils atteignent actuellement via les restrictions de localisation des données par rapport à l'économie, à la modernisation informatique et aux coûts d'opportunité de la sécurité. Les capacités de sécurité des opérateurs cloud à grande échelle non seulement prennent en compte les préoccupations prioritaires, mais fournissent une sécurité à un niveau supérieur à celui des installations traditionnelles sur site ou contractées localement. Les solutions de stratégies, telles que les accords de transfert des données et la mise à profit des accréditations de sécurité internationales reconnues, peuvent constituer un moyen suffisant pour répondre aux objectifs de localisation des données tout en encourageant les objectifs de transformation numérique du secteur public.