EBOOK

SYSTRAN

Traduction et souveraineté des données

Un enjeu majeur pour les entreprises européennes

Avant d'utiliser un Cloud, il faut se poser certaines questions.
Un Cloud reçoit en effet, par son utilisation et en fonction du contenu à traduire, des données stratégiques pour votre entreprise – voire extrêmement sensibles.

Où sont hébergées vos données ? Quelle loi s'applique sur le Cloud en question ? Qui peut y accéder ?

Ces questions sont essentielles. Certaines lois américaines, par exemple, s'appliquent au-delà des frontières des États-Unis, donnant la possibilité au gouvernement américain d'accéder aux données que vous traduisez.

Lesdites lois s'appliquent même aux données hébergées sur des serveurs français ou européens, tant que la société qui fournit le Cloud de la solution de traduction est américaine.

Ce sujet est complexe, et les risques peuvent être bien réels.

Sommaire

Quels risques pour vos traductions faites en France ?

USA PATRIOT Act & CLOUD Act : deux lois qui prévalent sur le RGPD

Ces deux lois américaines s'appliquent dès que la nationalité de l'entreprise qui a le contrôle des données est américaine – par exemple, Google, Meta, Microsoft, Apple, etc.

On parle d'**extraterritorialité du droit américain** : le département de la justice américaine peut entreprendre des actions et des poursuites judiciaires en dehors du territoire des États-Unis.

Ainsi, si votre solution de traduction utilise un Cloud géré par un organisme américain (Microsoft Translator ou Google Translate par exemple), vous pouvez être concerné et la sécurité de vos données peut ne pas être à 100 % garantie.

L'extraterritorialité : définition

L'extraterritorialité est le droit des pays à appliquer leurs lois en dehors de leurs frontières.

Il existe de nombreux exemples dans la finance ou le commerce, les deux plus connus étant l'extraterritorialité du droit américain et celle du droit européen. Ce principe est **encadré par le droit international**.

Selon Vie publique, « l'**extraterritorialité** se justifie par le lien qui existe entre un pays et ses ressortissants où qu'ils se trouvent. Ainsi, si un ressortissant français n'a pas respecté la loi dans son pays d'origine, la France peut le poursuivre et appliquer ses propres lois même si celui-ci est installé dans un autre pays. »

USA PATRIOT Act

En savoir plus

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

Voté et signé en 2001 à la suite du 11 Septembre, l'**USA PATRIOT Act** a pour objectif d'aider les autorités fédérales américaines à lutter contre le terrorisme.

Toutes les agences fédérales américaines (FBI, CIA, NSA, NCIS, l'armée, le fisc (IRS), etc.) peuvent accéder à des informations « dans le cadre d'une enquête relative à des actes de terrorisme, au moyen d'injonctions destinées à rester secrètes compte tenu de la sensibilité du sujet ».

Cela signifie que les propriétaires des données n'ont pas forcément à être notifiés si elles sont récupérées et inspectées au titre de l'USA PATRIOT Act.

CLOUD Act

Clarifying Lawful Overseas Use of Data Act

En savoir plus

Adopté en 2018, le **CLOUD Act** étend la portée géographique des demandes du gouvernement américain à pouvoir accéder aux données sur les serveurs. Celle-ci est invoquée autant lors d'enquêtes criminelles que lors de demandes d'accès à des données qui pourraient « menacer l'ordre public ».

Le CLOUD Act simplifie l'accès aux données entre pays : auparavant les procédures pour accéder à des données étaient longues et complexes, incluant des commissions rogatoires internationales.

Le CLOUD Act permet aux autorités compétentes d'un pays, sous réserve d'accord entre les deux gouvernements, **de formuler des demandes pour accéder au traitement et au stockage électronique de données qui les intéressent auprès de fournisseurs de services de communication.**

Quel impact sur les entreprises européennes ?

Selon le principe d'**extraterritorialité**, les lois américaines prévalent sur les lois européennes (y compris le RGPD) et peuvent donc potentiellement permettre l'accès à vos données.

Les lois américaines s'appliquent en outre sur un spectre très large : tous les secteurs d'activités, et tous les types de data sont concernés.

Beaucoup de données stratégiques et sensibles sont traduites en ligne, or beaucoup d'acteurs de traduction automatique en ligne sont assujettis au CLOUD Act et à l'USA PATRIOT Act.

Les données traduites par ces plateformes peuvent donc être récupérées et exploitées à des fins économiques.

Focus sur des cas avérés d'espionnage industriel

L'importance de la souveraineté des données a été mise en exergue suite à de nombreux cas avérés d'espionnage industriel.

Il a été démontré que les services américains étaient intervenus dans ces affaires via l'utilisation du CLOUD Act ou du PATRIOT Act :

- **General Electric** pour le rachat d'Alstom en 2014 ;
- **Boeing** pour la vente de 747 à l'Arabie saoudite ;
- **Raytheon** sur le dossier SIVAM 2 au Brésil ;
- **Hughes** pour l'exportation d'un système de télécommunication en Indonésie.

Pour éviter de tomber sous le coup de l'extraterritorialité, la meilleure approche est donc d'opter pour des services en ligne garantissant la **souveraineté de vos données**.

Souveraineté numérique ou souveraineté des données ?

La souveraineté numérique, à l'échelle d'un État

La souveraineté numérique désigne la capacité d'un État à « maîtriser l'ensemble des technologies, tant d'un point de vue économique que social et politique[1] ».

En d'autres mots, il s'agit de ne pas dépendre des outils technologiques d'autres pays, ainsi que de ne pas être influencé par un tiers.
La question est centrale depuis plusieurs années, avec la **prédominance des GAFAM** dans le monde numérique et la dépendance forte à des pays étrangers pour l'approvisionnement en composants et matières premières – notamment les « terres rares ».

69 %

En janvier 2021, 69 % des Français se sentaient contraints d'utiliser les services des géants du web américain (les GAFAM), en raison du manque d'alternatives venant d'autres pays, notamment d'Europe.

Source : Ifop | Les Français et la souveraineté numérique

Depuis la pandémie de Covid-19, la guerre russo-ukrainienne et la pénurie de puces électroniques, la question de la souveraineté est devenue beaucoup plus concrète. Le problème est réel : aujourd'hui, **personne en Europe** n'a la capacité d'être souverain en manière numérique.
Il faudrait par exemple que toutes les puces soient fabriquées en Europe.

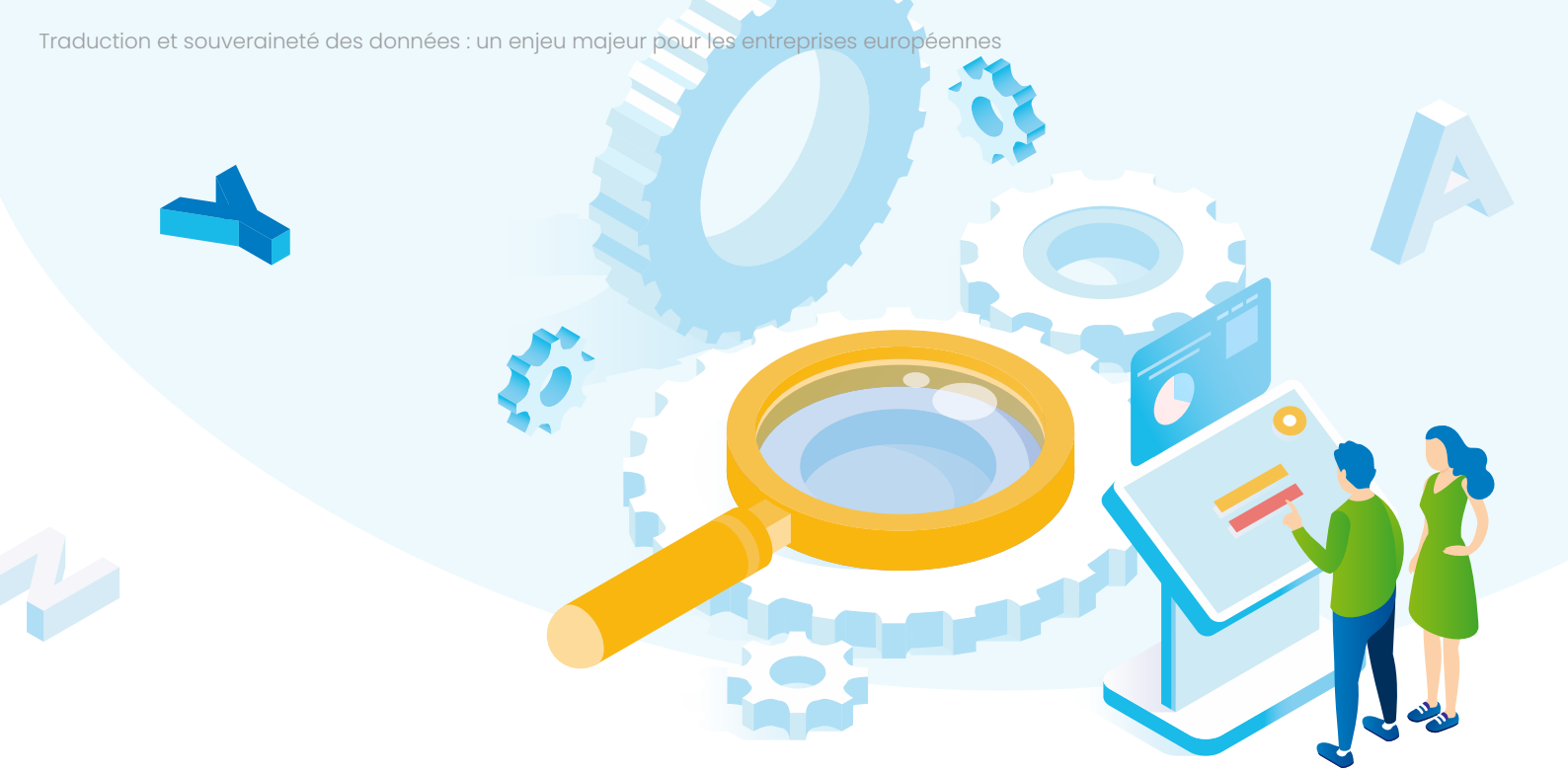
La souveraineté numérique est donc actuellement une chimère. L'enjeu le plus atteignable aujourd'hui pour les entreprises et les organisations est la **souveraineté des données**.

L'alternative atteignable : la souveraineté des données

Les données numériques sont soumises à la législation du pays où elles sont stockées.
La souveraineté des données, à l'échelle d'une organisation, désigne donc la capacité à protéger ses données d'éventuelles interférences, notamment en provenance de l'étranger. Cela implique qu'une entreprise doit agir de manière indépendante, en particulier dans des domaines stratégiques nécessaires à son développement.

Chaque organisation ne doit pas pour autant construire son propre Cloud ! Elle doit en revanche porter une attention particulière à la **localisation de ses données**, et utiliser des solutions de stockage et de traitement des données régis par des acteurs de son pays de domiciliation.

[1]Source : Bernard BENHAMOU, dans « Souveraineté numérique : un modèle à inventer », cité par Amaelle GUITON, Libération, 20 mai 2016



Panorama des solutions pour protéger ses données traduites

Les Clouds américains peuvent-ils être sécurisés ?

Pour rassurer leurs utilisateurs européens, certaines entreprises américaines développent des Clouds européanisés, c'est-à-dire avec des serveurs localisés en Europe. Or le problème reste le même, car le **CLOUD Act** s'applique dès que le fournisseur de service est américain, **indépendamment de la localisation du serveur**.

Pourtant, certaines organisations américaines font preuve de transparence et publient le nombre de demandes d'accès à des données par le gouvernement américain. Ainsi, elles espèrent démontrer le faible impact de ces lois sur les entreprises.

Cependant, la sécurité ne peut être garantie, car les Clouds restent soumis aux lois américaines.

Le chiffrage de données, une solution de façade

Une autre solution pourrait être le chiffrage de ses données de bout en bout mais, selon Jean-Albert Eude[2], cette solution pose plusieurs problèmes :

1. Les chiffrements peuvent être décodés, surtout quand ce sont des gouvernements qui interviennent.
2. Le chiffrement peut être limité dans des pays selon la législation en vigueur.
3. Cela peut poser des désagréments au niveau de la gestion en interne de l'entreprise, ce qui peut entraîner une perte d'efficacité, puis économique, par le temps de chiffrer et déchiffrer les informations à chaque utilisation.

Le cas est d'autant plus vrai dans le cadre de traduction : les données doivent être déchiffrables dans la solution de traduction. Cela complexifie les processus !

[2]Source : Jean-Albert Eude, Directeur du programme Innovation Business Solution Center - Société Générale

Un référentiel européen de confiance, le SecNumCloud

Créé en 2016 par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le SecNumCloud[3] s'inscrit dans le cadre européen du Cybersecurity Act de 2019.

Le SecNumCloud garantit la **sécurité du Cloud**, notamment le cloisonnement dans l'architecture du service entre ses différents commanditaires.

Une qualification est attribuée après un audit complet effectué par un organisme de certification en conformité cyber agréé par l'ANSSI, et elle a une durée de validité de 3 ans.

Lors de sa mise à jour en 2021, ce schéma a intégré des critères pour **se protéger de l'extraterritorialité des lois américaines** :

- obligation pour le siège du prestataire d'être localisé au sein d'un pays membre de l'UE ;
- limites concernant la nationalité de l'actionnariat et l'influence des entités basées en dehors de l'UE ;
- limites d'accès aux données par les prestataires non européens.

De plus, avec sa mise à jour, le référentiel est devenu **conforme au RGPD** en incluant les exigences relatives à la protection des données.

Une liste des produits et services qualifiés est mise à jour régulièrement sur le site internet de l'ANSSI.

Ce référentiel est une bonne initiative et un complément à prendre en compte lors du choix de son prestataire Cloud.

Dans ce contexte, comment choisir une solution de traduction automatique sécurisée dont l'utilisation ne met pas potentiellement l'entreprise en péril ?

[3]Source : Jean-Albert Eude, Directeur du programme Innovation Business Solution Center - Société Générale

La vraie solution pour la traduction de vos données : le Cloud souverain

Lors de l'utilisation d'une solution de traduction, la seule véritable solution est de choisir un logiciel qui utilise un **Cloud souverain**, c'est-à-dire un Cloud géré par un acteur européen uniquement.

L'hébergeur du Cloud peut posséder des serveurs aux États-Unis, cependant les architectures de leurs infrastructures doivent permettre d'**isoler les régions Cloud** : le serveur situé en France ne communique pas de données avec le serveur américain. On parle alors d'interopérabilité des systèmes : deux systèmes peuvent opérer ensemble tout en respectant les données.

Le mot de notre expert

Aujourd'hui, le choix de fournisseurs européens souverains pour l'hébergement de vos données est primordial.
Mais il ne vous exempte surtout pas d'avoir le réflexe d'étudier en détail leurs ***conditions contractuelles*** *concernant l'impact possible du CLOUD Act.*

EMMANUEL TONNELIER
Depuis une quinzaine d'années, il travaille sur la **souveraineté** des données et la **criticité** des outils les manipulant – dont les outils de traduction automatique.

Exemple d'un Cloud souverain : OVHcloud

Acteur européen reconnu pour la sécurité de ses serveurs, **OVHcloud**[4] est une entreprise d'origine française qui opère depuis plus de 20 ans.

La sécurité des données stockées chez OVHcloud est garantie :

- l'entreprise est transparente sur la **localisation du datacenter** où les informations sont hébergées, ainsi que sur le statut juridique applicable à ces dernières ;
- l'entreprise assure la protection des données ; OVHcloud est signataire du **code de conduite CISPE**, approuvé par la Commission européenne, qui facilite la mise en conformité du Cloud au RGPD.

OVHcloud

Le choix de SYSTRAN

C'est pour ces raisons que SYSTRAN a choisi le Cloud souverain d'OVHcloud pour sa solution de traduction en ligne.

[4]Source : OVHcloud / Du Cloud souverain au Cloud de confiance

SYSTRAN

Les informations que vous traduisez sont dépendantes des lois de protection des données appliquées aux Clouds sur lesquels elles sont stockées. En fonction de la juridiction appliquée, elles peuvent donc être consultées et réquisitionnées par des gouvernements étrangers – **à commencer par celui des États-Unis** – mais aussi être la proie d'espionnage industriel.

C'est d'autant plus délicat avec la pratique du « Shadow IT », lorsque les collaborateurs d'une organisation utilisent des logiciels non validés par leur DSI.

Face à la menace parfois douteuse, mais toujours légale, de l'extraterritorialité de certaines lois étrangères, le **Cloud souverain** s'impose comme la solution la plus sécurisée pour vos données et vos traductions.

Découvrir le partenariat SYSTRAN et OVHcloud