Impacts du Cloud Act sur les données de votre SI

Cloud Act, une loi controversée nécessitant l'application d'un principe de précaution

Bruno Le Maire a annoncé, mercredi 16 janvier, que les autorités françaises cherchaient un moyen de résister au « CLOUD Act ».

Voté en mars 2018, le « *Clarifying Lawful Overseas Use of Data Act* » ou CLOUD Act est une loi votée par le congrès américain précisant les règles d'accès aux données personnelles détenues par des entreprises américaines en dehors du territoire des Etats-Unis d'Amérique.

Ce texte, au cœur d'une controverse, quant à son mode d'adoption et à son impact sur le droit à la vie privée, propose une alternative au processus d'accès aux données actuellement en place (par le biais des MLAT, soit des commissions rogatoires internationales) pour raccourcir les délais d'investigation dans des enquêtes criminelles.

Le CLOUD Act s'applique à toutes les sociétés américaines, et aux sociétés qu'elles contrôlent. Ces sociétés doivent alors communiquer aux autorités américaines, sous certaines conditions, les données de communication placées sous leur contrôle sans considération du lieu où elles se trouvent stockées. Selon ce principe, les fournisseurs de service web tels que Microsoft, Google, IBM, AWS, Salesforce, Oracle, … sont concernés.

Le CLOUD Act prévoit également la possibilité pour les Etats-Unis de signer des accords internationaux – ou *executives agreements* – avec des gouvernements étrangers afin de permettre à chaque pays de demander directement aux *data providers* relevant de la juridiction du pays partenaire, la transmission de données électroniques sans passer par les MLAT.

La transmission des données dont il est question est encadrée :

- Les données demandées doivent s'inscrire dans le cadre d'une enquête judiciaire, avec une présomption sérieuse (la personne a commis ou est sur le point de commettre une grave infraction pénale) ; ces données doivent revêtir un caractère d'utilité à l'enquête ; cette demande est obligatoirement formalisée par un mandat délivré par une juridiction et non sur la seule demande émanant d'une autorité administrative.

- Lorsque les autorités américaines formulent ce type de requêtes, elles ne peuvent concerner qu'un ressortissant américain, un résident permanent sur le territoire ou une société immatriculée aux Etats-Unis.

En l'état actuel, plusieurs recours existent pour bloquer la transmission des données :

- Une société recevant une requête de transmission de données peut toujours, même dans le cas d'un *executive agreement*, s'opposer à transmettre les éléments demandés auprès d'une juridiction si, entre autres, elle estime qu'elle s'expose à un risque de sanction sérieux de la part du pays dans lequel sont hébergées les données ou si elle a un doute concernant la nature fondée de la relation entre son client ou usager et les Etats-Unis.

- La loi française dite « de blocage », et la règlementation européenne visant à protéger le secret des affaires sanctionnent la transmission de données sensibles pouvant porter préjudice aux entreprises ou à la nation en général.

- La RGPD en vigueur dans l'Union Européenne règlemente elle-même la transmission des données à caractère personnel pouvant être transférées vers des pays tiers ou à des organisations internationales. Cette règlementation bloque pour l'instant toute demande de transmission de données de la part des Etats-Unis s'ils ne passent pas par les MLAT.

Le risque demeure que les sociétés, malgré des doutes sur le bien-fondé d'une requête, transmettent tout de même les informations demandées aux autorités américaines en raison du risque d'image que cela leur fait encourir (ex : dans le cas d'une enquête sur du terrorisme).

Prenant en considération le CLOUD Act, l'Union Européenne doit étudier la possibilité de signer un *executive agreement* avec les Etats-Unis. Il nous semble alors nécessaire d'anticiper cette signature entre les Etats-Unis et l'Union Européenne, ou la France.

Comment s'assurer de prendre les bonnes décisions ?

Les entreprises peuvent appliquer un principe de précaution en ayant recours à des hébergeurs de données européens dont les datas centers sont implantés sur le sol européen. De cette façon, les conditions de traitement des données seront soumises à la règlementation Européenne.

Notre propos cible particulièrement les systèmes d'informations de gestion des ressources humaines ; cependant, tous les SI, toutes les data, sont concernés.

Dans les phases de choix, il nous semble particulièrement prudent de questionner l'éditeur sur ce point et d'interroger d'autres clients sur les choix effectués, leurs arguments. Nos récentes missions d'aide au choix ont apporté des éclairages intéressants aux dirigeants concernés sur les positions des différents éditeurs.

Le risque encouru doit être mesuré et discuté avec les éditeurs, hébergeurs afin de prendre les décisions en toute connaissance de cause.

Enfin, un certain nombre de choix techniques peuvent être décidés afin de limiter les accès aux données ; cryptage, séparation et règles de sécurité constituent alors un projet à part entière, selon la nature des données. Il sera alors important de considérer l'intégralité de la chaine, jusqu'à son maillon le plus faible … souvent nos PC et nos clés USB !

Catherine Bes-Francony
Directeur en charge des offres RH

Kathleen Lavander
Consultante RH