Faut-il avoir peur du CLOUD Act ?

Précisons tout d'abord que le terme CLOUD Act est en fait l'acronyme de *Clarifying Lawful Overseas Use of Data Act* que l'on pourrait traduire par « Loi pour clarifier l'utilisation légale des données à l'étranger ». En pratique, il s'agit d'un (minuscule) texte de 32 pages glissé incognito dans les quelques 2 232 pages de la loi sur les dépenses 2018 des États-Unis. Ce texte, qui n'a fait l'objet d'aucun débat au Congrès, n'a été médiatisé qu'après sa promulgation par Donald Trump le 23 mars 2018 mettant ainsi l'Europe et le reste du monde devant le fait accompli.

Le CLOUD Act permet de lutter efficacement contre la criminalité au niveau mondial et s'applique dans le cadre d'une procédure pénale suite à un crime ou un délit. Comme toute requête ne doit cibler qu'une personne ou qu'un seul élément identifiant en particulier, le CLOUD Act ne peut (à priori) servir à la réalisation d'opération de surveillance massive comme celles de la NSA révélées par Edward Snowden.

Cette Loi vient combler le vide juridique du Stored Communication Act (SCA) mis en lumière par l'affaire qui opposait depuis 2013 Microsoft à la justice US pour l'accès aux mails d'un présumé trafiquant de drogue stockées en Irlande.

Le CLOUD Act prévoit que les gouvernements étrangers puissent s'engager avec le gouvernement américain par le biais d'accords bilatéraux (executive agreement) afin de « fluidifier » l'accès aux données. Grâce à ce mécanisme et sous réserve que la cible ne soit pas un citoyen américain, l'entraide judiciaire se substitue aux accords d'assistance mutuelle classiques MLAT (*Mutual Legal Assistance Treaty*) dont la lourdeur impose un délai de plusieurs mois pour pouvoir accéder à des données à l'étranger.

La Loi prévoit également qu'un fournisseur US puisse s'opposer dans un délai de 14 jours à une telle demande s'il pense que la personne visée n'est pas un ressortissant américain et que la divulgation l'obligerait à enfreindre la réglementation du pays hébergeant les données. Sa demande sera alors portée devant un tribunal américain qui devra statuer selon les arguments avancés par les deux parties (Police US / Fournisseur US).

Trois questions se posent alors :

- Le CLOUD Act sera-t-il toujours utilisé exclusivement pour lutter contre la criminalité et en aucun cas pour de la surveillance à des fin politiques, stratégiques ou économiques ?
- L'article 48 du RGPD, parfois appelé bouclier Anti NSA, sera-t-il suffisamment protecteur pour empêcher les services américains d'accéder librement aux données

des fournisseurs américains situées au sein de l’UE ?
- L’UE doit-elle s’engager dans ce processus en signant un « executive agreement » avec le gouvernement américain ?

Pour la dernière question, il semble évident que l’Union ne doit pas accepter de signer un accord au terme duquel les Etats-Unis, en raison principalement de l’hégémonie des GAFAM, auraient accès aux données des citoyens européens, quel que soit leur lieu de stockage, tandis que les autorités européennes pourraient seulement accéder à des données stockées aux Etats-Unis en excluant toute donnée concernant des citoyens américains.

La seule attitude possible pour l’Union européenne, dans un souci de réciprocité et de juste équilibre entre la nécessité de lutter contre la criminalité et la protection des citoyens européens, serait de négocier avec les Etats-Unis un accord par lequel les autorités de chaque pays auraient accès de manière fluide aux données nécessaires à la lutte contre la criminalité, et à elles seules uniquement, sans considération de leur lieu de stockage et sans discrimination sur la nationalité des personnes ou des entreprises concernées.