Privacy Shield : Bouclier ou passoire pour les données européennes ?

Suite à l'invalidation du Safe Harbor par la CJUE le 6 octobre 2015 (voir à ce sujet notre article La CJUE invalide le Safe Harbor), la Commission européenne a adopté le 12 juillet 2016 une décision d'adéquation visant à reconnaitre au mécanisme « EU-U.S. Privacy Shield » (bouclier de protection des données UE-États-unis) un niveau de protection « *équivalent* » aux exigences européennes. Ce nouvel accord a pour effet d'autoriser les transferts de données à caractère personnel depuis l'Union européenne vers les entreprises établies aux Etats-Unis utilisant ce dispositif.

Afin de garantir la conformité aux exigences de l'europe en matière de traitement des données, l'accord définit des « Privacy Shield Principles » auxquels les entreprises se doivent d'adhérer et de respecter. Toute entreprise qui viole ces principes peut être sanctionnée et doit mettre fin à l'utilisation des données collectées.

Le Privacy Shield constitue une réelle avancée dans la protection des données européennes en prenant en compte les recommandations formulées par la Commission européenne en novembre 2013 mais également certaines exigences énoncées par la CJUE dans son arrêt du 6 octobre 2015. Pour avoir une vue d'ensemble des principales nouveautés de ce dispositif, on pourra consulter la FAQ publiée par la Commission européenne le 12 juillet.

Selon Maximilien Schrems, citoyen européen à l'origine de l'invalidation du Safe Harbor, « *le bouclier Vie privée est le produit de la pression des États-Unis et de l'industrie des technologies et non le fruit d'une démarche rationnelle ou de considérations raisonnables. Il est un peu plus qu'une petite mise à jour de Safe Harbor, mais non un nouvel accord* ».

Voici les principaux reproches que l'on peut formuler à cette décision d'adéquation :

- Tout comme le Safe Harbor, le principe de certification est déclaratif basé sur le principe de l'auto-régulation. En d'autres termes, pour collecter des données européennes, les entreprises américaines n'ont qu'à s'auto-proclamer « *Privacy Shield Compliant* ». Et bien évidemment la liste des entreprises certifiées est déja longue.
- Le Privacy Shield n'interdit pas l'accès au contenu des communications par les

services de renseignement américains. Bien sûr dans le texte, il n'est pas question de parler de « surveillance de masse » mais plutôt de « collecte ciblée ». Dans sa rédaction actuelle, le Privacy Shield ne semble pas respecter l'arrêt de la CJUE du 6 octobre 2015 considérant que la collecte effectuée par l'administration des États-Unis était contraire à la Charte des droits fondamentaux de l'Union européenne.

- Pour répondre aux exigences de la CJUE et du G29, un médiateur (Ombudsman) est chargé de traiter les plaintes de tout citoyen européen qui conteste un traitement ou une surveillance illégale. Mais quelle peut-être l'indépendance de ce médiateur dès lors qu'il est nommé par le Secrétaire d'État américain ? D'autre part, le médiateur ne pourra ni confirmer ni infirmer que les États-Unis se sont livrés à une surveillance du plaignant. L'ombudsman devra conclure en disant si les lois américaines ont été respectées ou que le problème de non-conformité a bien été résolu. Naturellement, aucune institution européenne ne sera habilitée à inspecter les Datacenters ou les logiciels américains. Dans ces conditions, le plaignant n'aura strictement aucun regard possible sur la réalité de la surveillance effectuée.
- Le Privacy Shield ne se substitue pas aux deux alternatives actuellement en vigueur que sont les clauses contractuelles types (EU model clauses) ou les règles internes d'entreprises (BCR). En conséquence, si une entreprise couverte par le Privacy Shield s'en fait exclure pour non-respect des obligations, elle pourra quand même continuer à traiter les données via l'un des deux mécanismes précédemment cités.
- La conservation des données n'est pas limitée dans le temps. Les sociétés américaines peuvent donc utiliser les données aussi longtemps qu'elles le souhaitent tant que cela sert l'objectif pour lequel elles ont été initialement collectées ou ultérieurement autorisées.
- Même si une révision annuelle est prévue, il parait surprenant que l'accord porte uniquement sur les exigences de la Directive 95/46/EC alors même qu'un nouveau règlement européen plus contraignant entrera en vigueur le 25 mai 2018 et abrogera la directive de 1995. Pourquoi n'a t-on pas prévu une clause de suspension afin de prendre en compte les exigences du nouveau règlement dans un nouvel accord UE/US ? Pourquoi la Commission européenne veut-elle alourdir les contraintes réglementaires sur les entreprises européennes alors que dans le même temps elle semble se satisfaire des promesses des sociétés américaines ?

Compte tenu des réserves que nous venons d'évoquer, il n'est pas impossible de voir le Privacy Shield faire l'objet d'un recours devant la CJUE, seule compétente pour constater la validité d'un acte de l'union conformément à l'article 263 du Traité sur le fonctionnement de l'Union européenne (TFUE).