Un nouveau cadre juridique pour les transferts de données personnelles des citoyens européens aux Etats-Unis

Le nouvel accord intitulé « US-EU Privacy Shield » doit permettre une meilleure protection des données pour les européens.

Des obligations fortes pour les entreprises américaines **:** la publication de ces engagements sera **contrôlée par le département du commerce**, ce qui les rendra exécutoires. Des sanctions, voire l'exclusion des entreprises importatrices de données du nouveau dispositif, pourraient être appliquées à l'encontre des entreprises se trouvant en violation de leurs obligations.

Des garanties sur l'accès aux données par le Gouvernement américain **:** l'accès aux données des européens par les autorités américaines feront l'objet de **limites claires, de garde-fous et de mécanismes de supervision.** Ces exceptions doivent être strictement nécessaires et proportionnées. Les Etats-Unis se sont engagés à ne pas effectuer de surveillance de masse généralisée. Toutefois, Vera Jourova (commissaire à la justice et aux consommateurs) a souligné qu'***« une lettre officielle du bureau de la NSA s'engageant dans le nouveau processus est la seule caution que nous ayons obtenue des Etats-Unis dans ce nouveau processus ».***

Des recours pour les citoyens européens **:** plusieurs recours sont ouverts pour les citoyens européens. Les entreprises ont des délais limites pour répondre aux plaintes reçues. En dernier lieu un arbitrage sera rendu. Les autorités européennes de protection des données pourront adresser des plaintes au Département du commerce et à la FTC. Pour les plaintes concernant l'accès des services de renseignements un « *ombudsman* » (médiateur indépendant) interviendra.

Un **rapport** annuel sur l'application de ce nouveau cadre sera publié.

Ce nouveau texte est destiné à remplacer l'accord « Safe Harbor » du 26 juillet 2000. Pour rappel, ce dernier permettait le transfert de données vers les entreprises adhérentes aux Etats-Unis, et donc la localisation dans des serveurs situés sur le sol des Etats-Unis, des données relatives à des citoyens européens[1]. Or, les révélations d'Edward **Snowden** sur le programme Prism, permettant à la NSA d'accéder aux données stockées par les géants du Net, ont mis en lumière la faiblesse de cette protection. En mars 2014, le Parlement européen demandait déjà la suspension du « Safe Harbor », et Bruxelles et Washington s'engageaient dans une renégociation. Mais c'est l'action du militant autrichien **Max Schrems** contre les pratiques de Facebook qui a conduit à l'**invalidation** de cet accord, par la Cour de justice de l'Union européenne, le 6 octobre dernier. Aux

lendemains de cette décision, le **G29**, qui réunit les autorités de protection des données de l'ensemble des pays européens, avait demandé aux autorités des deux continents de s'accorder sur un nouveau dispositif avant le 31 janvier. Malgré cette insécurité juridique, les entreprises peuvent, en attendant, avoir recours à des solutions alternatives, via des **clauses contractuelles** ou des **« binding corporate rules »** (règles internes aux entreprises). Cet accord doit mener à **un projet de décision pour les prochaines semaines.**

Par ailleurs, **tout citoyen européen devrait pouvoir à l'avenir faire valoir en justice ses droits sur ses données personnelles**. Cette possibilité a été introduite par voie d'amendement au ***Judicial Redress Act***, qui doit encore être adopté par le Sénat (à une date incertaine). Néanmoins, un sous amendement impose une réserve de taille à ce nouveau droit, rendant l'ensemble des nouvelles dispositions floues : ***« ces mesures ne seront appliquées qu'à partir du moment où elles n'entravent pas l'action des services de renseignement ».***

Le G29 s'est prononcé, ce jour, sur cet accord. Il considère que celui-ci n'est pas encore assez précisé pour l'estimer suffisant ou non. Les autorités attendent ainsi un document public d'ici fin février.

[1] Cela afin de garantir le **respect du droit européen**, et plus particulièrement à l'article 25 de la **directive 95/46 CE**, qui dispose qu'un transfert de données à caractère personnel n'est possible que si *« le pays tiers assure un niveau de protection adéquat »*.