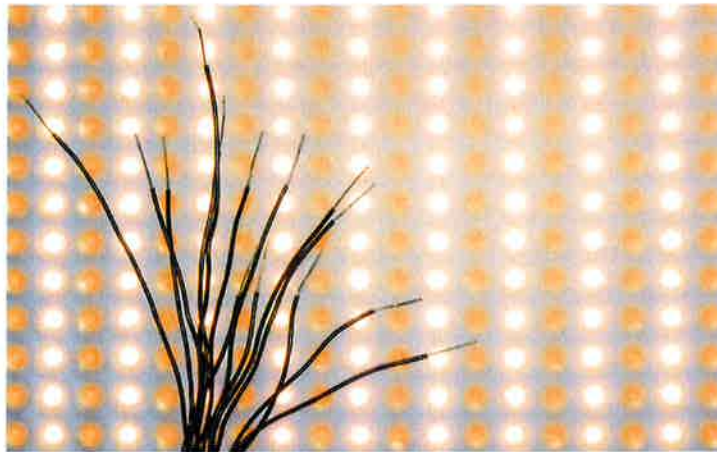


Invalidation de l'accord "Safe Harbor" : quel impact pour les entreprises ?

ANNA MILLERET-GODET / AVOCATE AU PÔLE SOCIAL DU CABINET COHEN & GRESSER PARIS | LE 30/10 À 12:36



Invalidation de l'accord "Safe Harbor" : quel impact pour les entreprises ?

La Cour de Justice de l'Union Européenne (CJUE) a rendu une décision jugée par certains comme historique : elle a invalidé le Safe Harbor, qui autorisait le transfert et le stockage de données aux États-Unis.

Le 6 octobre dernier, la Cour de Justice de l'Union Européenne (CJUE) a invalidé le Safe Harbor. Cet accord, entre l'UE et les États-Unis, autorisait le transfert et le stockage de données personnelles depuis l'Union européenne vers des entreprises américaines adhérentes (Facebook, Amazon...). Pourtant, une décision de la Commission européenne du 26 juillet 2000, l'avait jugé conforme aux exigences européennes et disposant d'un niveau de protection suffisant des données ainsi transférées.

Mais il est vrai que le Safe Harbor était déjà largement remis en cause depuis quelques années, et particulièrement depuis les révélations d'Edward Snowden. Dans cette lignée, un ressortissant autrichien, Maximilian Schrems a saisi la CJUE afin d'interdire le transfert de ses données personnelles en tant qu'utilisateur Facebook, depuis la filiale irlandaise à la société mère aux États-Unis.

À la suite de cette décision, le G29 (groupe regroupant les CNIL de toute l'Union européenne) a récemment apporté des précisions quant à ses conséquences juridiques, mais en pratique que doivent faire les entreprises européennes concernées ?

• L'Europe et la protection de la vie privée : une tradition de longue date

Alors que le projet de Règlement européen qui constituera à l'avenir le socle de la politique européenne en matière de protection de la vie privée fait débat entre le Parlement, le Conseil et la Commission, l'invalidation du Safe Harbor vient consolider le profond attachement de l'Europe à la protection des

données personnelles qui peut se révéler en totale opposition avec les lois américaines et notamment le programme de surveillance de la National Security Agency (NSA).

En résumé, les règles européennes interdisent les transferts de données personnelles d'un État membre vers un État tiers, sauf si ces transferts présentent un niveau de protection "adéquat", notamment dans le cadre du Safe Harbor. Pour autant, la loi américaine consacre la primauté des exigences relatives à la sécurité nationale, à l'intérêt public et au respect des lois des États-Unis qui permettent d'écarter "sans limitation" les clauses du Safe Harbor qui leur seraient contraires.

C'est pour cette raison que la CJUE a considéré que la Commission européenne, qui avait alors validé 15 ans plus tôt le dispositif de Safe Harbor, n'avait pas recherché si les États-Unis assuraient effectivement une protection adéquate et suffisante des données personnelles transférées et a ainsi invalidé la décision d'adéquation de la Commission.

La CJUE va même plus loin en considérant que même en présence d'une décision d'adéquation de la Commission européenne, les autorités nationales de protection des données (la CNIL en France) doivent néanmoins pouvoir examiner si le transfert des données personnelles de l'UE vers un pays tiers respecte ou non les exigences de la directive européenne, et ce en toute indépendance.

Ainsi, et comme le rappelle la CNIL sur son site internet, il n'est désormais plus possible de réaliser un transfert de données personnelles sur la base du Safe Harbor. Le G29 qui s'est réuni le 15 octobre dernier a néanmoins accordé un sursis de 3 mois aux autorités européennes et américaines pour trouver des "solutions politiques, juridiques et techniques permettant de transférer des données vers le territoire américain dans le respect des droits fondamentaux".

Si beaucoup évoquent déjà la simple mise en place d'un Safe Harbor 2, il semblerait que cette solution ne soit pas suffisante et qu'il faille en outre la mise en place de "mécanismes clairs et contraignants comportant au minimum des obligations de nature à garantir le contrôle des programmes de surveillance par les autorités publiques". Or, le G29 demande ici très concrètement une refonte profonde de la législation américaine ce qui ne risque pas d'arriver.

La Commission européenne et les autorités américaines ont jusqu'au 31 janvier 2016 pour trouver une solution satisfaisante. À défaut, le G29 s'engage à mettre en œuvre des mesures répressives, étant précisé qu'à ce jour, les sanctions prononcées par la CNIL à ce titre sont quasiment inexistantes.

• Conséquences de cette jurisprudence sur les entreprises

Dans l'attente d'une solution efficace à venir (ou bien à défaut de solution), les entreprises européennes, notamment celles qui font du Cloud, mais aussi plus généralement toutes celles ayant leur maison mère aux États-Unis, doivent faire preuve de vigilance concernant le transfert de données personnelles.

En effet, cela peut concerner de nombreuses données personnelles dans le domaine des ressources humaines notamment le système de rémunération, le développement de carrière, les enquêtes internes (en forte augmentation ces dernières années) concernant par exemple l'application des réglementations américaines, ou bien encore les projets de fusions ou d'acquisitions entre l'Europe et les États-Unis.

Pour ces entreprises, quelles sont donc les alternatives possibles au Safe Harbor ?

D'autres outils existent et sont prévus par la législation européenne afin d'autoriser ces transferts, notamment par le biais de clauses contractuelles types aux termes desquels les parties s'engagent à respecter certaines règles relatives à la protection des données des personnes concernées. Il peut également être recommandé, pour les transferts internes à un groupe international, d'adopter des règles internes d'entreprises ou BCR (Binding Corporate Rules).

Ces outils sont néanmoins plus contraignants à mettre en place en pratique et pourraient potentiellement ralentir le transfert des données personnelles entre UE et USA. En outre, il n'est pas exclu qu'ils soient eux-mêmes remis en cause par la CJUE dans le futur.

En effet, l'accès à des données privées dont jouissent les agences de renseignement américaines n'est pas plus limité en présence de clauses contractuelles types. Ainsi, les entreprises qui dépendent de ces mécanismes peuvent s'attendre à des contestations judiciaires futures à l'instar du Safe Harbor. ●