

Décryptage du Safe Harbor | Le Net Expert Informatique



Décryptage du Safe Harbor

La Cour de justice de l'Union européenne (CJUE) a rendu la semaine dernière une décision historique en invalidant le « Safe Harbor ». Cet accord, concocté par le Département du Commerce des États-Unis, approuvé par la Commission européenne, légalise le transfert de données personnelles de citoyens européens vers les États-Unis. Amazon, Facebook et les autres géants américains du Net pouvaient donc librement exporter nos données et les exploiter à leur guise à des fins publicitaires. Son invalidation va changer la donne, et les défenseurs du respect de la vie privée, parmi lesquels l'UFC-Que Choisir, s'en réjouissent.

Le Safe Harbor en deux mots

Europe et États-Unis ont une vision différente de la protection des données personnelles des citoyens. Leurs politiques respectives en la matière sont donc divergentes. L'Europe interdit notamment le transfert des données personnelles vers des pays qui offrent un niveau de protection inférieur au sien (1). Pour ne pas priver les entreprises américaines de cet « or numérique » en provenance de l'Europe, le Département du Commerce des États-Unis (l'équivalent d'un ministère du Commerce) a concocté un cadre juridique qui légalise le transfert de données personnelles : le Safe Harbor, aussi appelé Sphère de sécurité. Les entreprises qui souhaitent en profiter doivent garantir certaines conditions (information des consommateurs sur l'exploitation de leurs données, droit de rectification, sécurité des données, etc.) et obtenir une certification. 4 000 entreprises américaines en sont titulaires, parmi lesquelles Microsoft, Amazon, Google ou encore Facebook.

De quelles données parle-t-on ?

Les données personnelles sont au centre de la plupart des modèles économiques des entreprises du Net. Vos achats, les messages que vous publiez sur les réseaux sociaux, vos habitudes de navigation sur Internet, les mots que vous saisissez dans les moteurs de recherche, ou bien encore les livres et les films que vous achetez en ligne sont autant d'indicateurs qui permettent de définir finement des profils de consommation et de vous envoyer des publicités ciblées, donc efficaces, donc vendues à prix d'or.

Quels sont les fondements de la décision de la CJUE ?

Tout est parti d'une plainte de Maximillian Schrems, un citoyen autrichien, auprès de l'autorité irlandaise de contrôle, l'Office of the Data Protection Commissioner, l'équivalent de notre Cnil (2). Maximillian Schrems utilise Facebook et sait qu'en vertu du Safe Harbor, ses données sont traitées aux États-Unis. Mais les révélations d'Edward Snowden, en 2013, sur la surveillance opérée par la NSA (National Security Agency) prouvent que le pays n'offre pas un niveau de protection suffisant des données. Or le Safe Harbor engage les États-Unis à fournir un niveau de protection au moins équivalent à celui de l'Europe.

La CJUE s'est prononcée sur deux points. D'abord, elle a confirmé qu'une autorité nationale (la Cnil et les autres) a le droit d'enquêter lorsqu'elle est saisie par un citoyen sur le sujet, et ce malgré l'existence du Safe Harbor. Ensuite, elle estime que la Commission européenne a eu tort d'accepter cet accord sans vérifier que les États-Unis n'interdisaient pas les opérations de surveillance généralisée (comme celles de la NSA). Du coup, 15 ans après son entrée en application, la justice suspend le Safe Harbor. Une décision historique.

Cette décision va-t-elle changer quelque chose ?

À court terme, les entreprises du Safe Harbor se retrouvent dans un trou juridique. Elles doivent subitement gérer une situation passée de légale à illégale du jour au lendemain. Les grandes entreprises disposent des armes suffisantes pour poursuivre leurs activités à coup de bras de fer juridiques. Mais quid des entreprises plus modestes ?

À moyen terme, l'Europe réaffirme son attachement à la protection des données personnelles. Cette décision de la CJUE pèsera sans doute dans les discussions sur le projet de Règlement européen sur les données personnelles. Ce texte, actuellement au stade des négociations tripartites entre le Parlement, le Conseil et la Commission, constituera à l'avenir le socle de la politique européenne en matière de protection de la vie privée.

(1) Directive 95/46/CE sur la protection des données personnelles.

(2) Commission nationale de l'informatique et des libertés.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.quechoisir.org/telecom-multimedia/internet/actualite-donnees-personnelles-decryptage-du-safe-harbor>
Par Camille Gruhier