Avril 2015

A la une

Département Protection des données personnelles - vie privée

VERS UNE REMISE EN CAUSE DES ACCORDS SAFE HARBOR ?

Les accords Safe Habor sont-ils en danger ? La réponse est entre les mains de la CJUE qui doit rendre sa décision le 24 juin prochain.

La CJUE a examiné le 24 mars dernier l'affaire C-362/14 traitant des questions préjudicielles soulevées dans le cadre d'un contentieux opposant un étudiant autrichien à l'autorité Irlandaise de protection des données personnelles.

A l'origine de l'affaire, cet étudiant avait déposé une plainte devant l'autorité de protection des données irlandaise en lui demandant de suspendre les transferts de données (basés sur le Safe Harbor), concernant les utilisateurs Européens de Facebook, depuis la filiale Irlandaise vers Facebook US. A l'appui de sa demande, il affirmait qu'au vu des révélations faites par Edward Snowden, « le droit et les pratiques des Etats-Unis n'offr[aient] aucune protection réelle contre la surveillance de l'Etat. »

L'autorité irlandaise lui avait alors opposé (i) l'absence de preuve d'un quelconque manquement de la part de Facebook, (ii) la décision 2000/520/CE de la Commission Européenne du 26 juillet 2000 relative aux accords Safe Harbor (ci-après « la Décision de la Commission Européenne »), qui a reconnu que ce mécanisme assurait un niveau de protection adéquat des données à caractère personnel, et le fait qu'elle était lié par cette décision, en raison de la primauté du droit communautaire sur le droit national.

Face à ce refus, l'étudiant a donc saisi la juridiction irlandaise (*High Court*). Cette dernière a préféré transmettre des questions préjudicielles à la CJUE.

Voici donc les questions préjudicielles posées à la CJUE par la juridiction Irlandaise (High Court) :

1. Est-ce-qu'une autorité de protection des données saisie d'une plainte relative au transfert de données à caractère personnel vers un pays tiers (en l'occurrence les USA) dont le plaignant soutient que le droit et les pratiques n'offriraient pas des protections adéquates à la personne concernée est absolument liée par la constatation contraire de l'Union contenue dans la Décision de la Commission Européenne?

2. Dans le cas contraire, peut-elle ou doit-elle mener sa propre enquête en s'instruisant de la manière dont les faits ont évolué depuis la première publication de la décision de la Commission?

Quelles conséquences pour les entreprises françaises ?

Cette décision est très attendue, et pourrait avoir des conséquences importantes sur les transferts de données opérés entre entités européennes et américaines.

Par ailleurs, la réponse à la seconde question pourrait remettre en cause la philosophie même de la Directive Européenne **avec une possibilité de traitement différent du Safe Harbor d'un Etat membre de l'Union européenne à un autre.**

Pour les entreprises françaises et européennes, cette décision est loin d'être anodine, car le Safe Harbor est une base légale de transfert des données très utilisée par les responsables de traitement. En effet, un grand nombre de prestataires américains auxquels ont énormément recours les entreprises figurent sur la liste du Safe Harbor (notamment les prestataires de solutions informatiques).

Selon la décision rendue en juin par la CJUE, cela pourrait signifier :

- **la remise en cause des transferts de données vers les entreprises US sur la base du Safe Harbor ;**

- **la fin d'une politique harmonisée des différentes autorités nationales**, certaines pouvant décider de considérer que le Safe Harbor offre un niveau de protection adéquat, certaines autres pouvant décider le contraire ;

- que **les entreprises européennes n'auraient alors d'autre choix que de se tourner vers l'autre mécanisme** offert pour transférer des données en hors UE: les Clauses Contractuelles Types de la Commission Européenne.

  En France, ceci signifierait que ces transferts seraient alors soumis à autorisation préalable de la CNIL, ce qui n'est pas le cas des transferts de données vers une entreprise figurant sur la liste du Safe Harbor à l'heure actuelle (simple notification à la CNIL via l'Annexe Transfert ou inscription au registre pour les CIL).

SAFE HARBOR : DES ACCORDS DEJA CONTESTES

La décision de la CJUE dans l'affaire C-362/14 est donc très attendue, et constitue une suite dans les préoccupations émises l'année dernière par plusieurs autorités.

En effet, après l'affaire PRISM révélée par Edward Snowden, plusieurs autorités avaient émis des réserves sur les accords de Safe Harbor (notamment la conférence des commissaires allemands de protection des données), ce qui avait amené la Commission Européenne à émettre 13 recommandations en novembre 2013.

Ces 13 recommandations tendaient notamment (i) à promouvoir plus de transparence concernant les pratiques de protection des données personnelles des sociétés figurant sur la liste du Safe Harbor, (ii) à assurer la mise à disposition d'un mode alternatif de règlement des conflits, (iii) à limiter l'accès aux données par les autorités américaines, (iv) au renforcement des investigations/contrôles sur la conformité effective de ces sociétés auto-certifiées.

A la suite à ces recommandations, une réforme du Safe Harbor a été engagée entre les Etats-Unis et l'Union Européenne, dont l'issue est espérée pour le mois de mai prochain d'après Vera Jourova, chargée de la justice, des consommateurs et de l'égalité des genres à la Commission Européenne.

Quelques mois plus tard, en janvier 2014, la Commission des libertés civiles, de la justice et des affaires intérieures (du parlement Européen) avait, de son côté, demandé la suspension immédiate de la décision 2000/520/CE de la Commission Européenne qui considère les principes de Safe Harbor comme suffisamment protecteurs, et demandé aux autorités de protection des données de **suspendre immédiatement les flux de données vers une organisation ayant auto-certifiée son adhérence aux principes du Safe Harbor**. Cette demande n'avait toutefois pas été suivie d'effets.

La décision de la CJUE pourrait donc venir clarifier un peu les choses.

P.D.G.B Société d'Avocats
174, avenue Victor Hugo
75116 Paris
Tél. : 00 (33) 01.44.05.21.21
www.pdgb.com
helene.lebon@pdgb.com

Hélène LEBON - Sandra TUBERT

AUTRE PROBLEMATIQUE LIEE AUX RESEAUX SOCIAUX : L'EXAMEN DE LA CONFORMITE DE FACEBOOK AUX LOIS DE PROTECTION DES DONNEES

L'étudiant autrichien n'est pas le seul à dénoncer les pratiques du géant américain. En effet, l'autorité Belge de protection des données a commandé un rapport sur les pratiques du réseau social américain à deux universités, l'Université de Louvain et la Vreije Universiteit Brussels.

Le rapport conjoint de ces deux universités, publié en deux temps, révèle la non-conformité du réseau social américain aux lois européennes de protection des données.

Dans un premier temps, le rapport révélait notamment (i) que l'usage fait des données des utilisateurs était communiqué de manière générale et abstraite au moyen d'exemples vagues dans sa politique d'utilisation des données, (ii) et que les choix offerts par Facebook à ses utilisateurs étaient limités (du type « à prendre ou à laisser »), se traduisant par un faux sentiment de contrôle pour l'utilisateur.

La dernière version mise à jour du rapport semble, quant à elle, se concentrer sur l'installation et la collecte de données via les cookies « boutons de réseaux sociaux » (le bouton *Like* présent sur de très nombreux sites) qui seraient installés dès qu'un utilisateur se connecte à un site en contenant un.

Le rapport semble pointer du doigt le fait que Facebook traque ainsi les dispositifs des utilisateurs, que le bouton soit ou pas activé, que l'utilisateur soit ou non connecté à son compte, et ce sans son consentement, et donc en violation des **dispositions de la Directive Européenne dite « paquet télécom », qui exige le recueil du consentement préalable de l'utilisateur, ainsi que la délivrance d'une information claire, complète et précise**.

Mais le réseau social américain semble aller plus loin puisque, d'après le rapport, il traquerait également la navigation des personnes qui n'ont pas de compte Facebook, au moyen d'un identifiant unique qui serait attribué à chaque utilisateur qui aurait visité une page du domaine facebook.com. Ce tracking serait de proposer des publicités ciblées.

A la suite à sa publication, Facebook a précisé que ce rapport contenait de nombreuses inexactitudes et qu'il n'avait pas été contacté par ses auteurs avant sa publication.

Ce dossier présente un grand intérêt dans la mesure où les mentions d'information générales et abstraites sont relativement fréquentes. En conséquence, **cette position pourrait à l'avenir être utilisée par des autorités de protection des données ou des juridictions afin de contraindre des entreprises à adopter des mentions d'information plus précises.**

Par ailleurs, de nombreuses entreprises ont des partenariats commerciaux avec Facebook, ces entreprises risquent-elles de voir leur responsabilité engagée à ce titre ?

Il convient en outre de préciser que la Commission des clauses abusives a considéré, en novembre 2014 (Recommandation n°2014-02), que les conditions générales d'utilisation des réseaux sociaux contenant des clauses rédigées de manière confuse ou faisant référence, de manière imprécise, à différents types de documents (charte, politique de confidentialité, politique d'utilisation, etc) étaient abusives.

A cet égard, toute entreprise, quelle que soit son activité, pourrait voir ses clauses qualifiées d'abusives à partir du moment où celles-ci comportent des mentions d'informations aussi imprécises.