FIDAL

DELIBERATION SAN-2018-011 DU 19 DECEMBRE 2018

A titre liminaire, notons que l'organisation interne de Uber est la suivante : Uber a son siège social situé aux Etats-Unis (UBER TECHNOLOGIES INC.), elle détient son siège social européen aux Pays-Bas (UBER B.V) et dispose d'une filiale en France (UBER FRANCE SAS).

Le 21 novembre 2017, Uber publie sur son site internet un article révélant qu'elle a subi des cyber-attaques ; deux personnes extérieures à la société ont accédé aux données des utilisateurs de sa plateforme numérique, ce qui concerne, au total, 57 millions d'utilisateurs, dont 1.4 millions sont situés sur le territoire français.

Le 22 décembre 2017, la CNIL adresse un questionnaire aux sociétés UBER TECHNOLOGIES INC et UBER B.V visant à mettre en lumière les circonstances de la violation des données et les mesures prises pour y remédier.

Uber explique que des personnes extérieures sont parvenues à obtenir un accès à un espace privé de travail sur « GitHub », qui est une plateforme tierce de développement de logiciels sur internet utilisée par ses ingénieurs logiciels pour stocker du code. Les ingénieurs pouvaient ainsi se connecter à cette plateforme tierce en utilisant un nom d'utilisateur et un mot de passe, sans qu'un processus de retrait des habilitations soit mis en place lorsqu'un ingénieur quitte la société.
Les cyber-attaquants ont utilisé ces identifiants pour se connecter à la plateforme tierce et y ont trouvé une clé d'accès inscrite en clair dans un fichier de code source. Celle-ci permet d'accéder à la plateforme où sont stockées les données à caractère personnel des utilisateurs de la plateforme numérique de Uber. Ces données personnelles concernent le nom, le prénom, l'adresse de courrier électronique, la ville ou le pays de résidence, le numéro de téléphone mobile et le statut des utilisateurs (c'est-à-dire, s'ils sont conducteur, passager, ou les deux à la fois).

En premier lieu, la formation restreinte de la CNIL considère que UBER B.V et UBER TECHNOLOGIES INC revêtent la qualité de coresponsables de traitement. En effet, la qualité de responsable de traitement pour UBER B.V n'était pas contestée et UBER TECHNOLOGIES INC est responsable de traitement en ce qu'elle a géré les conséquences de la violation des données et a révélé son existence au public.

En second lieu, la formation restreinte retient l'application du droit français à UBER FRANCE SAS ; selon elle, le droit applicable d'un Etat membre dépend de deux conditions cumulatives (prévues par l'article 4.1 a) de la directive 95/46/CE et l'article 5.I 1° de la loi Informatique et Libertés) :

- l'existence d'un établissement du responsable de traitement sur le territoire de l'Etat membre, et
- la mise en œuvre du traitement des données dans le cadre des activités de cet établissement.

Or, en l'espèce, ces deux conditions sont, selon la formation restreinte, satisfaites et le droit français a donc vocation à s'appliquer.

En troisième lieu, le prononcé d'une sanction pécuniaire à l'encontre de cet établissement français ne méconnait pas le principe de personnalité des peines, comme avait pu le soutenir Uber dans le cadre de sa défense.

En quatrième et dernier lieu, la formation restreinte se prononce sur le manquement à l'obligation d'assurer la sécurité et la confidentialité des données reproché à la société Uber :

- tout d'abord, la formation restreinte estime que la plateforme tierce aurait dû être encadrée par des règles de sécurité adéquates concernant les données qu'elle stocke ayant permis d'accéder à des données à caractère personnel ; ainsi, elle aurait dû prévoir un processus relatif au retrait des habilitations des anciens ingénieurs de Uber ;
- puis, s'agissant des identifiants d'accès aux serveurs inscrits en clair dans le code source stocké sur la plateforme tierce, la formation restreinte estime que Uber aurait dû veiller à ce que ces identifiants ne puissent être divulgués à des tiers, ils ne devaient donc pas être stockés dans un fichier non protégé à l'instar du fichier de code source ;
- enfin, la formation restreinte considère que, lors de la connexion à la plateforme tierce, des précautions élémentaires en vue de préserver la sécurité et la confidentialité de cette connexion auraient dû être prises ; par exemple, avec la mise en place de mesures de filtrage des adresses IP.

Au regard de l'ensemble de ces éléments, la formation restreinte conclut à la négligence de Uber dans la mise en place de mesures élémentaires de sécurité, ce qui a permis aux cyber-attaquants de pirater sa base de données.

En conséquence, la formation restreinte prononce à l'encontre de Uber une amende pécuniaire de 400 000 euros et décide de rendre publique sa délibération.

A noter que cette décision prise sous l'empire de la loi n°78-17 du 6 janvier 1978, est riche d'enseignements sur les qualifications juridiques retenues, sur la notion de responsable de traitement, d'établissement, de loi applicable, et ceci, notamment, dans le cadre des futurs contrôles transnationaux qui seront effectués en application du RGPD (Règlement Général sur la Protection des Données).