19/12/18 - La CNIL condamne la société Uber France SAS à 400K€ d'amende !!!

Categories : Fil d'actualité RGPD

Date : jeudi 27 décembre 2018

Nota : Compte tenu de la date des faits, le RGPD n'était pas encore applicable.

Faits :

En novembre 2017, la société américaine Uber Technologies Inc. (ci-après Uber Inc.) a révélé dans la presse … avec un an de retard... que deux individus avaient piraté fin 2016 les données personnelles de 57 millions d'utilisateurs de ses services dont celles de 600 000 chauffeurs.

Avaient ainsi été volés les noms et prénoms des utilisateurs ainsi que leurs adresses électroniques, ville, pays de résidence, numéros de téléphone mobile et statut (chauffeur / passager). Uber avait gardé secret ce vol pendant douze mois ce qui constitue une violation de la loi américaine sur la sécurité informatique et a fait l'objet d'un important buzz négatif contre Uber fin 2017, d'autant qu'Uber aurait versé 100 000 dollars aux hackers afin qu'ils ne divulguent pas l'existence de cet incident et détruisent les informations collectées. Une pratique que tous les experts en informatique préconisent de bannir.

Le G29 a créé un groupe de travail pour coordonner les procédures d'enquêtes des autorités européennes de protection des données qui ont permis de comprendre l'attaque :

- Accès par les pirates à des identifiants stockés en clair sur la plateforme collaborative de développement « Github ».
- Utilisation de ces identifiants pour accéder à un serveur de stockage des données
- Téléchargement des informations relatives à 57 millions d'utilisateurs, dont 1,4 millions situés sur le territoire français.

Responsabilité : La responsabilité de Uber B.V. n'a pas été contestée. En revanche Uber Inc. invoquait sa position de simple sous-traitant sur la base d'un contrat signé avec Uber B.V. encadrant sa marge de manœuvre vis-à-vis du traitement de données. La CNIL n'a pas retenu cet argument considérant que c'était bien Uber Inc. qui déterminait les éléments essentiels des moyens du traitement de données.

En particulier, la CNIL retient que :

- le responsable de traitement ne peut être dessaisi de la gestion des conséquences d'une violation de données
- la multitude de champs d'actions d'Uber Inc. (rédaction des lignes directrices concernant la gestion des données et appliquées par l'ensemble des sociétés du groupe, formation des nouveaux employés, signature de contrats avec des tiers fournissant des outils essentiels au service) confirme son rôle déterminant dans la détermination des finalités et moyens du traitement.

La co-responsabilité de Uber B.V. et de Uber Inc. est retenue.

La CNIL décide que l'amende sera destinée à Uber France SAS en tant qu'établissement des responsables de traitement Uber B.V. et de Uber Inc., sachant qu'Uber dispose par ce biais de locaux stables en France et exerce une activité en France (à vocation de support des conducteurs/clients et de réalisation des campagne marketing en France).

Obligation d'assurer la sécurité et la confidentialité : Ce piratage n'aurait pas abouti si certaines mesures élémentaires en matière de sécurité avaient été mises en place et en particulier :

- même si cela ne correspondait pas aux recommandations (mais à une simple possibilité) de la plateforme collaborative de développement « Github », Uber aurait dû prévoir que ses ingénieurs se connectent à « Github » grâce à une mesure d'authentification forte (par exemple, un identifiant et un mot de passe puis un code secret envoyé sur un téléphone). En pratique, leur accès se faisait avec leur simple adresse e-mail personnelle et un mot de passe configuré par eux-mêmes et aucune procédure de retrait d'habilitation n'était prévue lorsqu'un ingénieur quittait la société ;
- Uber n'aurait pas dû stocker en clair au sein du code source de la plateforme « Github » des identifiants permettant d'accéder au serveur ;
- pour l'accès aux serveurs contenant les données des utilisateurs, elle aurait dû mettre en place un système de filtrage des adresses IP.

Dans ces conditions, la formation restreinte a estimé que la société avait manqué à son obligation de sécurité des données personnelles. Elle a condamné la société Uber France SAS, établissement des sociétés Uber Technologies Inc. et Uber B.V, à une amende de 400 000 euros.

Sanction : Une amende de 400K€

Publication de la décision : Au regard du nombre très important de personnes concernées et de la nécessité de sensibiliser les opérateurs

NB. Le 06/11/18, l'autorité néerlandaise de protection des données a prononcé une amende de 600K€ à l'encontre d'UBER pour manquement à l'obligation de notification de la violation de données. Le 26/11/18, l'autorité britannique a prononcé une sanction de 385 000 £ pour manquement à l'obligation de sécuriser les données.

NB. Rappelons que l'usage de la plateforme Ghitub avait déjà été lié en juillet 2018 à la condamnation de la société Dailymotion pour manquement à l'obligation de sécurité (voir Infra dans le Fil d'actu !).

https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037830841&fastReqId=413824161&fastPos=1