Uber France : sanction de 400 000€ prononcée par la CNIL

Date : 29 décembre 2018

Le 19 décembre 2018, la formation restreinte de la Commission nationale de l'informatique et libertés (CNIL) a prononcé une sanction pécuniaire de 400 000€ à l'encontre de la société Uber France SAS pour manquement à l'obligation d'assurer la sécurité des données à caractère personnel (Délibération n°SAN-2018-011 du 19 décembre 2018).

Rappelons qu'en novembre 2017, la société de transport avec chauffeur a révélé sur son site Internet qu'à la fin de l'année 2016, deux individus avaient eu accès aux données à caractère personnel relatives à 57 millions d'utilisateurs des services, dont 1,4 millions sur le territoire français (passagers et conducteurs).

A la suite de cette révélation, le Groupe de l'Article 29 (G29) avait créé un groupe de travail pour coordonner les procédures d'investigation des différentes autorités de protection des données.

L'autorité néerlandaise de protection des données a ensuite prononcé une sanction pécuniaire de 600 000€ à l'encontre de la société Uber. L'autorité anglaise a quant à elle prononcé une sanction pécuniaire d'environ 400 000€.

Mathias Avocats revient sur cette sanction et fait le point.

Quels sont les faits ?

La société Uber Technologies INC est une société donc le siège social est situé aux Etats-Unis et dont l'activité principale est le transport de personnes avec chauffeur. Elle possède une filiale sur le territoire

français, Uber France SAS.

Le 22 décembre 2017, la CNIL a adressé à la société de droit américain et à la société de droit néerlandais un questionnaire portant sur les circonstances de la violation de données. En l'espèce, il a été exposé que la société de transport utilisait GitHub, plateforme tierce de développement de logiciel sur le réseau Internet, pour stocker du code. Les ingénieurs de la société se connectaient à cette plateforme en utilisant une adresse électronique personnelle et un mot de passe qu'ils configuraient eux-mêmes, de manière individuelle.

Or, les attaquants ont utilisé ces identifiants pour se connecter à la plateforme GitHub et y ont trouvé une clé d'accès inscrite en clair dans un fichier de code source. Cette clé d'accès permettait d'accéder à la plateforme d'hébergement où sont stockées les données à caractère personnel des utilisateurs des services de la société de transport. Ils ont ainsi pu télécharger à partir de cette plateforme des données à caractère personnel.

Un manquement à l'obligation d'assurer la sécurité des données

Mathias Avocats vous souhaite une bonne lecture !

Le règlement général sur la protection des données (RGPD) n'étant pas applicable à l'époque des faits, la CNIL a appliqué la loi du 6 janvier 1978 modifiée. En application de l'article 34 de la loi du 6 janvier 1978 modifiée, le responsable du traitement est tenu de prendre toutes précautions utiles, en considération de la nature des données et des risques présentés par le traitement pour préserver la sécurité des données, et notamment empêcher que des tiers non autorités y aient accès. Au regard de ce texte, la délibération de la CNIL relève plusieurs manquements relatifs à la sécurité des données à caractère personnel.

- Le premier manquement relevé a trait à la sécurisation de l'accès à la plateforme GitHub.

La formation restreinte de la CNIL relève que la plateforme GitHub était un outil de travail central dans le développement des activités de la société, dont l'accès aurait dû être encadré par des règles de sécurité adéquates.

Dans ce contexte, le fait que la plateforme GitHub recommande que les ingénieurs utilisent des identifiants personnels pour se connecter n'a pas été pris en compte par la formation restreinte.

Cette dernière a ainsi estimé que malgré les recommandations de l'éditeur de la plateforme, la société – en tant que responsable du traitement – aurait du adopter les règles de nature à garantir la sécurité des informations qu'elle y stockait. Ces mesures s'imposant d'autant plus que, *in fine,* la connaissance desdites informations permettait d'accéder et d'extraire les données à caractère personnel de plusieurs millions d'utilisateurs.

L'absence de processus relatif au retrait des habilitations des anciens ingénieurs est également reprochée à la société de transport. Selon la formation restreinte de la CNIL, il s'agit d'une « négligence importante puisque la société était dans l'impossibilité de garantir que des personnes ayant quitté la société ne continuaient pas d'accéder aux projets développés ».

- Le deuxième manquement a trait à la présence en clair d'identifiants d'accès aux serveurs dans un code source stocké sur la plateforme GitHub.

La société a pu expliquer qu'il ne s'agissait que d'un incident isolé attribuable à une erreur humaine. Toutefois, la formation restreinte rappelle qu'en matière d'identification, il est important de veiller à ce que les identifiants permettant de se connecter à des serveurs hébergeant des données à caractère personnel ne puissent pas être divulgués. Il est donc impératif que de tels identifiants ne soient pas

stockés en clair au sein du code source de la plateforme, comme c'était le cas en l'espèce.

- Le troisième manquement a trait à la mise en place d'une mesure de filtrage des adresses IP autorisées à accéder aux serveurs.

La formation restreinte de la CNIL met en avant le fait que lorsque des collaborateurs sont amenés à se connecter à distance aux serveurs utilisés par une entreprise, la sécurisation de cette connexion constitue une précaution élémentaire afin de préserver la confidentialité des données traitées.

Cette sécurisation peut reposer *a minima* sur la mise en place d'une mesure de filtrage des adresses IP afin que seules soient exécutées des requêtes provenant d'adresses IP identifiées.

Or, une telle mesure de filtrage des adresses IP n'a pas été mise en place par la société de transport dès le début de l'utilisation du service.

Au regard des éléments énumérés ci-dessus la formation restreinte estime donc que la société a fait preuve de négligence et qu'elle n'a pas pris toutes les précautions utiles afin d'empêcher les tiers non autorisés d'accéder aux données traitées. Le manquement à l'article 34 de la loi du 6 janvier 1978 modifié est donc constitué.

Quelle sanction ?

La formation restreinte rappelle que le fait que les données accessibles ne contiennent aucune donnée pouvant être qualifiée de sensible, au sens de l'article 8 de la loi Informatique et Libertés, est sans influence sur la caractérisation du manquement à l'obligation incombant à un responsable de traitement d'assurer la sécurité des données qu'il traite.

En outre, elle souligne que la violation a concerné :

- un nombre très important d'utilisateurs (1,4 millions sur le territoire français),
- des données identifiantes tels que le nom, le prénom, l'adresse de courrier électronique, la ville ou le pays de résidence et le numéro de téléphone mobile.

Tout en relevant qu' « aucun dommage subi par les personnes à la suite de la violation de données n'a été rapporté à ce jour », la formation restreinte souligne que la société de transport ne peut pas invoquer avec certitude l'absence totale de dommage subi par les personnes concernées dans la mesure où il n'est pas contesté que les attaquants ont eu accès à des données à caractère personnel. La formation restreinte estime donc qu'un usage malveillant desdites données est toujours possible.

Ainsi, la formation restreinte de la CNIL prononce une sanction pécuniaire de 400 000€ à l'encontre de la filiale française.

La publicité de la sanction est quant à elle motivée par la gravité du manquement, le contexte de multiplication des incidents de sécurité et la nécessité de sensibiliser les responsables de traitements et les utilisateurs quant aux risques pesant sur la sécurité des données

Que retenir ?

La lecture de la délibération de la formation restreinte conduit donc à insister sur l'importance des mesures de sécurité à mettre en œuvre, notamment dans l'hypothèse du recours à une plateforme tierce.

Ainsi, la mise en place de mesures d’authentification fortes des personnes accédant aux données, la révocation des autorisations d’accès, le filtrage d’adresses IP ou encore le stockage sécurisé des identifiants seront autant de mesures à définir.

Cette sanction de 400 000€ euros vient s’additionner aux sanctions prononcées par les autorités anglaises et néerlandaises. Le montant cumulé des sanctions pécuniaires prononcées contre les entités européennes du groupe de transport à la suite de la violation de données s’élève ainsi à 1,4 millions d’euros.

Mathias Avocats vous souhaite une bonne lecture !