Le : 27/03/2019

Date de publication sur legifrance: 20/12/2018

Commission Nationale de l'Informatique et des Libertés

Délibération n°SAN-2018-011 du 19 décembre 2018
Délibération de la formation restreinte n° SAN-2018-011 du 19 décembre 2018 prononçant une sanction pécuniaire à l'encontre de la société UBER FRANCE SAS

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ , Président, M. Alexandre LINDEN, Vice-président, Mme Dominique CASTERA, Mme Marie-Hélène MITJAVILE et Monsieur Maurice RONAI, membres ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, notamment ses articles 45 et suivants ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par le décret n° 2007-451 du 25 mars 2007 ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2017-279C du 8 décembre 2017 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification de l'ensemble des traitements de données à caractère personnel portant, en tout ou partie, sur des données relatives à la commercialisation ou à l'utilisation des produits ou services rattachés à la marque UBER ;

Vu la décision de la Présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 13 juin 2018 ;

Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, notifié à la société UBER FRANCE SAS le 6 août 2018 et adressé pour information aux sociétés UBER B.V et UBER TECHNOLOGIES INC. ;

Vu les observations écrites des sociétés UBER FRANCE SAS, UBER B.V et UBER TECHNOLOGIES INC. reçues le 24 septembre 2018 ;

Vu la réponse du rapporteur aux observations des sociétés UBER FRANCE SAS, UBER B.V et UBER TECHNOLOGIES INC., notifiée le 9 octobre 2018 ;

Vu les nouvelles observations écrites des sociétés UBER FRANCE SAS, UBER B.V et UBER TECHNOLOGIES INC. reçues le 23 octobre 2018 ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Etaient présents, lors de la séance de la formation restreinte du 8 novembre 2018 :

· M. François PELLEGRINI, Commissaire, en son rapport ;

En qualité de représentant de la société UBER FRANCE SAS :
· […]

En qualité de représentant de la société UBER B.V :
· […]

En qualité de conseil des sociétés UBER FRANCE SAS, UBER B.V et UBER TECHNOLOGIES INC. :
· […]
· […]
· […]
· […]
· […]

En qualité d'interprète :
· […]

Mme Eve JULLIEN, Commissaire du Gouvernement adjointe, n'ayant pas formulé d'observations ;

Les représentants de la société UBER ayant pris la parole en dernier ;

A adopté la décision suivante :

I- Faits et procédure

La société UBER TECHNOLOGIES INC., fondée en 2009 et dont le siège social est situé au 1455 Market Street à San Francisco aux Etats-Unis, a pour activité principale le transport de personnes avec chauffeur, dit VTC , *via* une plateforme web et une application mobile.

Afin de proposer ce service dans d'autres pays, plusieurs filiales ont été créées dans le monde, dont la société UBER B.V, située au 7 Meester Treublaan, à Amsterdam aux Pays-Bas et la société UBER FRANCE SAS, située 5, rue Charlot, à Paris. La société UBER compte environ 16 000 salariés. En 2017, elle a réalisé un chiffre d'affaires d'environ 6 milliards d'euros.

Le 21 novembre 2017, la société UBER TECHNOLOGIES INC. a publié sur son site internet un article faisant état de ce qu'à la fin de l'année 2016, deux individus extérieurs à la société avaient accédé aux données de 57 millions d'utilisateurs des services UBER à

travers le monde. Cette information a ensuite été reprise dans de nombreux articles de presse dont certains faisaient état de ce que la société avait versé aux attaquants la somme de 100 000 dollars américains afin que ceux-ci détruisent les données en question et qu'ils ne révèlent pas l'existence de cet incident.

Le 28 novembre 2017, la société UBER B.V a adressé un courrier à la Présidente du Groupe de travail de l'article 29 sur la protection des données (ci-après G29) l'informant des circonstances de la violation de données et de sa volonté de coopérer avec toutes les autorités compétentes sur cette affaire.

Le 29 novembre 2017, l'Assemblée Plénière du G29 a mandaté la création d'un groupe de travail appelé *taskforce* dans le but de coordonner les procédures d'investigations de différentes autorités de protection des données. Ce groupe de travail est composé des autorités néerlandaise, espagnole, française, belge, italienne, britannique et slovaque.

En application de la décision n° 2017-279C du 8 décembre 2017 de la Présidente de la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission), une délégation de la CNIL a adressé le 22 décembre 2017 aux sociétés UBER TECHNOLOGIES INC. et UBER B.V (ci-après la société UBER ou la société) un questionnaire portant notamment sur les circonstances de la violation de données et sur les mesures prises par les sociétés pour assurer la sécurité des données traitées.

Le 22 janvier 2018, la société a répondu au questionnaire, expliquant que la violation de données s'était déroulée en trois étapes.

En premier lieu, la société a précisé que des *personnes extérieures ont obtenu l'accès à un espace de travail privé Uber sur GitHub. GitHub est une plateforme tierce de développement de logiciel sur internet qui était utilisée par les ingénieurs logiciels chez Uber au moment de l'incident pour stocker du code pour la collaboration et le développement .* Elle a indiqué que *les ingénieurs d'Uber se connectaient à GitHub en utilisant un nom d'utilisateur et un mot de passe configuré par eux-mêmes. Ces identifications prenaient le format d'une adresse email personnelle au titre de nom d'utilisateur ainsi qu'un mot de passe individuel.* Elle a précisé que la plateforme était utilisée par […] ingénieurs et qu'il n'existait pas de processus de retrait des habilitations lorsqu'un ingénieur quitte la société.

En deuxième lieu, la société a indiqué que les attaquants avaient utilisé ces identifiants pour se connecter à la plateforme GitHub et avaient trouvé une clé d'accès inscrite en clair dans un fichier de code source. Cette clé d'accès était relative à un compte de service permettant d'accéder à la plateforme d'hébergement […] où sont stockées les données à caractère personnel des utilisateurs des services UBER.

En troisième lieu, la société a expliqué que les attaquants avaient utilisé cette clé d'accès pour accéder aux bases de données de la société UBER stockées sur les serveurs […], et ainsi télécharger une quantité importante de données personnelles.

La société a expliqué que la violation de données avait concerné 57 millions d'utilisateurs dans le monde dont 1,4 million sur le territoire français. Parmi ces utilisateurs se trouvaient 1,2 million de passagers et 163 000 conducteurs. La société a précisé que les attaquants avaient eu accès aux données suivantes : nom, prénom, adresse de courrier électronique, ville ou pays de résidence, numéro de téléphone mobile et statut des utilisateurs (conducteur, passager ou les deux).

La société a enfin expliqué qu'à la suite de la violation de données, elle avait mis en place […]

Aux fins d'instruction de ces éléments, la Présidente de la Commission a désigné M. François PELLEGRINI en qualité de rapporteur, le 13 juin 2018, sur le fondement de l'article 46 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après loi du 6 janvier 1978 modifiée ou loi Informatique et Libertés).

A l'issue de son instruction, le rapporteur a notifié à la société UBER FRANCE SAS le 6 août 2018, et communiqué pour information aux sociétés UBER B.V et UBER TECHNOLOGIES INC., un rapport détaillant les manquements à la loi qu'il estimait constitués en l'espèce et a proposé à la formation restreinte de la CNIL de prononcer une sanction pécuniaire de quatre cent mille (400.000) euros qui serait rendue publique. Ce rapport était accompagné d'une convocation pour la séance de la formation restreinte du 11 octobre 2018 et invitait la société à produire des observations en réponse dans un délai courant jusqu'au 24 septembre 2018. Par courrier du 2 octobre 2018, la société a été informée que la séance de la formation restreinte était reportée au 8 novembre suivant.

Le 24 septembre 2018, la société a, par l'intermédiaire de son conseil, produit des observations écrites auxquelles le rapporteur a répondu le 9 octobre suivant en application des dispositions prévues par l'article 75 du décret n° 2005-1309 du 20 octobre 2005 modifié.

Le 23 octobre 2018, la société a produit de nouvelles observations en réponse à celles du rapporteur.

II- Motifs de la décision

1. Sur la qualité de responsable de traitement des sociétés UBER TECHNOLOGIES INC. et UBER B.V

Le I de l'article 3 de la loi du 6 janvier 1978 modifiée dispose que le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.
Cette disposition constitue la transposition de l'article 2 d) de la directive qui définit le responsable de traitement comme la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel.
La société UBER fait valoir que seule la société UBER B.V peut être considérée comme responsable de traitement et que la société UBER TECHNOLOGIES INC. n'agit qu'en qualité de sous-traitant de la société UBER B.V. Elle rappelle que l'ensemble des tâches accomplies par UBER TECHNOLOGIES INC. dans le cadre du traitement s'inscrivent dans la marge de manœuvre dont dispose cette société, en tant que sous-traitant, dans la manière dont le traitement des données est effectué. Elle rappelle qu'un contrat de sous-traitance a été conclu entre les deux sociétés et que c'est en tant que sous-traitant que la société UBER TECHNOLOGIES INC. a rédigé des lignes directrices concernant la gestion des données, qu'elle assure la formation des nouveaux employés du groupe, qu'elle a signé des contrats avec des sociétés tierces et qu'elle a géré les conséquences de la violation de données.

En premier lieu, la formation restreinte relève que la qualité de responsable de traitement de UBER B.V n'est pas contestée.

En second lieu, la formation restreinte rappelle que selon l'avis n° 1/2010 du G29 du 16 février 2010 sur les notions de responsable du traitement et de sous-traitant , un sous-traitant qui acquiert un rôle important dans la détermination des finalités ou des moyens essentiels du traitement est davantage un (co-)responsable du traitement qu'un sous-traitant. L'avis du G29 précise que la notion de responsable de traitement repose sur une analyse factuelle plutôt que formelle.

Elle relève par ailleurs que cet avis fait état de ce qu' *alors que la détermination de la finalité du traitement emporterait systématiquement la qualification de responsable du traitement, la détermination des moyens impliquerait une responsabilité uniquement lorsqu'elle concerne les éléments essentiels des moyens.*

La formation restreinte note encore qu'il ressort des pièces du dossier que le service proposé *constitue une application unique conçue et développée aux Etats-Unis par* la société UBER TECHNOLOGIES INC, application qui a été dans un second temps proposée dans d'autres régions du monde, en étant, en tant que de besoin, simplement adaptée en fonction des législations des Etats.

La formation restreinte relève en particulier que c'est bien la société UBER TECHNOLOGIES INC. qui a géré les conséquences de la violation de données. En particulier, ce sont les équipes d'UBER TECHNOLOGIES INC. qui […].

La société UBER B.V n'est pas intervenue au cours de ce processus alors même que la violation de données concernait pour partie des données relatives aux utilisateurs de l'application UBER se trouvant sur le territoire de l'Union européenne, territoire pour lequel la société UBER B.V est pourtant décrite dans les observations comme seule responsable de traitement. La formation restreinte relève encore que c'est la société UBER TECHNOLOGIES INC […].

Enfin, c'est la société UBER TECHNOLOGIES INC. qui a, par l'intermédiaire d'un article publié par son directeur général, révélé l'existence de la violation au public.

La formation restreinte considère que la gestion des conséquences de la violation de données n'est pas une simple question technique ou d'organisation qui peut entièrement relever de la marge de manœuvre dont dispose un sous-traitant. Au contraire, la gestion d'une violation de données est une question attachée à un élément essentiel d'un moyen de traitement, dont le responsable de traitement ne peut être dessaisi.

A cette fin, la société UBER TECHNOLOGIES INC. a rédigé plusieurs documents clés relatifs à la gestion des données personnelles collectées, dont les directives qui sont appliquées par l'ensemble des entités du groupe UBER. C'est également cette entité qui est en charge de la formation des nouveaux employés du groupe. La formation restreinte souligne également que c'est la société UBER TECHNOLOGIES INC. qui a conclu des contrats avec plusieurs sociétés tierces, dont […], qui fournissent des outils essentiels au fonctionnement du service tels que ceux permettant la gestion de campagnes marketing.

La formation restreinte considère que la multitude des champs d'actions dans lesquels intervient la société UBER TECHNOLOGIES INC. témoignent *du rôle déterminant qui est le sien dans* la détermination des finalités et moyens du traitement. En conséquence, les

sociétés UBER. B.V et UBER TECHNOLOGIES INC. doivent être conjointement qualifiées de responsables de traitements.

2. Sur le droit applicable

Le I de l'article 5 de la loi du 6 janvier 1978 modifiée dispose que *s ont soumis à la présente loi les traitements de données à caractère personnel : 1°Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi* .

Cet article constitue la transposition en droit interne de l'article 4-1-a) de la directive 95/46/CE du 24 octobre 1995 sur le droit national applicable qui dispose que : *1. Chaque État membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque : a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre ; si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable .*

Au regard de ces dispositions, le droit applicable d'un État membre dépend de deux conditions cumulatives : l'existence d'un établissement du responsable de traitement sur le territoire d'un État membre et la mise en œuvre du traitement de données dans le cadre des activités de cet établissement.

S'agissant du premier critère, la formation restreinte rappelle que dans son arrêt *Weltimmo* , du 1er octobre 2015, la Cour de justice de l'Union européenne a précisé que *la notion d'établissement, au sens de la directive 95/46, s'étend à toute activité réelle et effective, même minime, exercée au moyen d'une installation stable* , le critère de stabilité de l'installation étant examiné au regard de la présence de *moyens humains et techniques nécessaires à la fourniture de services concrets en question* (points 30 et 31 de l'arrêt).

En l'espèce, la formation restreinte relève tout d'abord que la qualité d'établissement de la société UBER FRANCE SAS n'est pas contestée. Elle relève ensuite que cette société dispose de locaux stables situés en France au sein desquels ses employés sont notamment en charge d'activités de support à l'attention des conducteurs et de la réalisation de campagnes marketing du groupe sur le territoire français.

La formation restreinte considère donc, au vu de ces éléments et à la lumière de la jurisprudence de la Cour de justice de l'Union européenne en la matière, que la société UBER FRANCE SAS dispose d'une installation stable sur le territoire français au moyen de laquelle elle exerce une activité réelle et effective grâce à des moyens humains et techniques nécessaires notamment à la fourniture des services des sociétés UBER B.V et UBER TECHNOLOGIES INC.

S'agissant du second critère, la formation restreinte rappelle que dans son arrêt *Costeja* du 13 mai 2014 , la Cour de justice de l'Union européenne a précisé qu'un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement lorsque celui-ci est destiné à assurer l'activité de promotion et de vente des espaces publicitaires pour les besoins d'une entreprise située dans un État tiers. Elle relève qu'en l'espèce, la société UBER FRANCE SAS réalise des campagnes marketing pour

promouvoir les services de la société UBER et assure un service de support auprès des clients et des conducteurs. Par conséquent, le traitement en cause doit être regardé comme étant effectué dans le cadre des activités d'un établissement des responsables de traitements que sont les sociétés UBER B.V et UBER TECHNOLOGIES INC.

La formation restreinte conclut que les deux critères prévus par l'article 4.1 a) de la directive et l'article 5.I.1° de la loi Informatique et Libertés étant remplis, le droit français s'applique, y compris la possibilité pour la CNIL de prononcer une sanction pécuniaire.

3. Sur le destinataire de la mesure

La société UBER considère que la CNIL ne peut imposer une sanction qu'à un responsable de traitement et non à un simple établissement à qui les manquements à la loi Informatique et Libertés ne sauraient être imputés. Elle rappelle qu'en l'espèce, la survenance de la violation de données est uniquement imputable à UBER B.V en tant que responsable de traitement. Elle estime par conséquent que prononcer une sanction à l'encontre de la société UBER FRANCE SAS constituerait une violation manifeste du principe de personnalité des peines.

La formation restreinte rappelle que la Cour de Justice de l'Union européenne a dit pour droit dans son arrêt *Wirtschaftsakademie Schleswig-Holstein GmbH* du 5 juin 2018 que *lorsq u'une entreprise établie en dehors de l'Union dispose de plusieurs établissements dans différents Etats membres, l'autorité de contrôle d'un Etat membre est habilitée à exercer les pouvoirs que lui confère l'article 28, paragraphe 3, de cette directive à l'égard d'un établissement de cette entreprise situé sur le territoire de cet Etat membre alors même que, en vertu de la répartition des missions au sein du groupe, d'une part, cet établissement est chargé uniquement de la vente d'espaces publicitaires et d'autres activités de marketing sur le territoire dudit Etat membre et, d'autre part, la responsabilité exclusive de la collecte et du traitement des données à caractère personnel incombe, pour l'ensemble du territoire de l'Union, à un établissement situé dans un autre Etat membre.*
Cela implique par conséquent que, dès lors qu'un pouvoir dont une autorité de contrôle d'un État membre souhaite faire usage entre dans le champ de cet article, il peut être exercé à l'égard de l'établissement du responsable de traitement situé sur le territoire de cet État membre, quel que soit le type de pouvoir envisagé.
L'article 28, paragraphe 3, de la directive 95/46/CE du 24 octobre 1995 relative à la protection des données dispose que :
Chaque autorité de contrôle dispose notamment :

- *de pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle,*
- *de pouvoirs effectifs d'intervention, tels que, par exemple, celui de rendre des avis préalablement à la mise en œuvre des traitements, conformément à l'article 20, et d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement ou celui de saisir les parlements nationaux ou d'autres institutions politiques, […]*

La portée des pouvoirs dont disposent les autorités de contrôle en application de l'article 28, paragraphe 3, de la directive a été précisée par la Cour de Justice de l'Union européenne notamment dans sa décision *Weltimmo* précitée.
En effet, au point 49 de sa décision, la Cour a indiqué que *Compte tenu du caractère non exhaustif des pouvoirs ainsi énumérés et du type de pouvoirs d'intervention mentionnés à*

cette disposition ainsi que de la marge de manœuvre dont disposent les États membres pour la transposition de la directive 95/46, il y a lieu de considérer que ces pouvoirs d'intervention peuvent comprendre celui de sanctionner le responsable du traitement de données en lui infligeant, le cas échéant, une amende.
En droit interne, la possibilité pour la formation restreinte de la CNIL de prononcer une sanction pécuniaire est expressément prévue par l'article 45 de la loi Informatique et Libertés (dans sa version applicable au jour des faits) qui constitue la transposition des dispositions de l'article 28, paragraphe 3, de la directive.
La formation restreinte considère donc que dans la mesure où le pouvoir de prononcer une sanction pécuniaire entre dans le champ prévu par l'article 28, paragraphe 3, de la directive, que cette possibilité est offerte par l'article 45 de la loi Informatique et Libertés et que la société UBER FRANCE SAS constitue un établissement des sociétés UBER TECHNOLOGIES INC. et UBER B.V, responsables de traitements, il résulte de ces dispositions, telles qu'éclairées par la jurisprudence de la Cour de Justice de l'Union européenne, que le pouvoir de prononcer une sanction pécuniaire peut être exercé à l'encontre de la société UBER FRANCE SAS. Compte tenu, par ailleurs, de la nature des liens entre la société UBER FRANCE SAS et les responsables du traitement, qui mettent en œuvre leurs opérations de traitement dans le cadre des activités propres de leur établissement français, le prononcé d'une sanction pécuniaire à l'encontre de ce dernier ne saurait être regardé comme méconnaissant le principe de personnalité des peines.

4. Sur le manquement à l'obligation d'assurer la sécurité et la confidentialité des données

L'article 34 de la loi du 6 janvier 1978 modifiée dispose que *le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès .*

Il appartient à la formation restreinte de décider si la société UBER a manqué à son obligation de mettre en œuvre des moyens propres à assurer la sécurité des données à caractère personnel traitées et, en particulier, celles des utilisateurs du service UBER, afin notamment que ces données ne soient pas accessibles à des tiers non autorisés.

En défense, la société estime qu'elle n'a commis aucun manquement à ses obligations dans la mesure où, préalablement à la survenance de la violation, elle avait mis en place des mesures de sécurité suffisantes.

Tout d'abord, s'agissant de la sécurisation de l'accès à la plateforme GitHub, la société estime ne pas avoir fait preuve de négligence en autorisant ses ingénieurs à utiliser des identifiants personnels pour se connecter à GitHub. Elle précise que cette pratique constitue d'ailleurs une recommandation émise par la plateforme GitHub relative aux bonnes pratiques en matière de développement de projets. Elle explique que la mise en place d'une mesure d'authentification multifactorielle sur GitHub n'était pas obligatoire dans la mesure où cette plateforme n'était pas utilisée comme un outil interne à la société sur laquelle étaient conservées des données à caractère personnel.

La formation restreinte relève que la plateforme GitHub étant utilisée par […], elle constituait 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. En l'espèce, nonobstant la recommandation de la plateforme GitHub, il revenait bien à la société, en

tant que responsable de traitement, d'adopter des règles à même de garantir la sécurité des informations stockées sur GitHub qui, si elles ne constituaient pas en elles-mêmes des données à caractère personnel (il s'agissait des clés d'accès aux serveurs […]), permettaient en revanche d'accéder directement à une grande quantité de données relatives aux utilisateurs du service UBER, puisque ces données étaient conservées sur les serveurs […].

La formation restreinte relève que la possibilité de mettre en place une mesure d'authentification multifactorielle était exposée dans la même recommandation que celle référencée par la société. […]

Enfin, la formation restreinte considère que l'absence de processus relatif au retrait des habilitations des anciens ingénieurs constitue 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 sur Github.

Ensuite, s'agissant de la présence en clair d'identifiants d'accès aux serveurs […]dans du code source stocké sur la plateforme GitHub, la société explique qu'il s'agissait d'un incident isolé attribuable à une erreur humaine. Elle précise qu'au moment de l'incident […].

La formation restreinte rappelle qu'en matière d'authentification, il est important de veiller à ce que des identifiants permettant de se connecter de manière sécurisée à des serveurs contenant une grande quantité de données à caractère personnel ne puissent pas être divulgués. Il est donc impératif que de tels identifiants ne soient pas stockés dans un fichier qui ne serait pas protégé. Au demeurant, la formation restreinte note que la société […] recommande elle-même aux utilisateurs de ses services […] de ne pas stocker directement des identifiants dans des fichiers de code.

La formation restreinte considère que la décision de la société […] démontre qu'elle avait conscience d'une part, que des identifiants d'accès étaient potentiellement présents dans son code source et d'autre part, que la présence de telles informations au sein de GitHub était une source de risques.

Par ailleurs, s'agissant de l'absence de sécurisation de l'accès aux serveurs, la société explique […]

La formation restreinte relève que si une mesure […].

Enfin, la société explique que la mise en place d'une mesure de filtrage des adresses IP autorisées à accéder aux serveurs […].

La formation restreinte considère 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, par exemple, 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, ce qui permet d'éviter toute connexion illicite, en sécurisant les échanges de données et en authentifiant les utilisateurs.

Elle considère que compte tenu du nombre très important de personnes dont les données personnelles sont conservées les serveurs […], la mise en place d'un système de filtrage

des adresses IP, quand bien même cela nécessitait un long développement, constituait un effort nécessaire qui aurait dû être planifié dès le début de l'utilisation des services […].[…].

Au regard de ces éléments, la formation restreinte relève que la société a fait preuve de négligence en ne mettant pas en place certaines mesures élémentaires de sécurité. Ce manque de précautions généralisé est manifeste dans la mesure où le succès de l'attaque menée par les pirates a résulté d'un enchainement de négligences, illustré par les trois étapes de l'attaque. La formation restreinte considère donc que la société n'a pas pris toutes les précautions utiles afin d'empêcher que des tiers non autorisés aient accès aux données traitées et que le manquement à l'article 34 de la loi du 6 janvier 1978 modifiée est constitué.

5. Sur la sanction et la publicité

La formation restreinte rappelle que la présente décision concerne un manquement continu qui s'est prolongé après le 7 octobre 2016, date d'entrée en vigueur de la Loi pour une République numérique , et qui a été constaté à l'occasion de violation de données des faits. Par conséquent, les manquements reprochés à la société UBER doivent être appréciés sous l'empire de cette loi, qui assure la transposition en droit interne de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 (ci-après la directive) et qui était applicable à l'époque des faits.

Aux termes du I de l'article 45 de la loi du 6 janvier 1978 modifiée, dans sa version applicable au jour des constats

Lorsque le responsable d'un traitement ne respecte pas les obligations découlant de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut le mettre en demeure de faire cesser le manquement constaté dans un délai qu'il fixe. En cas d'extrême urgence, ce délai peut être ramené à vingt-quatre heures.

Si le responsable du traitement se conforme à la mise en demeure qui lui est adressée, le président de la commission prononce la clôture de la procédure. Dans le cas contraire, la formation restreinte de la commission peut prononcer, après une procédure contradictoire, les sanctions suivantes :
1° Un avertissement ;
2° Une sanction pécuniaire, dans les conditions prévues à l'article 47, à l'exception des cas où le traitement est mis en œuvre par l'Etat ;
3° Une injonction de cesser le traitement, lorsque celui-ci relève de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25.

Lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la formation restreinte peut prononcer, sans mise en demeure préalable, et après une procédure contradictoire, les sanctions prévues au présent I.

Les alinéas 1er et 2ème de l'article 47 de la loi précitée, dans sa version applicable au jour des constats, précisent que :

Le montant de la sanction pécuniaire prévue au I de l'article 45 est proportionné à la gravité du manquement commis et aux avantages tirés de ce manquement. La formation

restreinte de la Commission nationale de l'informatique et des libertés prend notamment en compte le caractère intentionnel ou de négligence du manquement, les mesures prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées, le degré de coopération avec la commission afin de remédier au manquement et d'atténuer ses effets négatifs éventuels, les catégories de données à caractère personnel concernées et la manière dont le manquement a été porté à la connaissance de la commission.
Le montant de la sanction ne peut excéder 3 millions d'euros .

La société considère que le montant de 400 000 euros n'est pas justifié dès lors que les données concernées par la violation ne sont pas des données sensibles, qu'elle a réagi promptement en prenant les mesures nécessaires afin de limiter l'impact de la violation, qu'elle a communiqué l'existence de la violation au public, que la violation n'a causé aucun préjudice aux personnes concernées et qu'elle a coopéré avec la CNIL.

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. Elle souligne en outre que la violation de données a concerné 1,4 million d'utilisateurs, soit un nombre très important de personnes, et des données identifiantes tels que le nom, le prénom, l'adresse de courrier électronique, la ville ou pays de résidence et le numéro de téléphone mobile.

Par ailleurs, si aucun dommage subi par les personnes à la suite de la violation de données n'a été rapporté à ce jour, la preuve de l'absence totale de dommage ne peut être invoquée par la société. Au demeurant, il est établi que les attaquants se sont emparés des données leur laissant ainsi la possibilité, quoique soutienne la société, d'un usage ultérieur.

Au regard des éléments développés ci-dessus, les faits constatés et le manquement constitué à l'article 34 de la loi du 6 janvier 1978 modifiée justifient que soit prononcée une sanction d'un montant de 400 000 (quatre cent mille) euros.

Enfin, la formation restreinte considère qu'au regard de la gravité du manquement précité, du contexte actuel dans lequel se multiplient les incidents de sécurité et de la nécessité de sensibiliser les responsables de traitements et les internautes quant aux risques pesant sur la sécurité des données, il y a lieu de rendre publique sa décision, conformément à l'article 46 de la loi du 6 janvier 1978.

PAR CES MOTIFS

La formation restreinte de la CNIL, après en avoir délibéré, décide :

- **de prononcer à l'encontre de la société UBER FRANCE SAS, agissant en tant qu'établissement des sociétés UBER INC et UBER BV, une sanction pécuniaire**

d’un montant de 400 000 (quatre cent mille) euros ;

- **de rendre publique sa délibération sur le site de la CNIL et sur le site de Légifrance, qui sera anonymisée à l’expiration d’un délai de deux ans à compter de sa publication.**

Le Président

Jean-François CARREZ

Cette décision est susceptible de faire l’objet d’un recours devant le Conseil d’Etat dans un délai de deux mois à compter de sa notification.