Commission Nationale de l'Informatique et des Libertés

Délibération n°SAN-2017-011 du 20 juillet 2017

Délibération de la formation restreinte n° SAN-2017-011 du 20 juillet 2017 prononçant un avertissement public à l'encontre de la société OUICAR

Etat: VIGUEUR

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ, Président, de M. Alexandre LINDEN, Vice-président, Mme Dominique CASTERA, Mme Marie-Hélène MITJAVILE et M. 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 loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 45 et suivants ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés 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 les décisions n° 2016-226C et 2016-231C du 27 juillet 2016 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder, d'une part, à une mission de vérification de tous traitements relatifs au site OUICAR.FR et, d'autre part, à une mission de vérification auprès de la société OUICAR ;

Vu la décision de la Présidente de la Commission portant désignation d'un rapporteur devant la formation restreinte, en date du 20 avril 2017 ;

Vu le rapport de Monsieur François PELLEGRINI, commissaire rapporteur, notifié par lettre recommandée avec avis de réception à la société OUICAR le 11 mai 2017 ;

Vu la demande de huis clos de la société OUICAR du 23 mai 2017 à laquelle il n'a pas été fait droit par courrier du 6 juin 2017 ;

Vu les observations écrites de la société OUICAR reçues le 8 juin 2017, 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 22 juin 2017 qui s'est tenue publiquement :

M. François PELLEGRINI, Commissaire, en son rapport ;

Maîtres X et Y, en qualité de conseils de la société OUICAR ;

M. Z, Directeur Technique de la société ;

M. W, Directeur Opérations et Finances de la société.

Mme Nacima BELKACEM, Commissaire du Gouvernement, n'ayant pas formulé d'observations ;

Les conseils de la société OUICAR ayant eu la parole en dernier ;

A adopté la décision suivante :

Faits et procédure

La société OUICAR (ci-après la société), anciennement dénommée ZILOK AUTO, a été créée le 27 juillet 2012 et emploie 45 salariés. Son siège social est situé 9, rue du 4 septembre à Paris (75002). Elle édite le site internet www.ouicar.fr , plateforme de location de véhicules entre particuliers, qui compte [...] membres et propose entre [...] et [...] véhicules à la location sur toute la France.

En juillet 2016, l'éditeur du site www.zataz.com a informé les services de la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission) d'une violation de données à partir du site www.ouicar.fr . Il lui a ainsi

transmis deux exemples d'URL (Uniform Resource Locator) permettant d'accéder à des données à caractère personnel.

En application des décisions n° 2016-126C et n° 2016-231C de la Présidente de la CNIL du 27 juillet 2016, des délégations de la Commission ont procédé à des missions de contrôle en ligne du site www.ouicar.fr les 29 juillet 2016 et 31 janvier 2017, ainsi qu'à un contrôle sur place au sein des locaux de la société OUICAR le 3 août 2016. Les procès-verbaux de constats n° 2016-226/1, n° 2016-226/2 et n° 2016-226/3, dressés à l'issue de ces missions, ont été notifiés à la société respectivement les 1er et 5 août 2016 et le 6 février 2017.

Lors de la mission de vérification en ligne réalisée le 29 juillet 2016, la délégation de contrôle a saisi dans la barre de son navigateur l'URL https://www.ouicar.fr/api/car/search?dpt=75 .

Elle a constaté qu'aucune page web n'était affichée mais que l'adresse URL renvoyait des données au format JSON (JavaScript Object Notation), qui est un format directement lisible, correspondant à la réponse d'une interface de programmation applicative ou API (Application Programming Interface) d'un service web.

Elle a ainsi eu accès à une liste des données des véhicules proposés à la location en Ile de France par le site www.ouicar.fr , ainsi qu'aux données de leurs propriétaires et des locataires ayant déposé un ou des avis sur la prestation offerte. Les données affichées étaient structurées en plusieurs parties, dénommées de la façon suivante :

cars décrivant notamment la marque et le modèle du véhicule et indiquant le prix de mise en location ;

owner relative au propriétaire du véhicule, comportant les champs suivants : nom, prénom, adresse postale, téléphone fixe ou portable, date de naissance, numéro de permis de conduire et date d'obtention du permis ;

location reprenant les éléments permettant de localiser le véhicule : l'adresse postale, complétée par l'indication de sa longitude et de sa latitude ;

evaluations ayant trait aux commentaires laissés par des utilisateurs à la suite de la location du véhicule et comprenant les nom, prénom et identifiant de l'auteur du commentaire ;

events reprenant les données à caractère personnel du propriétaire et d'autres utilisateurs.

La délégation de contrôle a constaté qu'il était possible de consulter les données des utilisateurs pour l'ensemble des départements français, à l'exclusion de Saint-Pierre-et-Miquelon, en modifiant la variable correspondant au numéro de département dans l'URL saisie dans le navigateur. Elle a ainsi eu accès à une liste comportant les noms et prénoms de tous les propriétaires et locataires d'un véhicule proposé à la location au moment de la recherche, associés dans la plupart des hypothèses à leur adresse, numéro de téléphone fixe et/ou portable et à la localisation de leurs véhicules, soit aux données de 52 505 personnes.

Elle a, par ailleurs, constaté qu'il était également possible d'accéder aux données de n'importe quel utilisateur en indiquant cette fois comme variable l'identifiant attribué à un utilisateur donné, c'est-à-dire en saisissant une URL du type https://www.ouicar.fr/api/v1/user/get?id=347242 .

A l'issue du contrôle du 29 juillet 2016, la délégation a pris contact avec la société pour l'informer de l'existence d'une violation de données à caractère personnel sur le site.

Le 1er août 2016, la société a répondu qu'elle avait effectué des modifications significatives du code de son site web et envisageait de mettre en production une nouvelle version du site dès le lendemain soir.

Lors d'une deuxième mission de contrôle effectuée au sein des locaux de la société OUICAR le 3 août 2016, la délégation a été informée que les API à l'origine de la violation de données avaient été soit supprimées soit modifiées. La société a, en effet, supprimé les API devenues obsolètes et conservé celles nécessaires à l'affichage du site web mais en modifiant leur réponse de sorte que les données transmises soient identiques à celles affichées sur la page web et donc correspondent uniquement à celles nécessaires à la fourniture du service. Les modifications de ces API ont été effectives le 2 août 2016 à 19 heures.

Par ailleurs, en réponse à une demande de la délégation, la société a indiqué dans un courrier du 11 août 2016 qu'il n'était pas possible de déterminer avec précision la date de mise en production des API qui avaient permis d'accéder librement aux données des utilisateurs. Elle a néanmoins précisé que le site web de la société avait été créé en juillet 2012 et qu'il était établi que les API étaient déjà mises en production en novembre 2013.

[…]

Le 31 janvier 2017, la délégation a procédé à de nouvelles vérifications en ligne et a constaté que la saisie des URL litigieuses dans la barre du navigateur ne permettait plus d'accéder à des données à caractère personnel.

Aux fins d'instruction de ces éléments, la Présidente de la Commission a désigné M. PELLEGRINI en qualité de rapporteur, le 20 avril 2017, sur le fondement de l'article 46 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

A l'issue de son instruction, le rapporteur a notifié à la société OUICAR, le 11 mai 2017, un rapport détaillant le manquement à la loi Informatique et Libertés qu'il estimait constitué en l'espèce.

Ce rapport proposait à la formation restreinte de la CNIL de prononcer un avertissement public.

Etait également jointe au rapport une convocation à la séance de la formation restreinte du 22 juin 2017, indiquant à l'organisme qu'il disposait d'un délai d'un mois pour communiquer ses observations écrites.

Le 23 mai 2017, la société OUICAR a sollicité que les débats se déroulent à huis clos, ce qui a été refusé par courrier du Président de la formation restreinte du 6 juin suivant, considérant qu'aucun risque d'atteinte à l'ordre public ou à la protection de secrets protégés par la loi n'était caractérisé.

La société a produit le 8 juin 2017 des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte du 22 juin suivant.

Lors de la séance du 22 juin 2017, la société a renouvelé sa demande de huis clos, à laquelle le Président de la formation restreinte a décidé, pour les mêmes motifs, de ne pas faire droit.

Motifs de la décision

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 OUICAR a manqué à l'obligation lui incombant de mettre en œuvre des moyens propres à assurer la sécurité des données à caractère personnel contenues dans son système d'information et, en particulier, celles des utilisateurs du site www.ouicar.fr , afin notamment que ces données ne soient pas accessibles à des tiers non autorisés.

En défense, la société soutient que la violation de données résulte d'une simple erreur de code, qui est très répandue et qui n'a causé aucune atteinte à la vie privée des personnes concernées.

Elle affirme, par ailleurs, que la vérification de la violation de données par l'éditeur du site www.zataz.fr avait un caractère frauduleux dès lors que ce dernier ne bénéficie pas du statut protecteur des lanceurs d'alerte.

Elle soutient, en outre, que seule une obligation de moyens et non de résultat était à sa charge et qu'elle a déployé tous les moyens nécessaires afin d'assurer la sécurité des données des utilisateurs. Elle fait, enfin, valoir qu'elle a pris de nombreuses mesures correctives après la révélation de la violation de données.

La formation restreinte relève que le statut de l'éditeur du site www.zataz.fr est sans incidence sur la procédure qui a conduit à sa saisine, les faits et manquements reprochés se fondant sur les seules constatations effectuées par les agents de la CNIL lors des missions de contrôle. Elle note, à cet égard, que les constats de la délégation sont corroborés par la société qui ne conteste pas la survenance d'un incident de sécurité sur le site www.ouicar.fr ayant entrainé une violation de données à caractère personnel.

Tout en soulignant la bonne foi de la société OUICAR qui a réagi immédiatement après la révélation de la violation de données, la formation restreinte estime qu'elle n'avait pas pris en amont les mesures élémentaires de sécurité qui s'imposaient.

La formation restreinte considère, d'une part, que la société aurait dû mettre en place un processus d'authentification permettant de restreindre l'accès aux résultats affichés par les API. Cette simple mesure aurait permis d'empêcher que tout internaute puisse interroger et consulter librement les réponses de ces dernières. D'autre part, la formation restreinte relève que la violation de données aurait pu être réduite si la société avait veillé à n'intégrer dans les réponses des API que les seules données strictement nécessaires à l'affichage de son site web. Elle note que cette mesure de sécurité aurait notamment permis de ne révéler que la première lettre du nom patronymique des utilisateurs et non l'intégralité de ce dernier.

La formation restreinte relève, de surcroît, que cet incident de sécurité a été d'une particulière ampleur en raison du nombre de personnes impactées et de la multitude des catégories de données concernées. Elle rappelle, en effet, que la saisie des URL litigieuses permettaient d'accéder aux données de l'ensemble des utilisateurs du site, soit plus de […] personnes, et d'obtenir ainsi des renseignements particulièrement précis sur ces derniers tels que leurs nom, prénom, date de naissance, date de délivrance et numéro de permis de conduire, adresse postale, coordonnées téléphoniques et données de localisation des véhicules mis en location.

La formation restreinte considère, par ailleurs, que la gravité de cette fuite de données a été accentuée par sa durée. Elle rappelle que les données à caractère personnel sont restées librement accessibles pendant près de trois ans puisque les API se trouvant à l'origine de la violation de données ont été mises en production entre juillet 2012 et novembre 2013. La résolution de la violation de données date, quant à elle, d'août 2016.

Par conséquent, la formation restreinte considère que la société n'a pas pris toutes les précautions utiles afin d'empêcher que des tiers non autorisés aient accès aux données traitées.

Sur la sanction et la publicité

Au regard des éléments développés ci-dessus, les faits constatés constituent un manquement aux dispositions de l'article 34 de la loi du 6 janvier 1978 modifiée.

La formation restreinte considère que la gravité de la fuite de données justifie que soit prononcé à l'encontre de la société OUICAR un avertissement, eu égard au volume important de personnes concernées, à savoir plus de […] personnes, à l'étendue des données à caractère personnel rendues accessibles et à la durée de la violation.

Ces mêmes circonstances conduisent la formation restreinte à rendre publique sa décision.

PAR CES MOTIFS

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

de prononcer un avertissement à l'encontre de la société OUICAR ;

de rendre publique sa délibération, 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.

Nature de la délibération: SANCTION
Date de la publication sur legifrance: 26 juillet 2017