COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES

Délibération n°2016-108 du 21 avril 2016

Délibération de la formation restreinte n° 2016-108 du 21 avril 2016 prononçant un avertissement à l'encontre de la société RICARD

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 Marie-Hélène MITJAVILE, Mme Dominique CASTERA, 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 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 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 ;

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° 2015-200C du 8 juillet 2015 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 tous les traitements relatifs au site RICARD.COM ;

Vu la décision de la Présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur, en date du 8 janvier 2016 ;

Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, adressé à la société RICARD le 12 janvier 2016 ;

Vu la demande de huis clos présentée par la société RICARD le 25 janvier 2016 à laquelle il a été fait droit par courrier du 4 février 2016 ;

Vu les observations écrites versées par la société RICARD le 19 février 2016 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 25 février 2016 :

- Monsieur François PELLEGRINI, commissaire, entendu en son rapport ;
- En qualité de représentants de la société RICARD :

-En qualité de conseil de la société RICARD :

Madame Catherine POZZO DI BORGO, commissaire du Gouvernement adjoint, n'ayant pas formulé d'observation ;

Les représentants de la société RICARD ayant eu la parole en dernier ;

Après en avoir délibéré, a adopté la décision suivante :

I. Faits et procédure

La société RICARD (ci-après la société), dont le siège social est situé 4/6 rue Berthelot à Marseille (13014) emploie environ 800 salariés. En 2014, elle présentait un chiffre d'affaires d'environ 500.000.000 € pour un résultat net de près de 52.000.000 €.

La société a pour activité la production de boissons alcooliques distillées et édite le site www.ricard.com destiné à gérer les inscriptions au programme fidélité Place Ricard et l'envoi d'objets promotionnels aux personnes inscrites.

Le 8 juillet 2015, la Présidente de la Commission nationale de l'informatique et des libertés (ci-après CNIL ou la Commission) a ordonné une mission de vérification de tous les traitements liés au site www.ricard.com afin d'en vérifier la conformité à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après Informatique et Libertés).

À l'occasion des constatations en ligne effectuées le 9 juillet 2015, la délégation de contrôle a notamment consulté les informations contenues dans le fichier robots.txt du site web.

Ce fichier texte indique aux robots d'indexation des moteurs de recherche, les pages du site à exclure de l'indexation à laquelle ils procèdent sur Internet.

Il ressort des éléments du dossier qu'en saisissant dans l'URL du navigateur, à la suite de l'adresse du site de la société, le nom des répertoires listés dans le fichier robots.txt , la délégation est parvenue à accéder à des ressources exclues de l'indexation mais dont l'accès n'était pas restreint par des mesures de sécurité particulières.

En naviguant parmi ces ressources, elle a été en mesure de télécharger, à partir des répertoires auxquels elle a eu accès, plus de 1.000 fichiers contenant les données à caractère personnel suivantes : nom, prénom, date de naissance, adresse postale, adresse électronique, numéro de téléphone, ainsi que des informations relatives à des paiements (date, montant et statut de la transaction, moyen de paiement utilisé, adresse électronique associée).

À l'issue de ces vérifications, la société a été informée de la fuite de données constatée et le procès-verbal de contrôle n° 2015-200 lui a été notifié. La société a immédiatement indiqué avoir pris les mesures nécessaires, par l'intermédiaire de son hébergeur, pour bloquer l'accès aux données recueillies via son site web, ce qu'elle a confirmé par courrier du 23 juillet 2015.

À l'occasion d'un second contrôle daté du 27 novembre 2015, il a été constaté qu'il n'était plus possible d'afficher le contenu des répertoires litigieux.

Toutefois, la délégation est parvenue à consulter les fichiers contenant les données nominatives en recomposant l'URL d'accès direct dont elle avait eu connaissance lors du précédent contrôle.

À l'occasion de ces nouvelles vérifications, elle a constaté qu'étaient également accessibles des données relatives aux cartes bancaires des internautes (numéro tronqué de la carte bancaire et date de validité).

Le procès-verbal n° 2015-200/2 lui a été notifié par courrier du 4 décembre 2015.

Par courrier du 16 décembre 2015, la société a indiqué avoir averti son prestataire de la persistance de la fuite de données et adopté les correctifs nécessaires afin que les données des internautes inscrits au programme de fidélité Place Ricard et ayant commandé des objets promotionnels de la marque depuis son site ne soient plus accessibles en ligne.

Au vu des constats opérés révélant des défaillances en termes de sécurité et de confidentialité des données à caractère personnel collectées par la société via son site www.ricard.com , la Présidente de la Commission a décidé, le 8 janvier 2016, sur le fondement de l'article 46 de la loi Informatique et Libertés, d'engager une procédure de sanction en désignant M. François PELLEGRINI en qualité de rapporteur.

À l'issue de son instruction, celui-ci a notifié à la société, le 12 janvier 2016, un rapport détaillant le manquement à la législation précitée qu'il estimait constitué et sollicitant le prononcé d'un avertissement public.

Était également jointe au rapport une convocation à la séance de la formation restreinte du 25 février 2016 indiquant à la société qu'elle disposait d'un délai d'un mois pour communiquer ses observations écrites.

La société a produit, le 19 février 2016, des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte du 25 février 2016, laquelle s'est déroulée à huis clos sur demande de la société.

II. Motifs de la décision

Sur l'existence d'un manquement à l'obligation de veiller à la sécurité et la confidentialité des données à caractère personnel

Il est reproché à la société d'avoir manqué à son obligation de préserver la sécurité et la confidentialité des données à caractère personnel des internautes dont les données sont collectées via son site www.ricard.com , en violation de l'article 34 de la loi Informatique et Libertés qui dispose : 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 .

Dans ses observations écrites, la société reconnaît la fuite de données mais conteste avoir manqué à l'obligation précitée.

Elle soutient avoir satisfait à son obligation de moyens en ayant eu recours à des professionnels reconnus dans ce secteur, tant pour l'hébergement de son site web que pour la gestion de son contenu.

Sur ce point, la formation restreinte rappelle qu'en vertu de l'article 35 de la loi Informatique et Libertés, l'existence d'une relation de sous-traitance n'est pas de nature à exonérer le responsable de traitement de ses obligations au regard des données collectées et traitées pour son compte.

La société précise également que les manœuvres utilisées par la délégation de contrôle pour accéder aux données lors des deux missions de vérifications étaient particulièrement complexes de sorte que celles-ci n'étaient pas librement accessibles du public.

En l'espèce, la formation restreinte retient que le manquement est caractérisé par le fait qu'aucune mesure de protection particulière n'encadrait l'accès aux données.

En effet, il ressort des éléments du dossier que celles-ci ont pu être consultées sans restriction sur la base d'informations contenues dans le fichier robots.txt accessible à la racine du site web de la société.

C'est en saisissant dans l'URL du navigateur les noms des répertoires contenus dans le fichier robots.txt , à la suite de l'adresse du site de la société, qu'il a été possible à la délégation d'accéder aux données à caractère personnel de plusieurs milliers de clients de la société.

De plus, si à la suite de cette première alerte la société a renforcé la sécurité des données en empêchant l'accès aux répertoires litigieux, il n'est pas contesté que l'accès direct aux fichiers était toujours autorisé (en renseignant l'URL recherchée dans le navigateur).

La formation restreinte considère, ainsi, que la société n'avait pas pris toute mesure utile de nature à garantir la sécurité et la confidentialité des données collectées.

La société soutient également qu'aucun préjudice n'a été subi par les personnes impactées par la fuite de données. Or, cette circonstance est sans influence sur la caractérisation du manquement qui est constitué par l'absence de mise en œuvre de mesures visant à empêcher l'accès aux données par des tiers non autorisés. L'établissement du manquement n'est donc pas subordonné à la démonstration d'un tel accès par des tiers ou à l'existence d'un préjudice pour les personnes concernées.

Enfin, la société a présenté les mesures mises en œuvre à la suite du second contrôle afin de renforcer la sécurité des données identifiantes qu'elle collecte et a indiqué être en cours de déploiement d'un nouveau site web doté de mesures de sécurité conformes à l'état de l'art.

La formation restreinte prend acte de ces engagements destinés, à l'avenir, à sécuriser les données à caractère personnel des clients de la société mais considère que le manquement à l'article 34 précité n'en demeure pas moins caractérisé.

III. Sur la sanction et la publicité

Au vu des éléments qui précèdent, la formation restreinte décide de prononcer à l'encontre de la société RICARD, en application de l'article 45 de la loi du 6 janvier 1978 modifiée, un avertissement qui sera rendu public.

Cette sanction est justifiée par le nombre et la nature des données concernées par la faille de sécurité, par la nécessité de sensibiliser les responsables de traitement à leurs obligations en matière de confidentialité des données à caractère personnel collectées et par la persistance du manquement malgré l'alerte de la Commission.

PAR CES MOTIFS

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

- de prononcer un avertissement ;
- de rendre publique sa délibération.

Le Président

Jean-François CARREZ