Chez Ricard, les données personnelles étaient en open bar

La CNIL pointe du doigt des failles dans la sécurisation du site de Ricard. La société française de boissons anisées, qui fait partie du groupe français Pernod Ricard, reçoit un avertissement public de la Commission nationale de l'informatique et des libertés pour un défaut de sécurisation des données personnelles recueillies via son site Web. Sur ce dernier, la société propose l'adhésion à un programme de fidélité et la commande d'objets promotionnels de la marque.

Or, un contrôle en ligne effectué par la CNIL, en juillet dernier, a permis de montrer que la sécurisation des données ainsi recueillies était par trop insuffisante. Les experts de la Commission sont parvenus à accéder à « *plusieurs milliers de données* » : des noms, prénoms, dates de naissance, adresses postales et électroniques, numéros de téléphones et informations relatives à des cartes bancaires (dates, montants et statuts des transactions, moyen de paiement employé, e-mail associé).

Exploiter le fichier « robots.txt » de Ricard

Pour accéder à ces données personnelles, les inspecteurs de la CNIL n'ont pas eu besoin d'exploiter une faille connue que les équipes de Ricard auraient oublié de patcher. En effet, certains répertoires « *ne faisaient pas l'objet de mesure de sécurité particulière permettant d'en restreindre l'accès alors qu'ils contenaient de nombreuses données personnelles* », souligne la CNIL. Pour accéder à ces répertoires, cette dernière a simplement consulté le fichier « robots.txt » du site Web, fichier indiquant aux moteurs de recherche les pages à exclure de leur indexation. C'est en explorant ces URL que les inspecteurs de la Commission ont déniché, dans des répertoires, plus de 1 000 fichiers renfermant des données personnelles.

Informée, « *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* », écrit la CNIL. Sauf que les mesures en question se sont révélées insuffisantes. Lors d'un second contrôle en novembre dernier, les inspecteurs de la CNIL ont certes constaté que les répertoires litigieux n'étaient plus accessibles, mais les fichiers renfermant les données personnelles eux le demeuraient (pour peu qu'on en connaisse l'URL). Ces nouvelles vérifications ont aussi permis de constater que des données sensibles relatives aux cartes bancaires des clients de l'apéritif anisé étaient aussi accessibles (numéros tronqués des cartes et dates de validité). Ricard s'est alors de nouveau tourné vers son prestataire pour corriger ces erreurs.

Externaliser ne suffit pas à se dédouaner

Ces manquements valent à la société française, qui réalise environ 500 millions d'euros de chiffre d'affaires et emploie 800 personnes, un avertissement public, la CNIL rejetant les arguments de Ricard qui estimait avoir respecté son obligation de moyens en ayant fait appel à des professionnels reconnus tant pour l'hébergement que pour la gestion des contenus. « *La formation*

restreinte (de la CNIL, NDLR) 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 », écrit la Commission dans sa délibération. La société échappe toutefois à une sanction financière.

A lire aussi :

Protection des données : la Cnil tape sur les doigts de Numericable

Loi Lemaire : la CNIL va-t-elle pouvoir montrer les crocs ?

Données de santé : la Cour des comptes pointe la frilosité de la CNIL