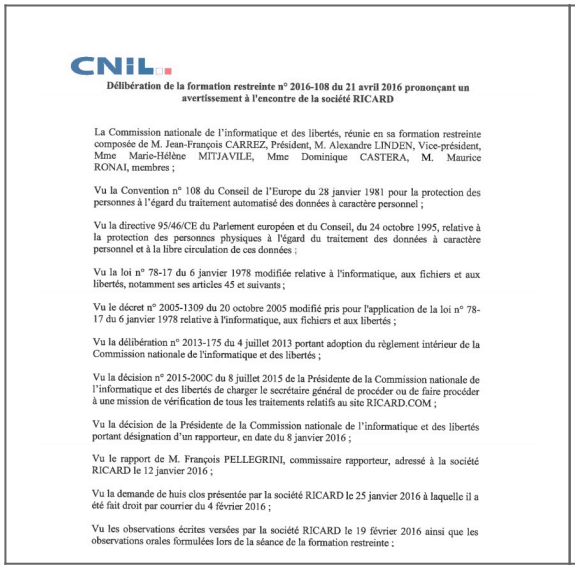
La CNIL inflige une sanction à Ricard pour défaut de sécurité – Le Monde Informatique



CNIL

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 ;

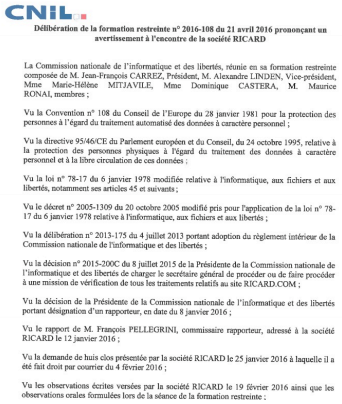
Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, adressé à la société RICARD le 12 janvier 2016 ;

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 ;

La CNIL inflige une sanction à Ricard pour défaut de sécurité

La CNIL vient de publier un avertissement public contre Ricard pour défaut de sécurisation des données d'un programme de fidélité accessible sur le web.



CNIL.

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 MITTAVILLE, 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 ;

Voilà une publicité dont Ricard se serait bien passé mais la sanction est cependant bien légère. La CNIL vient en effet de sanctionner le distributeur de produits alcoolisés pour un programme de fidélité présenté sur son site web. Les données personnelles des membres de ce programme n'étaient en effet pas protégées. L'autorité administrative indépendante, constatant l'absence de préjudice réel et la correction du problème, n'a cependant pas sanctionné très durement l'entreprise puisqu'elle lui a juste infligé un avertissement public par une décision du 21 avril 2016 publiée le 24 mai.

Concrètement, les données personnelles (noms, prénoms, dates de naissance, moyens de paiements, achats opérés, adresses électroniques, téléphones…) étaient stockées dans un répertoire du site web qui n'était ni bloqué en accès (par un *.htaccess* par exemple) ni crypté. La seule précaution prise était une demande de désindexation du répertoire dans les moteurs de recherche via une instruction dans le *robot.txt*. Donc, une simple lecture du*robot.txt*, par nature en clair, permettait de savoir où chercher des informations intéressantes…

Incompétence du prestataire, indifférence du responsable de traitement

Après un premier contrôle opéré le 8 juillet 2015, la CNIL prévient Ricard du problème. La société déclare avoir effectué le nécessaire en le commandant à son prestataire, information confirmée par un courrier du 23 juillet. Or, le 27 novembre 2015, un nouveau contrôle aboutit au constat que, certes, l'affichage du contenu du répertoire indiqué dans le*robot.txt* n'est plus possible mais l'accès en lecture aux URL directes des fichiers l'est toujours ! Un nouveau procès-verbal d'infraction lui est donc adressé le 4 décembre 2015, notification à l'origine de la procédure dont nous parlons ici. Le site web a finalement été refondu pour être à l'état de l'art en matière de sécurité.

Cette affaire est l'occasion de plusieurs rappels intéressants. Tout d'abord, pour la CNIL, le seul et unique responsable est et demeure l'entreprise qui ordonne la création et maîtrise le traitement de données. Cette entreprise ne peut en aucun cas se défausser sur un prestataire. C'est au commanditaire de bien vérifier la mise en place des mesures obligatoires. Mais, et c'est induit, le commanditaire, responsable du traitement, doit effectivement commander et vérifier la mise en place des telles mesures.

Une mise en cause du prestataire délicate

La délibération de la CNIL ne mentionne pas le sous-traitant en cause. Une porte-parole de la CNIL précise : « pour l'instant, le seul responsable pour nous est Ricard en tant que responsable du traitement même si, avec le nouveau Règlement Européen, la place du prestataire va évoluer. » Le groupe Pernod-Ricard, sollicité par la rédaction, n'a pas encore officialisé une réaction ni précisé quel était le prestataire en cause.

Cela dit, dans l'absolu, le prestataire pourrait être poursuivi civilement par Ricard. Le producteur de pastis pourrait lui demander une indemnisation pour le préjudice subi de son fait, notamment le préjudice d'image.

Mais encore faudrait-il que la faute puisse être caractérisée et prouvée. En effet, les attentes en matière de sécurité doivent être spécifiées contractuellement pour qu'un manquement soit caractérisé. Et les instructions du commanditaire, Ricard en l'occurrence, ne doivent pas être contraires directement ou indirectement aux bonnes pratiques. En général, ce genre d'affaires se règle discrètement dans les bureaux des entreprises concernées et il est peu probable que le résultat de ces palabres ne soit un jour connu.

MISE À JOUR : COMMUNIQUÉ DE RICARD

En réponse à notre sollicitation, Ricard nous a fait parvenir un communiqué laconique, sans citer le prestataire mis en cause, mais insistant sur les limites du manquement relevé par la CNIL. « Suite à la délibération de la CNIL du 21 avril 2016 prononçant un avertissement à l'encontre de la société Ricard pour son site internet Ricard.com, la société Ricard prend acte de cette décision et précise, comme le rappelle la CNIL, que la faille de sécurité identifiée a été corrigée sur le site existant. La société Ricard entend préciser que les données étaient exclues d'une indexation sur Internet et n'ont donc jamais été accessibles par des moteurs de recherche. La société Ricard confirme en outre avoir développé un nouveau site Ricard.com qui sera mis en ligne début juin et qui répond également aux normes de sécurité ».

Article de Bertrand Lemaire

Réagissez à cet article

Source : *La CNIL inflige une sanction à Ricard pour défaut de sécurité – Le Monde Informatique*