Le mot de passe insuffisant : une violation de l'art. 32 RGPD

Célian Hirsch, le 21 septembre 2020

Une société dont le site Internet exige un mot de passe composé d'au moins six caractères sans nécessairement contenir plusieurs types de caractère viole l'art. 32 RGPD.

Délibération de la CNIL n°SAN-2020–003 du 28 juillet 2020 concernant la société SPARTOO SAS

L'autorité française compétente en matière de protection des données (la Commission nationale de l'informatique et des libertés (CNIL)) a rendu Le 28 juillet 2020 une délibération concernant la société SPARTOO SAS, à qui elle reprochait diverses violations du RGPD. Le présent commentaire se concentre sur le manquement à l'obligation d'assurer la sécurité des données (art. 32 RGPD).

La société SPARTOO SAS est une société spécialisée dans la vente à distance de chaussures. Afin d'exercer ses activités, la société dispose de seize sites Internet dans treize pays de l'Union européenne. Lorsqu'un utilisateur désire créer un compte sur l'un de ces sites, il doit indiquer un mot de passe composé d'au moins six caractères sans nécessairement contenir plusieurs types de caractère.

Par ailleurs, afin de lutter contre les fraudes, la société demande à ses clients de lui envoyer une copie du recto de leur carte bancaire lorsque le protocole 3DSecure n'est pas validé. Elle a ainsi reçu par courriel non chiffré des photographies et scan de clients contenant l'intégralité des numéros de leur carte bancaire. La société a également conservé ces données en clair dans sa base de données pendant six mois.

L'art. 32 al. 1 du Règlement général européen sur la protection des données prévoit notamment ce qui suit :

> « Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les

> mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ».

Concernant les mots de passe, la société soutient devant la CNIL qu'elle a préféré opter pour l'imposition de mots de passe courts et plus simples, lesquels seraient moins prévisibles pour un éventuel attaquant.

La CNIL souligne d'emblée ce qui suit :

> « la longueur et la complexité d'un mot de passe demeurent des critères élémentaires permettant d'apprécier la force de celui-ci. (…) [P]our assurer un niveau de sécurité suffisant et satisfaire aux exigences de robustesse des mots de passe, lorsqu'une authentification repose uniquement sur un identifiant et un mot de passe, le mot de passe doit comporter au minimum douze caractères – contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial – ou le mot de passe doit comporter au moins huit caractères – contenant trois de ces quatre catégories de caractères – et être accompagné d'une mesure complémentaire comme par exemple la temporisation d'accès au compte après plusieurs échecs (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (ex : captcha) et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses ».

Or, en l'espèce, le fait d'accepter un mot de passe composé uniquement de six caractères et d'une seule catégorie de caractère ne correspond pas aux exigences requises susmentionnées en matière de sécurité. Partant, la société a violé l'art. 32 RGPD.

Concernant les données bancaires, la CNIL constate que la société n'a mis en place aucune mesure apte à garantir la sécurité de ces données. Au contraire, elle a reçu l'intégralité des numéros des cartes, alors qu'elle aurait dû en demander qu'une partie tronquée afin de lutter contre les fraudes. Par ailleurs, elle a reçu ces données bancaires en clair et par courriel non chiffré. Enfin, elle les a conservées pendant six mois en clair. Partant, la CNIL considère que la société a également violé l'art. 32 RGPD en ne mettant pas en place des mesures de sécurité permettant de garantir la sécurité des données bancaires de ses clients.

En droit suisse, l'art. 7 al. 1 LPD ancre dans la loi le principe de de la sécurité des données :

> « Les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées ».

Dans son Guide relatif aux mesures techniques et organisationnelles de la protection des données, le Préposé fédéral à la protection des données et à la transparence se prononce sur les exigences de robustesse des mots de passe que sous l'angle de l'accès aux données par des employés au sein de l'entreprise. Il précise que le mot de passe doit être fort, c'est-à-dire qu'il doit contenir au minimum 8 caractères dont des lettres (majuscules et minuscules), des chiffres et des caractères spéciaux. À notre connaissance, le Préposé ne se prononce toutefois pas sur les exigences de robustesse des mots de passe créés par des utilisateurs sur un site Internet. Vu l'absence de recommandation helvétique en la matière, les sociétés suisses pourraient, à notre avis, s'inspirer notamment des Recommandations de sécurité relatives aux mots de passe émises par l'Agence nationale de la sécurité des systèmes d'information française afin de respecter l'art. 7 LPD.

Notons enfin qu'un manquement, sans motif justificatif, à l'art. 7 LPD constitue un acte illicite qu'un lésé peut invoquer afin de demander des dommages-intérêts. A notre avis, une personne qui verrait son compte piraté, en raison de l'absence d'exigence d'un mot de passe suffisamment robuste, pourrait néanmoins se voir imposer, selon les circonstances, une réduction de l'indemnité demandée en raison d'une faute concomitante de sa part (art. 44 CO).

Désormais, les sociétés seraient ainsi bien avisées de suivre les exigences préconisées par la CNIL en matière de robustesse des mots de passe.

Proposition de citation : Célian Hirsch, Le mot de passe insuffisant : une violation de l'art. 32 RGPD, 21 septembre 2020 *in* www.swissprivacy.law/3