Deux courriels au mauvais destinataire peuvent coûter cher

Célian Hirsch, le 21 octobre 2021

L'envoi d'un courriel à un mauvais destinataire constitue une violation de la sécurité des données s'il contient des données personnelles. Lorsque ces données sont sensibles, on retiendra plus facilement un risque élevé pour la personne concernée par la violation de confidentialité. Il en découle un devoir d'informer l'autorité, voire la personne concernée, selon le RGPD.

Délibération de la Commission nationale pour la protection des données n° 31FR/2021 du 5 août 2021

Envoyer un courriel professionnel au mauvais destinataire par mégarde ne semble pas si grave. Cela étant, si ce le courriel contient des données sensibles, et que l'erreur se produit deux fois dans un court laps de temps, les conséquences financières peuvent être importantes et atteindre tout de même EUR 135'000.-. Une société d'assurance en a récemment fait les frais.

En novembre 2018, une employée d'une société d'assurance luxembourgeoise envoie par inadvertance un courriel à un mauvais destinataire. Le courriel contient notamment le nom de famille de l'assuré, son sexe, ainsi que des indications détaillées quant à certaines pathologies. L'assuré est informé de cette erreur vingt jours plus tard.

Vingt jours plus tard, la même employée réitère son erreur. Le courriel comprend cette fois-ci notamment le nom de famille de l'assuré, des questions très précises quant à une pathologie spécifique et le nom de famille du docteur de l'assurance-vie. L'assurance informe l'assuré de cette inadvertance quelques jours plus tard. Elle lui assure que « toutes les mesures seront prises pour éviter de tels incidents dans le futur ».

Peu rassuré, et probablement contrarié par cette double erreur, l'assuré saisit la Commission nationale pour la protection des données luxembourgeoise (CNPD). Celle-ci décide d'ouvrir une enquête et effectue une visite dans les locaux de la société.

En premier lieu, la Commission constate que le registre des violations de données à caractère personnel ne contient aucune inscription. Or l'art. 33 par. 5 RGPD impose au responsable du

traitement de documenter toute violation. L'art. 33 par. 5 *in fine* RGPD précise que la documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect de cette disposition.

L'assurance admet les faits reprochés, mais soutient que la combinaison des données divulguées (nom de famille et conditions de santé) ne permettrait pas d'identifier directement ou indirectement l'assuré. Elle aurait d'ailleurs procédé à une recherche sur internet qui n'aurait affiché aucun lien à l'assuré. Les informations dans les deux courriels ne contiendraient ainsi aucune donnée personnelle. Partant, les obligations découlant du RGPD ne trouveraient pas application.

Après avoir rappelé la notion large de données personnelles, la CNPD considère que les données contenues dans les deux courriels permettent d'identifier l'assuré, du moins indirectement. Or l'envoi de courriels à un destinataire erroné constitue une violation de données à caractère personnel au sens de l'art. 4 ch. 12 RGPD (violation de la confidentialité). Partant, l'assurance aurait dû documenter dans son registre interne un tel événement.

Dans un deuxième temps, la Commission examine si elle devait être notifiée de cette violation de données à caractère personnel.

L'art. 33 par. 1 RGPD impose au responsable du traitement de notifier l'autorité compétente de toute violation de données à caractère personnel, à moins que la violation ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.

L'art. 34 par. 1 RGPD impose par ailleurs au responsable du traitement d'informer sans délai la personne concernée de la violation de données à caractère personnel lorsqu'elle est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne concernée.

La CNPD souligne d'emblée que les données en question constituent des données de santé. Elles sont ainsi dites « sensibles ». La Commission considère qu'en raison de ce « caractère hautement sensible », les dommages potentiels pour l'assuré sont particulièrement graves, car la violation pourrait entraîner des dommages matériels ou moraux « si, par exemple, ces informations seraient publiées ou seraient transmises à d'autres tiers, voire à son employeur ».

Par ailleurs, ces données sont également protégées tant par le secret médical que par le secret professionnel. La CNPD en déduit une « obligation renforcée du respect de la confidentialité » en raison du caractère « très sensible » des données. En outre, l'assurance n'a pas

prouvé avoir demandé aux destinataires non autorisés de supprimer les courriels reçus par erreur.

Partant, la violation de données à caractère personnel aurait dû être notifiée tant à la CNPD qu'à l'assuré.

L'assurance souligne qu'elle a précisément informé l'assuré de ces erreurs. Cela étant, la Commission lui rétorque que non seulement cela n'a pas été effectué sans délai, mais qu'en plus elle n'a pas fourni à l'assuré les informations qu'elle aurait dû lui fournir selon l'art. 34 par. 2 RGPD.

Troisièmement, la CNPD examine si le responsable du traitement avait mis en place des mesures techniques et organisationnelles appropriées selon le risque, au sens de l'art. 32 RGPD.

Elle constate que l'assuré avait consenti à ce que l'assurance lui envoie des données par courriel. Cela étant, un tel consentement n'exonère pas le responsable du traitement d'adopter des mesures de sécurité appropriées, en particulier lorsqu'il s'agit de données sensibles.

Selon la Commission, l'assurance aurait dû chiffrer les communications ou adopter une technique semblable. Or aucune mesure technique de protection ne protégeait l'envoi des courriels litigieux. Partant, l'assurance a violé le principe de sécurité des données.

Enfin, la CNPD se penche sur les mesures correctrices (art. 58 RGPD) et le montant de l'amende (art. 83 RGPD) en raison de ces multiples manquements.

En particulier, la société traite à grande échelle des données sensibles protégées également par le secret médical. Elle est ainsi tenue à une obligation renforcée du respect de la confidentialité. Or, non seulement elle n'a pas adopté les mesures de sécurité nécessaires, mais en plus elle a procédé à une interprétation erronée d'une notion de base de protection des données en affirmant que les courriels ne contenaient en l'espèce pas des données personnelles.

En outre, la CNPD souligne qu'en raison de cette erreur d'interprétation, il y a un risque que beaucoup d'autres cas de violation de données à caractère personnel n'aient pas été détectés par l'assurance. Ainsi, le nombre de personnes potentiellement concernées est élevé.

En raison de ces éléments, la Commission fixe l'amende à EUR 135'000.- et impose

à l'assurance de protéger l'envoi de courriels contenant des données sensibles, par exemple à l'aide d'un chiffrement par cryptage ou par des mots de passe.

Cette décision devrait rappeler à tout responsable du traitement qu'une petite erreur, sans réaliser les conséquences juridiques qui en découlent, peut coûter particulièrement cher. La personne concernée déçue par l'absence de sécurité adéquate des données n'hésitera d'ailleurs probablement pas, comme dans le cas d'espèce, à dénoncer le responsable du traitement à l'autorité compétente.

On peut toutefois s'étonner que la décision ne mentionne que de potentiels dommages pour la personne concernée, sans retenir une quelconque conséquence concrète. La CNPD adopte cette même approche abstraite en considérant qu'il y a potentiellement d'autres personnes concernées par le même genre de violation de la sécurité des données. Pour le juriste suisse, cette approche abstraite semble assez inhabituelle.

Les responsables du traitement suisses peuvent être d'une part rassurés, de l'autre également inquiets. En effet, bien que le droit suisse (actuel et futur) ne prévoie pas d'amende administrative en cas de violation des normes de la protection des données, le RGPD déploie des effets extraterritoriaux potentiellement applicables en Suisse (cf. swissprivacy.law/22/). Il n'est toutefois pas clair si des amendes prononcées dans l'Union européenne à l'encontre de sociétés suisses peuvent être exécutables dans le territoire helvétique (cf. not. Benhamou Yaniv, Jacot-Guillarmod Emilie. RGPD sur sol suisse : mise en œuvre, digma, 2018 p. 142–149).

Proposition de citation : Célian Hirsch, Deux courriels au mauvais destinataire peuvent coûter cher, 21 octobre 2021 *in* www.swissprivacy.law/96