Les données de douze millions de consommateurs en libre accès

Célian Hirsch, le 31 janvier 2022

Laisser en libre accès sur Internet les données de douze millions de personnes constitue une violation de la sécurité des données (art. 32 RGPD), même s'il n'est pas avéré qu'un accès mal intentionné à ces données a eu lieu.

Délibération de la Commission nationale de l'informatique et des libertés n°SAN-2021–020 du 28 décembre 2021 concernant la société SLIMPAY

Lorsque vous procédez à un paiement en ligne, une société de paiement s'interpose souvent, mais discrètement, entre vous et le commerçant. SlimPay est l'une de ces sociétés, sise en France. Elle traite ainsi les données de consommateurs pour les commerçants en ligne. Malheureusement pour ces consommateurs, la société française a commis une petite erreur de sécurité des données, ce qui lui a valu une amende la Commission nationale de l'informatique et des libertés (CNIL, autorité française de protection des données).

En 2015, SlimPay décide de réutiliser les données de douze millions de consommateurs dans le cadre d'un projet de recherche interne sur un mécanisme de lutte contre la fraude. Ces données comprennent les informations relatives à l'état civil (civilité, nom, prénom), aux coordonnées postales, électroniques et téléphoniques, et aux informations bancaires (BIC/IBAN). Cela étant, à la fin du projet en juillet 2016, les données restent sur un serveur qui est librement accessible depuis Internet.

Ce n'est qu'en février 2020 qu'un commerçant lui fait remarquer ce « petit » problème. En raison de l'obligation légale d'annoncer les violations de la sécurité (art. 33 RGPD), la société de paiement notifie la violation de données à la CNIL, qui ouvre une procédure pour violation du RGPD (délibération SAN-2021–020 du 28 décembre 2021).

Contrat de sous-traitance (art. 28 RGPD)

Grâce à la notification, la CNIL découvre d'autres manquements au RGPD. En particulier, l'autorité française souligne ce qui suit :

> « le fait que les investigations de la CNIL aient été initialement motivées par la surve-

> nance de la violation de données, à la suite de sa notification, est sans incidence sur la possibilité de constater l'existence d'autres manquements au RGPD au regard des faits constatés dans le cadre des investigations menées par la délégation de contrôle de la CNIL ».

L'autorité française retient une violation de l'obligation de prévoir contractuellement diverses obligations à la charge du sous-traitant (art. 28 par. 3 RGPD). En effet, certains contrats ne contenaient pas toutes les clauses prévues par l'art. 28 par. 3 RGPD. Trois autres contrats ne comportaient même aucune des mentions obligatoires prévues par cet article.

Dans sa défense, SlimPay soutient que des négociations sont en cours afin de modifier ces contrats. La CNIL lui rétorque laconiquement que :

> « le fait que la société ait entamé des démarches auprès des sous-traitants dans le cadre de la présente procédure démontre bien qu'elle n'était pas en conformité au moment des investigations menées par la CNIL ».

Sécurité des données (art. 32 RGPD)

Au regard de la sécurité des données, l'art. 32 RGPD impose au responsable du traitement de mettre en œuvre les mesures techniques et organisationnelles appropriées au risque.

En l'espèce, les données étaient accessibles depuis Internet, sans autre restriction d'accès ou mesure de sécurité. Il suffisait de disposer de l'adresse IP du serveur pour y accéder.

La société de paiement invoque que l'obligation de sécurité est une obligation de moyens, et non de résultat. Elle souligne que l'absence de sécurité était due à une négligence humaine. Enfin, l'adresse IP du serveur n'était pas référencée sur un moteur de recherche.

La CNIL lui répond que l'adresse IP était facilement identifiable à l'aide de programmes de balayage de ports. Or ces programmes sont disponibles sur le web et souvent utilisés par les attaquants afin de détecter des serveurs non ou mal sécurisés.

En outre, SlimPay n'avait adopté aucune mesure de journalisation des accès au serveur (*logs*). Or une telle mesure aurait permis de détecter les actions effectuées sur le serveur. Elle est d'ailleurs considérée comme « indispensable à la gestion de la sécurité des systèmes

d'information » par l'Agence nationale de la sécurité des systèmes d'information.

SlimPay soutient que cet éventuel manquement n'aurait causé aucun préjudice. En effet, un audit serait arrivé à la conclusion que les données n'ont pas été exploitées par un attaquant.

La CNIL n'est pas convaincue par cette approche. Il s'agit en l'espèce de données de plus de 12 millions d'Européens. Or la violation de l'art. 32 RGPD ne dépend pas d'un résultat, mais de l'existence d'un risque. Ce risque était, *in casu*, bien réel. En raison de leur nature, ces données librement accessibles ont créé un risque d'hameçonnage et d'usurpation d'identité pour les personnes concernées.

Communication à la personne concernée d'une violation de données (art. 34 RGPD)

Après avoir constaté une violation de la sécurité des données, la CNIL se penche dans un troisième temps sur l'obligation de communiquer aux personnes concernées la violation de données.

L'art. 34 par. 1 RGPD impose au responsable du traitement de communiquer la violation de données à caractère personnel à la personne concernée dans les meilleurs délais lorsque la violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées par la violation.

La CNIL balaie tout d'abord l'argument de SlimPay selon lequel le risque n'était pas élevé. En effet, en raison de sa nature, du volume, de la facilité d'identification et des conséquences possibles, le risque lié à la violation des données doit être considéré élevé.

Selon l'art. 34 par. 3 let. c RGPD, le responsable du traitement peut renoncer à informer les personnes concernées de la violation de données si la communication exige « des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ».

Dans sa défense, SlimPay invoque encore le fait qu'elle n'a pas l'intégralité des adresses électroniques des personnes concernées. En outre, une communication publique sur son site web n'aurait pas été pertinente puisque les personnes concernées ne savent pas si elles ont utilisé SlimPay.

Premièrement, la CNIL souligne que la société de paiement dispose tout de même de la moitié des adresses électroniques des personnes concernées. Elle aurait ainsi pu, à tout le moins, contacter ces personnes.

Deuxièmement, la communication publique aurait pu être reprise par des journaux ainsi que dans les réseaux sociaux et, ainsi, atteindre les personnes concernées. Le site web de SlimPay aurait ainsi été seulement le point de départ de cette communication publique, laquelle aurait ensuite gagné en importance.

Grâce à une communication publique, les personnes qui auraient voulu savoir si elles étaient concernées par la violation de données auraient pu ensuite contacter la société française. Partant, la communication publique aurait permis d'atteindre les personnes concernées.

Conclusion et amende

En conclusion, la CNIL retient, en plus d'une violation des art. 28 RGPD (contrat de sous-traitance) et art. 32 RGPD (sécurité des données), une violation de l'art. 34 RGPD (communication à la personne concernée d'une violation de données à caractère personnel). Notamment en raison du chiffre d'affaires de la société (caviardé dans la décision), l'autorité française impose à SlimPay une amende de EUR 180'000.- (art. 83 RGPD).

Bref commentaire

Cette décision française rappelle l'approche du RGPD fondée sur le risque. Une violation de la sécurité des données peut ainsi être retenue lors de la simple création d'un risque, même s'il n'y a eu aucun accès non autorisé.

En Suisse, l'actuel art. 7 LPD (art. 8 nLPD) retient la même approche. Dans la nouvelle loi (art. 61 let. c nLPD), une amende pénale est même prévue lors d'une violation intentionnelle des « exigences minimales en matière de sécurité des données édictées par le Conseil fédéral ».

Cela étant, l'actuel projet d'ordonnance relative à la loi fédérale sur la protection des données ne semble pas prévoir de telles « exigences minimales ». Si l'ordonnance n'est pas précisée, la conséquence pénale d'une violation de la sécurité des données restera probablement lettre morte.

Proposition de citation : Célian Hirsch, Les données de douze millions de consommateurs en libre accès, 31 janvier 2022 *in* www.swissprivacy.law/120