La conservation des données de cartes de crédit : est-ce licite ?

Célian Hirsch, le 18 juin 2021

La conservation de données de cartes de crédit par un commerce en ligne après une transaction unique nécessite le consentement de la personne concernée (art. 6 par. 1 let. a RGPD). En effet, les autres motifs justificatifs prévus par l'art. 6 par. 1 RGPD ne peuvent pas s'appliquer dans une telle situation.

Comité européen de la protection des données, *Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions*, 19 mai 2021.

Dans une recommandation du 19 mai 2021 (fondée sur l'art. 70 par. 1 let. e RGPD), le Comité européen de la protection des données (CEPD) se penche sur la légalité de la conservation des données de cartes de crédit dans le seul but de faciliter les potentiels futurs achats.

À titre liminaire, le CEPD justifie la publication de sa recommandation en raison du développement du commerce en ligne causé par la pandémie. En effet, l'augmentation de la conservation des données de cartes de crédit accroît le risque de vol de données et, par conséquent, de fraudes.

Par ailleurs, le CEPD constate une pratique courante des commerces en ligne : lorsqu'un consommateur achète un bien en ligne, le vendeur aura tendance à enregistrer les données de la carte de crédit utilisée afin de faciliter d'éventuels futurs achats. Or cette conservation des données doit nécessairement reposer sur l'un des motifs justificatifs mentionnés à l'art. 6 par. 1 RGPD. Le CEPD examine ainsi les potentiels motifs justificatifs à cette conservation de données. Son analyse ne s'applique toutefois ni aux fournisseurs de services de paiement, ni aux autorités publiques, ni lorsque le contrat prévoit des paiements récurrents.

Premièrement, le CEPD exclut que la conservation des données de cartes de crédit soit nécessaire « au respect d'une obligation légale à laquelle le responsable du traitement est soumis » (art. 6 par. 1 let. c RGPD). En effet, le CEPD exclut expressément du champ de son analyse les données qui sont précisément recueillies à des fin de *compliance*.

Deuxièmement, le CEPD considère que la conservation des données de cartse de crédit après

le paiement ne peut pas être considérée comme « nécessaire à l'exécution » du contrat (art. 6 par. 1 let. b RGPD). En effet, l'enregistrement de ces données peut uniquement être considéré comme nécessaire pour la transaction en question, mais non pour les potentielles transactions subséquentes.

Troisièmement, le responsable du traitement pourrait prétendre que la conservation de données de cartes de crédit est nécessaire pour ses intérêts légitimes (art. 6 par. 1 let. f RGPD).

Pour que cette condition soit remplie, non seulement le responsable devrait bénéficier d'un intérêt légitime à conserver les données de cartes de crédit, mais en plus l'enregistrement des données devrait être nécessaire pour atteindre cet intérêt légitime. Or le CEPD considère que d'éventuelles transactions futures dépendent uniquement du choix du consommateur. Par ailleurs, ces transactions ne dépendraient pas de la possibilité d'achat « en un clic » *(one click shopping*).

Enfin, pour que la condition des « intérêts légitimes du responsable du traitement » soit remplie, il faut encore procéder à une pesée des intérêts. Or le CEPD souligne que les données financières sont de nature hautement personnelle (*highly personal nature*), car leur violation peut manifestement avoir des conséquences graves sur la vie quotidienne de la personne concernée. Le fait que ces données soient conservées après la transaction augmente logiquement le risque d'un accès non autorisé à ces données. Par ailleurs, la personne concernée ne s'attend pas raisonnablement à ce que les données de sa carte de crédit soient conservées pendant une durée supérieure à celle nécessaire au paiement des biens ou des services qu'elle est en train d'acheter.

Par conséquent, le responsable de traitement ne peut en principe pas invoquer ses intérêts légitimes afin de conserver les données de cartes de crédit. Il ne peut donc que s'appuyer sur le consentement de la personne concernée (art. 6 par. 1 let. a RGPD).

Afin que le consentement de la personne concernée soit valable, celle-ci doit l'exprimer par une action affirmative et *user-friendly*, par exemple en cochant une case (et non avec une case précochée). Selon le CEPD, le consentement ne peut pas provenir des conditions générales de vente et ne peut pas non plus constituer une condition à la conclusion du contrat.

Cette recommandation risque d'avoir des conséquences concrètes pour de nombreux commerces en ligne. Ceux-ci ont évidemment un fort intérêt commercial à faciliter la conclusion définitive de l'achat le plus rapidement possible, sans que le consommateur doive effec-

tuer le moindre effort. Or il semblerait que le fait de devoir donner à nouveau les informations de sa carte de crédit réduit la probabilité que le consommateur finalise son achat. Il est probable que de nombreux commerces en ligne doivent désormais modifier leur pratique, afin que le stockage des données de cartes de crédit soit licite au regard de cette nouvelle recommandation.

En droit suisse, la situation nous semble différente. Le traitement de données personnelles ne nécessite pas en soi un motif justificatif. Seul le traitement qui porte atteinte à la personnalité d'une personne concernée, notamment lorsque les principes généraux de la protection des données ne sont pas respectés (art. 4 ss LPD ; art. 6 et 8 nLPD), requiert un motif justificatif (art. 12 s. LPD ; art. 30 s. nLPD).

À notre avis, la conservation des données de cartes de crédit ne constitue pas *per se* une atteinte à la personnalité. Les commerces en ligne suisses n'ont dès lors pas besoin de justifier ce stockage de données, notamment en obtenant le consentement de la personne concernée. Ces données doivent néanmoins être protégées par des mesures techniques et organisationnelles (art. 7 LPD et 8 nLPD ; cf. not. les mesures mentionnées par l'autorité anglaise dans sa décision contre Marriott : swissprivacy.law/68/)

Cela étant, vu l'application extraterritoriale du RGPD (art. 3 par. 2 RGPD), les commerces en ligne suisses auraient tout intérêt à s'aligner sur le droit européen. Par ailleurs, vu que les données de cartes de crédit sont particulièrement visées par les *hackers* (cf. not. swissprivacy.law/19/), un éventuel vol de données pourrait sérieusement attirer l'attention des autorités européennes, même si l'*e-commerce* se trouve en Suisse. Il pourrait dès lors être pertinent d'obtenir le consentement des personnes concernées avant de garder les données de cartes de crédit, ou simplement d'abandonner la pratique de « l'achat en un clic ».

Proposition de citation : Célian Hirsch, La conservation des données de cartes de crédit : est-ce licite ?, 18 juin 2021 *in* www.swissprivacy.law/80