Délibération n° 2019-084 du 15 mai 2019

de la Commission de Contrôle des Informations Nominatives portant recommandation sur la sécurité devant entourer les cartes de paiement en matière de vente de biens ou de fourniture de services à distance ainsi que les sites web

Vu la Constitution du 17 décembre 1962 ;

Vu le Pacte international relatif aux droits civils et politiques du 16 décembre 1966, rendu exécutoire par l'Ordonnance Souveraine n°13.330 du 12 février 1998 ;

Vu la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe du 4 novembre 1950, rendue exécutoire par l'Ordonnance Souveraine n°408 du 15 février 2006 ;

Vu la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe du 28 janvier 1981, ainsi que son Protocole additionnel du 8 novembre 2001 ;

Vu la Loi n° 1.165 du 23 décembre 1993, modifiée, relative à la protection des informations nominatives ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, susvisée ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives.

La Commission de Contrôle des Informations Nominatives,

Préambule

Conformément à l'article 1er alinéa 1 de la Loi n° 1.165 du 23 décembre 1993, les traitements automatisés ou non automatisés d'informations nominatives ne doivent pas porter atteinte aux libertés et droits fondamentaux consacrés par le titre III de la Constitution.

La Commission de Contrôle des Informations Nominatives, Autorité Administrative Indépendante, a pour mission de veiller au respect de ces dispositions. A ce titre, elle est notamment habilitée à formuler toutes recommandations entrant dans le cadre des missions qui lui sont conférées par la Loi.

Aussi elle souhaite, par la présente recommandation, préciser les grands principes applicables à la sécurité devant entourer les cartes de paiement en matière de vente de biens ou de fourniture de services à distance ainsi que les sites web, eu égard au nombre croissant de responsables de traitement effectuant auprès d'elle des formalités relatives à la mise en œuvre de sites Internet de vente en ligne.

Les principes ainsi consacrés par la présente délibération s'appliquent à tous les types de responsables de traitement, quelle que soit la formalité à laquelle ils sont soumis.

Paragraphe unique relatif à la sécurité

- **Carte bancaire**

L'utilisation de moyens de paiements en ligne et la conservation de numéros de cartes bancaires doivent faire l'objet de mesures de traçabilité permettant de détecter *a posteriori* tout accès illégitime aux données et de l'imputer à la personne ayant accédé illégitimement à ces données.

Le responsable de traitement doit prendre les mesures organisationnelles et techniques appropriées afin de préserver la sécurité, l'intégrité et la confidentialité des numéros de cartes bancaires contre tout accès, utilisation, détournement, communication ou modification non autorisé en recourant à des systèmes de paiement sécurisés conformes à l'état de l'art et à la réglementation applicable. Ces données doivent être notamment chiffrées par l'intermédiaire d'un algorithme réputé fort.

Lorsque le responsable de traitement conserve les numéros de carte bancaire pour une finalité de preuve en cas d'éventuelle contestation de la transaction, ces numéros doivent faire l'objet de mesures techniques visant à prévenir toute réutilisation illégitime, ou toute ré-identification des personnes concernées. Ces mesures peuvent notamment consister à stocker les numéros de carte bancaire sous forme hachée avec utilisation d'une clé secrète.

En outre, compte tenu de la sensibilité de cette donnée, le numéro de la carte de paiement ne peut être utilisé comme identifiant commercial.

Le responsable de traitement, ou son prestataire, ne peut demander la transmission de la photocopie ou de la copie numérique du recto et/ou du verso de la carte de paiement même si le cryptogramme visuel et une partie des numéros sont masqués, la transmission de ce document n'étant pas compatible avec les obligations de sécurité et les conditions d'utilisation que doit respecter le titulaire de la carte de paiement conformément à l'article L.133-16 du Code monétaire et financier.

Lorsque la collecte du numéro de la carte de paiement est effectuée par téléphone, il est nécessaire de mettre en place des mesures de sécurité telle que la traçabilité des accès aux numéros de la carte. Une solution alternative sécurisée, sans coût supplémentaire, doit être proposée aux clients qui ne souhaitent pas transmettre les données relatives à leurs cartes par ce moyen.

Lorsqu'un responsable de traitement veut s'assurer de l'identité d'un titulaire de carte bancaire, ou lorsqu'il doit effectuer un paiement ou un remboursement, il peut demander l'envoi sécurisé d'une copie d'un document d'identité à titre de justificatif s'il n'existe aucune autre modalité permettant de vérifier l'identité de la personne concernée.

L'accès à cette information doit être limité et restreint aux seules personnes qui, en raison de leurs fonctions, peuvent légitimement en avoir connaissance au regard de la finalité du traitement.

Le processus de collecte, lorsqu'il intervient sur un moyen de communication en ligne, doit être protégé et les copies de documents d'identité doivent être déposées sur une page sécurisée.

Il est recommandé que les copies de carte d'identité transmises lors de relations ou de ventes à distance ne soient pas en couleur et soient barrées, afin de rendre difficiles d'éventuelles reproductions du document concerné.

❖ **Site web et sécurité des traitements**

En ce qui concerne la sécurité des traitements, le responsable de traitement doit notamment s'assurer :

- que les utilisateurs s'authentifient individuellement avec un identifiant et un mot de passe réputé fort, ou par tout autre moyen d'authentification apportant au moins le même niveau de sécurité ;

- que les habilitations et les mots de passe soient régulièrement mis à jour afin de garantir que seules les personnes habilitées puissent accéder aux données nécessaires à la réalisation de leurs missions ;

- que les mesures techniques déployées garantissent la sécurité des données stockées ou échangées, en particulier lors de communications sur Internet ;

- de la mise en place d'un mécanisme de journalisation des opérations et accès effectués sur le traitement, ainsi que de la conservation des données de journalisation pendant une durée de un an à compter de leur collecte.

Dans le cas de l'utilisation d'un service de communication au public en ligne, le responsable de traitement prend les mesures nécessaires pour se prémunir contre toute atteinte à la confidentialité des données traitées (exemple : mise en place d'un protocole de communication sécurisé : SSL/TLS). Les données transitant sur des canaux de communication non sécurisés doivent notamment faire l'objet de mesures techniques visant à rendre ces données incompréhensibles à toute personne non autorisée.

Le responsable de traitement prend les mesures nécessaires pour assurer la maintenance du matériel.

Les interventions de maintenance doivent faire l'objet d'une traçabilité et le matériel remisé ne devra plus contenir de données à caractère personnel.

L'usage d'outils ou de logiciels développés par des tiers dans le cadre de la mise en œuvre d'un traitement de données à caractère personnel reste sous la responsabilité du responsable de traitement, qui doit notamment vérifier que ces outils ou logiciels respectent l'ensemble des obligations que l'article 17 de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée, met à sa charge.

Le Président

Guy MAGNAN