Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Legifrance.gouv.fr
LE SERVICE PUBLIC DE LA DIFFUSION DU DROIT

Commission Nationale de l'Informatique et des Libertés

Délibération n°2013-358 du 14 novembre 2013

Délibération n° 2013-358 du 14 novembre 2013 portant adoption d'une recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance et abrogeant la délibération n°03 034 du 19 juin 2003

NOR: CNIX1329360X

Etat: VIGUEUR
La Commission nationale de l'informatique et des libertés ;
Vu la Convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;
Vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;
Vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

Vu le code civil;
Vu le code de la consommation;
Vu le code monétaire et financier;
Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
Vu le décret n°2005-1309 du 20 octobre 2005 modifiée pris pour l'application de la loi n°78-17 du 6 janvier 1978 modifiée ;
Vu la délibération n°2012-209 du 21 juin 2012 portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n°2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel ;

Vu la recommandation n° R (90) 19 du Conseil de l'Europe relative à la protection des données à caractère personnel à des fins de paiement et autres opérations connexes ;
Vu les recommandations de la banque centrale européenne pour la sécurité des paiements par internet publiées le 31 janvier 2013;

Après avoir entendu Monsieur Bernard PEYRAT, Commissaire, en son rapport et M. Jean- Alexandre SILVY, Commissaire du gouvernement, en ses observations ;

Formule les observations suivantes :
La Commission a adopté une délibération, le 19 juin 2003, portant adoption d'une recommandation relative au stockage et à l'utilisation du numéro de carte bancaire dans le secteur de la vente à distance .
Dix ans après l'adoption de cette recommandation, l'utilisation de la carte pour les paiements à distance suscite toujours autant d'inquiétudes de la part des consommateurs. En effet, la carte de paiement reste le moyen privilégié pour les transactions en ligne malgré le développement de solutions alternatives de paiement. La sécurité et la confidentialité des données relatives à la carte est dès lors un élément clé pour garantir la confiance dans le commerce électronique.
Les plaintes reçues par la Commission ainsi que les différents contrôles menés ces dernières années ont mis en lumière la nécessité d'actualiser ses recommandations afin d'apporter des réponses concrètes aux différentes parties prenantes et de prendre en compte l'évolution du cadre légal et technologique.
Dans la perspective de la modification de la recommandation de 2003, la Commission a consulté les principaux organismes concernés parmi lesquels la Banque de France, le Groupement des cartes bancaires ainsi que les représentants des principales associations de consommateurs et des acteurs du e-commerce et de la vente à distance.
Les dispositions de la présente recommandation, qui abroge celle de 2003, s'appliquent au traitement de données relatives à la carte de paiement (carte interbancaire ou dispositif similaire), ci-après la carte , lors de toute vente d'un bien ou fourniture d'une prestation de service conclut, sans la présence physique simultanée des parties, entre un consommateur (personne physique) et un professionnel qui, pour la conclusion de ce contrat, utilisent exclusivement une ou plusieurs techniques de communication à distance (internet, téléphone, etc.).
Les cartes de paiement visées sont celles qui permettent notamment d'effectuer des achats chez un commerçant ou un prestataire de services affiliés à un réseau de paiement national ou international (système CB , Visa, Mastercard, etc.) mais aussi les cartes de paiement dites privatives (cartes émises par les commerçants ou par les établissements financiers spécialisés dans le crédit à la consommation) et accréditives (carte présentée par un adhérent à un fournisseur affilié au réseau de l'émetteur de la carte).
La présente délibération a pour objet, en l'état du droit et des procédés actuels de paiement, de préciser les recommandations de la Commission et les garanties minimales à respecter lors de la mise en œuvre, par les professionnels, de traitements afférents à des données relatives à la carte de paiement.

Article 1 : Finalités du traitement
La protection des données personnelles et par là même de la vie privée doit être envisagée comme la capacité de l'individu à maîtriser la collecte, l'enregistrement et l'utilisation des données à caractère personnel qu'il est tenu de communiquer dans le cadre d'un paiement.

La finalité première de l'utilisation d'un numéro de carte de paiement est la réalisation d'une transaction, c'est à dire la délivrance d'un bien ou la prestation d'un service en contrepartie du complet paiement d'un prix.

La collecte des données relatives à une carte de paiement remplit toutefois d'autres finalités liées à la particularité des opérations à distance :

- La réservation d'un bien ou d'un service ;

- La conservation du numéro de la carte du client afin de faciliter ses éventuels achats ultérieurs sur le site du commerçant ;

- L'offre de solutions de paiement dédiées à la vente à distance par des prestataires de services de paiement (cartes virtuelles, wallets , comptes rechargeables, etc.). Ces solutions visent à éviter aux consommateurs de saisir les données relatives à leur carte lors d'achats effectués à distance ;

- La lutte contre la fraude à la carte de paiement.

La Commission considère que ces finalités sont déterminées, explicites et légitimes.

Toutefois, la conservation des données relatives à la carte au-delà de la réalisation d'une transaction ne peut se faire qu'avec le consentement préalable de la personne concernée ou poursuivre l'intérêt légitime du responsable de traitement en ce qui concerne la lutte contre la fraude au paiement en ligne afin de ne pas méconnaître l'intérêt ou les droits et libertés des personnes, conformément à l'article 7 de la loi du 6 janvier 1978 modifiée.

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

La Commission considère que la responsabilité du traitement visant à conserver le numéro de la carte du client afin de faciliter ses éventuels achats ultérieurs sur un site marchand incombe en principe au commerçant bénéficiant du stockage des données relatives à la carte, c'est-à-dire à celui au bénéfice duquel les transactions réalisées avec les données stockées seront opérées. Les prestataires qui réalisent le stockage des données relatives à la carte pour le compte du commerçant ont la qualité de sous-traitant et sont tenus à la mise en place de mesures de sécurité adaptées.

Lorsqu'un responsable de traitement souhaite utiliser des données relatives à la carte à des fins de lutte contre la fraude au paiement et, le cas échéant, conserver une trace de comportements frauduleux ayant généré des impayés lui ayant porté préjudice, la Commission rappelle que ce traitement doit faire l'objet d'une demande d'autorisation sur le fondement des dispositions de l'article 25, I, 4° de la loi du 6 janvier 1978 modifiée. L'utilisation du numéro de carte pour cette finalité ne saurait aboutir à un refus de vente, même si elle peut conduire légitimement le commerçant à refuser ce mode de paiement.

Article 2 : Les données collectées

Les données nécessaires à la réalisation d'une transaction à distance par carte de paiement sont le numéro de la carte, la date d'expiration et le cryptogramme visuel.

La Commission rappelle que seules les données adéquates, pertinentes et non excessives au regard de la finalité du traitement doivent être collectées.
S'agissant de l'identité du titulaire de la carte, dès lors que cette donnée n'est pas requise pour la réalisation d'une transaction en ligne, elle ne doit pas être collectée par le système de paiement sauf lorsqu'elle est justifiée pour la poursuite d'une finalité déterminée et légitime, telle que la lutte contre la fraude.

La Commission considère également que 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. En effet, la transmission de ce document n'est 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.

Article 3 : Sur la durée de conservation des données :

La Commission considère que la durée de conservation des données relatives à la carte doit correspondre au délai nécessaire à la réalisation de la transaction, c'est-à-dire au paiement effectif qui peut être différé à la réception du bien, augmenté, le cas échéant, du délai de rétractation prévu pour les ventes de biens et fournitures de prestations de services à distance (article L. 121-20 du code de la consommation).

S'agissant des commerçants en ligne, le risque financier d'une utilisation non autorisée pesant in fine sur ces derniers, dès lors qu'ils n'ont pas mis en œuvre un système d'authentification de leurs clients, la Commission estime qu'ils peuvent conserver le numéro de carte et la date de validité de celle-ci, à l'exclusion du cryptogramme visuel, dès lors que cette conservation est nécessaire pour la gestion des éventuelles réclamations des titulaires de cartes de paiement. Les données peuvent être conservées pour la durée prévue par l'article L 133-24 du code monétaire et financier, en l'occurrence 13 mois suivant la date de débit. Ce délai peut être étendu à 15 mois afin de prendre en compte la possibilité d'utilisation de cartes de paiement à débit différé.

Les données ainsi conservées à des fins de preuve doivent être versées en archives intermédiaires et utilisées uniquement en cas de contestation de la transaction. Les numéros de carte de paiement conservés à cette fin doivent faire l'objet de mesures de sécurité techniques, telles que décrites à l'article 5 de la présente recommandation, visant à prévenir toute réutilisation illégitime.

Dans les cas où les données relatives à la carte seraient collectées par un organisme assujetti aux obligations de lutte contre le blanchiment de capitaux pour offrir une solution de paiement à distance, elles peuvent être conservées jusqu'à la clôture du compte puis, le cas échéant, archivées conformément aux obligations légales en la matière.

La Commission observe que la finalité du cryptogramme visuel est de s'assurer que le porteur est bien en possession du support physique de la carte. Dès lors, toute conservation du cryptogramme est susceptible de porter atteinte à cette finalité. En conséquence, la conservation du cryptogramme est interdite au-delà du temps strictement nécessaire à la réalisation de la transaction, y compris en cas de paiements successifs ou de conservation du numéro de la carte pour les achats ultérieurs.

Dans les cas où le numéro de la carte serait utilisé à d'autres fins, telles que la constitution d'un compte client visant à faciliter les achats ultérieurs ou la lutte contre la fraude, sa durée de conservation ne saurait excéder la durée nécessaire à l'accomplissement de cette finalité.

Article 4 : Les droits des personnes :
Toute utilisation du numéro de carte de paiement, quelle qu'en soit la finalité, doit faire l'objet d'une information complète et claire auprès des personnes.
De manière générale, la personne concernée est informée de l'identité du responsable du traitement, des finalités du traitement, du caractère obligatoire ou facultatif des informations à renseigner, des conséquences éventuelles, à leur égard, d'un défaut de réponse, des destinataires des données, de l'existence et des modalités d'exercice de ses droits d'accès, de rectification et d'opposition au traitement de ses données et le cas échéant des transferts de données hors Union européenne.
Dans l'hypothèse où les données relatives à la personne ont été communiquées à un tiers par le commerçant, celui-ci doit informer ces tiers sans délai de l'exercice du droit d'opposition ou de rectification par la personne concernée.

Lorsque les données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention de ces informations conformément au dernier alinéa de l'article 32 de la loi du 6 janvier 1978 modifiée.
Lorsque les données relatives à la carte sont conservées au-delà du temps strictement nécessaire à la réalisation de la transaction, pour simplifier un paiement ultérieur, la Commission considère que ce traitement doit également avoir reçu le consentement libre, spécifique et informé de la personne concernée conformément aux dispositions de l'article 7 de la loi du 6 janvier 1978 modifiée.

La Commission estime, en effet, que ces données ne sont pas collectées pour permettre la réalisation d'un paiement mais pour offrir un service supplémentaire au client, en l'occurrence ne pas avoir à ressaisir son numéro de carte lors d'un prochain achat. Dès lors, ce traitement de données doit être effectué avec le consentement préalable de la personne concernée. Celui-ci ne se présume pas et doit prendre la forme d'un acte de volonté explicite, par exemple au moyen d'une case à cocher (non pré-cochée par défaut). L'acceptation des conditions générales d'utilisation ou de vente n'est pas considérée comme une modalité suffisante du recueil du consentement des personnes.

La Commission recommande également que le responsable de traitement intègre directement sur son site marchand un moyen simple de retirer, sans frais, le consentement donné pour la conservation des données de la carte afin de faciliter les achats ultérieurs.

Article 5 : Les mesures de sécurité
La Commission observe que les pratiques liées à la collecte du numéro de carte de paiement entraînent la multiplication de bases de données pouvant potentiellement faire l'objet d'une réutilisation frauduleuse, en cas notamment de faille de sécurité aboutissant à la compromission de ces données.
La Commission considère en conséquence que les responsables de traitement doivent s'efforcer d'élaborer et d'adopter des pratiques exemplaires et promouvoir des comportements qui tiennent compte des impératifs de sécurité et qui respectent les intérêts légitimes des individus. A cet égard, la Commission rappelle que :
- l'article 34 de la loi Informatique et Libertés impose au responsable de traitement de prendre des mesures de sécurité afin d'éviter notamment tout accès illégitime aux données traitées. Ces mesures doivent être proportionnées aux risques engendrés par le traitement pour les personnes concernées. Les accès non autorisés aux données relatives à la carte pouvant déboucher sur la réalisation de transactions frauduleuses, la confidentialité de ces données se doit d'être spécifiquement protégée. Le non-respect de cette obligation de sécurité est sanctionné par l'article 226-17 du code pénal ;
- l'article 35 de la loi Informatique et Libertés impose au responsable de traitement désirant externaliser la gestion du système de paiement de choisir un sous-traitant présentant des garanties suffisantes permettant de s'assurer de la mise en œuvre des mesures de sécurité rendues nécessaires au titre de l'article 34, et de fixer contractuellement les objectifs de sécurité qu'ils imposent à leur sous-traitant. Dans tous les cas, le recours à la sous-traitance ne dispense en aucun cas le responsable de traitement de ses obligations au titre de l'article 34.

Ceci étant rappelé, elle recommande que :
- Les responsables de traitements utilisent uniquement des services de paiement en ligne sécurisés et conformes à l'état de l'art et à la réglementation applicable. A cet égard, seuls les dispositifs conformes à des référentiels reconnus en matière de sécurisation de données relatives à la carte au niveau européen ou international (par exemple le standard PCI DSS) doivent être utilisés. Le responsable doit également s'assurer de la conformité du traitement aux exigences des articles 34 et 35 de la loi du 6 janvier 1978 modifiée, au travers notamment de la mise en œuvre d'une démarche de gestion des risques de manière à déterminer les mesures de sécurité organisationnelles et techniques nécessaires. Pour accompagner les responsables dans cette démarche, des guides "Gestion des risques vie privée" sont accessibles sur le site Internet de la Commission ;

- les responsables de traitement et leurs sous-traitants éventuels adoptent une politique de gestion stricte des habilitations de leurs personnels ne donnant accès au numéro de la carte de paiement des clients que lorsque cela est rigoureusement nécessaire. Des mesures d'obfuscation (masquage de tout ou partie du numéro de la carte lors de leur affichage ou de leur stockage) ou de tokenisation (remplacement du numéro de carte par un numéro non signifiant) doivent être mises en œuvre afin de limiter l'accès aux numéros de carte. Le personnel doit être sensibilisé aux risques de fraudes en matière de données relatives à la carte et aux mesures de sécurité permettant de les éviter ;
- les responsables de traitements et leurs sous-traitants éventuels ne procèdent en aucun cas à l'enregistrement de données relatives à la carte de paiement sur le terminal de leurs clients, et ne doivent pas non plus inciter ces derniers à procéder à un tel enregistrement, ces terminaux n'étant pas conçus pour assurer la sécurité de ce type de données ;
- les responsables de traitement et leurs sous-traitants éventuels prennent les mesures nécessaires pour se prémunir contre toute atteinte à la confidentialité des données relatives à la carte lorsque celles-ci sont collectées via un service de communication au public en ligne. Les données transitant sur des canaux de communication publics ou interceptables doivent notamment faire l'objet de mesures techniques visant à rendre ces données incompréhensibles à toute personne non autorisée ;
- Lorsque les données relatives à la carte de paiement sont conservées afin de faciliter la réalisation ultérieure de transactions, les accès ou utilisations de ces données doivent faire l'objet de mesures de traçabilité spécifiques permettant de détecter a posteriori tout accès ou utilisation illégitime des données et de l'imputer à la personne responsable.
- la Commission estime nécessaire une notification aux personnes dont les données ont fait l'objet d'une violation de sécurité afin qu'elles puissent prendre les mesures appropriées pour limiter les risques de réutilisation frauduleuse de leurs données (contestation de paiements frauduleux, mise en opposition de la carte, etc.).
- Lorsque les données relatives à la carte de paiement sont conservées pour une finalité de lutte contre la fraude, elles doivent faire l'objet de mesures techniques visant à prévenir toute réutilisation illégitime. Ces mesures peuvent notamment consister à stocker les numéros de la carte de paiement sous forme hachée avec utilisation d'une clé secrète.
- La Commission recommande la mise en place de moyens d'authentification renforcée du titulaire de la carte de paiement visant à s'assurer que celui-ci est bien à l'origine de l'acte de paiement à distance.
- Lorsque la collecte du numéro de la carte de paiement est effectuée par téléphone, la Commission rappelle qu'il est également nécessaire de mettre en place des mesures de sécurité telle que la traçabilité des accès aux numéros de la carte. Elle recommande qu'une solution alternative sécurisée, sans coût supplémentaire, soit proposée aux clients qui ne souhaitent pas transmettre les données relatives à leurs cartes par ce moyen.

Article 6

La délibération n° 03-034 du 19 juin 2003 est abrogée.

La présente délibération est publiée au Journal Officiel de la République française

La Présidente

Isabelle FALQUE-PIERROTIN

Nature de la délibération: RECOMMANDATION
Date de la publication sur legifrance: 7 décembre 2013