Délibération n° 2018-303 du 06 septembre 2018 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° 2017-222 du 20 juillet 2017

Lien Légifrance : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000037481613/

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 le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données - RGPD) ;

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 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

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 les lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est susceptible d'engendrer un risque élevé aux fins du règlement (UE)2016/679 adoptée le 4 octobre 2017 par le groupe de travail de l'article 29 sur la protection des données ;

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 M. François PELLEGRINI, Commissaire, en son rapport, et Mme Nacima BELKACEM, 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, la Commission a adopté une nouvelle délibération visant à l'actualiser et à proposer des préconisations concrètes à l'utilisation du numéro de carte bancaire par les professionnels de la vente à distance dans un traitement automatisé.

Elle estime aujourd'hui nécessaire d'actualiser sa recommandation au regard de l'évolution des pratiques du commerce en ligne, ainsi que de celle du cadre légal et technologique.

Les dispositions de la présente recommandation, qui abroge celle de 2017, 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 conclu, sans la présence physique simultanée des parties, entre un consommateur (personne physique) et un professionnel, et 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 Commission précise que l'article 35 du RGPD prévoit la conduite d'une analyse d'impact relative à la protection des données (AIPD), lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, compte tenu notamment de la nature des données traitées. A cet égard, la Commission rappelle que les données financières, dont les données relatives aux cartes de paiement, sont qualifiées de données à caractère hautement personnel compte tenu de la gravité des impacts pour les personnes concernées que leur violation pourrait engendrer (utilisation pour des paiements frauduleux par exemple).

La Commission rappelle aux organismes qui mettraient en œuvre un tel traitement de données de paiement qu'ils sont susceptibles d'être tenus, selon l'ampleur du traitement et les modalités de sa mise en œuvre, de réaliser une AIPD.

Article 1er : Finalités du traitement

La protection des données personnelles, et par là même de la vie privée, implique 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 de permettre la réalisation d'une transaction visant à la délivrance d'un bien ou la prestation d'un service en contrepartie du paiement complet d'un prix.

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

- la réservation d'un bien ou d'un service ;
- le règlement d'abonnements souscrits en ligne impliquant des paiements définis et réguliers ;
- la simplification des 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, porte-cartes numériques dits *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.

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

Elle rappelle que les données collectées et traitées aux fins de règlement de paiements multiples et réguliers dans le cadre d'abonnements ne peuvent être ultérieurement utilisées pour une autre finalité telle que, par exemple, faciliter des paiements ponctuels ultérieurs, et inversement.

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

Article 2 : Base légale du traitement

La Commission considère que la base légale du traitement des données bancaires peut varier en fonction de la finalité poursuivie, de la nature de la transaction conclue et des modalités de son exécution, conformément à l'article 6 du RGPD.

La Commission rappelle qu'il appartient au responsable de traitement de s'assurer des conditions de licéité de son traitement et, notamment, de la base légale sur laquelle le fonder.

2.1. Le paiement unique

La Commission relève que le numéro de carte bancaire ne peut être collecté et traité que pour permettre la réalisation d'une transaction dans le cadre de l'exécution du contrat conclu par la personne concernée conformément à l'article 6-1-b du RGPD (exécution contractuelle). Ainsi, en cas de contrat impliquant un paiement unique, la Commission estime que les données n'ont donc pas vocation à être conservées au-delà du temps de transaction commerciale.

2.2. L'abonnement impliquant des paiements multiples

La Commission considère que dans le cadre d'un contrat d'abonnement souscrit en ligne impliquant, de fait, des paiements successifs et réguliers, la conservation des données bancaires satisfait également à la condition prévue à l'article 6-1-b du RGPD (exécution contractuelle).

2.3. Les solutions de paiement dédiées à la vente à distance

En ce qui concerne le traitement des données bancaires dans le cadre de la souscription d'une solution de paiement dédiée à la vente à distance par des prestataires de services de paiement (cartes virtuelles, porte-cartes numérique – *wallets* , comptes rechargeables, etc.), la Commission estime que la communication des coordonnées bancaires entre également dans le cadre de l'exécution du contrat, celui-ci visant précisément à conserver les données relatives à la carte de paiement afin d'éviter aux consommateurs d'avoir à les saisir lors d'achats effectués à distance.

2.4. L'option permettant de faciliter les éventuels paiements ultérieurs

La Commission estime que la conservation du numéro de la carte du client afin de faciliter ses éventuels paiements ultérieurs, et éventuellement pouvoir procéder à un achat en un clic sur le site du commerçant, va au-delà de l'exécution du contrat conclu.

Elle retient que cette faculté constitue une option indépendante de l'acte initial ayant conduit à la collecte des coordonnées bancaires et rappelle qu'un tel traitement nécessite que soit recueilli au préalable le consentement libre, spécifique, éclairé et univoque des personnes, en application de l'article 6-1-a du RGPD.

2.5. La souscription à un abonnement, à titre gratuit ou onéreux, donnant accès à des services additionnels, traduisant l'inscription du client dans une relation commerciale régulière

La Commission rappelle que la conservation du numéro de la carte du client afin de faciliter ses éventuels paiements ultérieurs sur le site du commerçant va au-delà de l'exécution du contrat conclu.

La Commission considère cependant que le fait pour une personne de souscrire à un abonnement qui donne accès à des prestations additionnelles à celles accessibles à tout client peut traduire l'intention du client de s'inscrire dans une relation commerciale régulière. Ces prestations additionnelles peuvent prendre la forme de services supplémentaires annexes demandés par le client (livraison rapide, accès à des ventes privées ou à des contenus complémentaires, etc.).

Dans de tels cas, la Commission estime que la conservation des données bancaires de la personne pour faciliter ses achats ultérieurs peut être basée sur l'intérêt légitime du responsable de traitement, la personne pouvant, dans ses conditions, raisonnablement s'attendre à ce que ses données bancaires soient conservées pour simplifier ses achats ultérieurs.

La Commission précise que l'intention du client de s'inscrire dans une relation commerciale régulière doit être manifeste. La souscription à un tel abonnement doit donc être distincte de la simple création d'un compte client donnant accès aux services de base. Il doit s'agir d'une démarche complémentaire à la création et au fonctionnement courant d'un compte client. La souscription à l'abonnement peut néanmoins intervenir de manière concomitante à la création d'un compte client.

De même, la Commission estime que la simple inscription à un programme ou compte de fidélité, en contrepartie d'avantages et de récompenses, qui ne donnerait pas accès à des prestations supplémentaires visant à faciliter les achats, ne saurait suffisamment traduire l'intention du client de procéder à des achats réguliers auprès du commerçant, justifiant ainsi la conservation de ses données bancaires par défaut, sur la base de l'intérêt légitime du responsable de traitement.

De plus, pour pouvoir s'appuyer sur la base de l'intérêt légitime à réaliser un tel traitement, le responsable du traitement doit clairement en informer les personnes concernées ainsi que leur permettre de s'y opposer en faisant figurer une mention et un moyen visible, explicite et ergonomique tel qu'une case à cocher, directement sur le support de collecte (voir article 5 de la présente délibération portant sur l'information et les droits des personnes).

La lutte contre la fraude à la carte de paiement

La Commission estime que la conservation des données relatives à la carte de paiement au-delà de la réalisation d'une transaction à des fins de lutte contre la fraude à la carte de paiement ne rentre pas dans le cadre du contrat. Elle considère en effet que ce traitement relève de l'intérêt légitime du responsable de traitement, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés des personnes en application de l'article 6-1-f du RGPD, en garantissant notamment le respect des principes de transparence et l'effectivité de l'exercice de leurs droits par les personnes concernées.

La Commission rappelle que l'utilisation du numéro de carte bancaire dans le cadre d'un traitement visant à lutter contre la fraude et, le cas échéant, la conservation d'une trace de comportements frauduleux ayant généré des impayés, ne saurait aboutir à un refus de vente. La Commission précise que cette utilisation peut néanmoins conduire le commerçant à refuser ce mode de paiement.

Article 3 : 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 limitées à ce qui est nécessaire 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 4 : Sur la durée de conservation des données

La Commission rappelle qu'en application de l'article 5-1-e du RGPD, les données doivent être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

Elle rappelle à cet égard que la conservation du cryptogramme après la réalisation de la première transaction est interdite, dans tous les cas de figure, y compris pour les abonnements nécessitant différents paiements.

4.1. Les paiements uniques et abonnements

La Commission précise que :

- **s'agissant de paiements uniques** (achats ponctuels ou abonnement sans tacite reconduction, réglé en une seule fois), 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 ou à l'exécution de la prestation de service, augmenté, le cas échéant, du délai de rétractation prévu pour les ventes de biens et fournitures de prestations de services à distance (article L.121-20-12 du code de la consommation) ;
- **en ce qui concerne les abonnements impliquant des paiements échelonnés**, la conservation de ses données bancaires est justifiée :
- jusqu'à la dernière échéance de paiement, si l'abonnement ne prévoit pas de tacite reconduction ;

- jusqu'à résiliation de l'abonnement en cas de renouvellement par tacite reconduction, sous réserve des dispositions applicables et notamment de l'information des personnes concernées avant le renouvellement.

4.2. La gestion des réclamations

S'agissant des commerçants en ligne, le risque financier d'une utilisation non autorisée pesant *in fine* sur ces derniers dans le cas où 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 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 6 de la présente recommandation, visant à prévenir toute réutilisation illégitime.

4.3. La lutte contre le blanchiment

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.

4.4. Autres finalités

Dans les cas où le numéro de la carte serait utilisé à d'autres fins, dans le cadre d'une simple option visant à faciliter les achats ultérieurs, d'un abonnement donnant accès à des services additionnels ou d'un traitement de lutte contre la fraude, sa durée de conservation ne saurait excéder la durée nécessaire à l'accomplissement de cette finalité.

Article 5 : Les droits des personnes

5.1. L'obligation générale d'information

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. Elles doivent être informées de ce qu'il sera fait de leurs données et ce, dès le stade de la collecte, dans les conditions prévues par les articles 13 et 14 du RGPD.

Elles doivent être informées de la manière d'exercer les droits :

- de retrait de leur consentement ou d'opposition au traitement de leurs données ;
- d'accès, rectification et effacement des données qui les concernent ;
- à la limitation du traitement ; par exemple, lorsque la personne conteste l'exactitude de ses données, elle peut demander par ailleurs le gel temporaire du traitement des données le temps que l'organisme procède aux vérifications nécessaires ;
- à la portabilité : le responsable de traitement doit permettre à toute personne de recevoir, dans un format structuré couramment utilisé, l'ensemble des données traitées par des moyens automatisés qui auraient été fournies par la personne sur la base de son

consentement ou d'un contrat. Il est donc recommandé de préciser aux personnes concernées les traitements concernés par ce droit.

Selon la finalité poursuivie, le consentement des personnes (en cas de conservation des données aux seules fins de faciliter des paiements ultérieurs, par exemple) ou un moyen de s'opposer à certaines opérations de traitement (telle que la conservation des données dans le cadre d'un abonnement donnant accès à une relation commerciale privilégiée, par exemple) devra également être prévu sur le support de collecte des données.

5.2 L'information spécifique lors de la reconduction tacite de l'abonnement

En ce qui concerne les contrats d'abonnement avec reconduction tacite, la Commission rappelle que le responsable de traitement est tenu d'informer la personne concernée de la reconduction tacite de son contrat et, sauf opposition de sa part, de la conservation de ses coordonnées bancaires pour le paiement des échéances du nouveau contrat.

5.3 L'information et le recueil du consentement lors de la conservation des données aux fins de faciliter des paiements ultérieurs

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 avoir reçu le consentement libre, spécifique, éclairé et univoque de la personne concernée, conformément aux dispositions de l'article 6 du RGPD.

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 et/ou permettre qu'elle puisse procéder à un achat en un clic . Dès lors, ce traitement de données nécessite que soit recueilli le consentement préalable de la personne concernée. Celui-ci ne se présume pas et doit prendre la forme d'un acte de volonté univoque, 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.

Afin de satisfaire l'obligation prévue à l'article 7-3 du RGPD, la Commission recommande que le responsable de traitement intègre directement sur son site marchand un moyen simple de retirer, sans frais, le consentement donné.

5.4 L'information et l'opposition préalable à la conservation des données bancaires en cas de souscription à un abonnement donnant accès à des services additionnels facilitant les achats, traduisant l'inscription du client dans une relation commerciale régulière

La Commission estime que le fait pour une personne de souscrire un abonnement lui donnant accès à des prestations annexes (livraison rapide, accès à des ventes privées ou contenus supplémentaires, etc.) peut traduire l'intention du client de s'inscrire dans une relation commerciale régulière.

Dans de tels cas, la Commission estime que la conservation des données bancaires de la personne pour faciliter ses achats ultérieurs peut être basée sur l'intérêt légitime du responsable de traitement, la personne pouvant, dans ces conditions, raisonnablement s'attendre à ce que ses données bancaires soient conservées pour simplifier ses achats ultérieurs.

Toutefois, pour pouvoir valablement s'appuyer sur la base légale de l'intérêt légitime, le responsable du traitement doit clairement informer les personnes concernées, lors de la saisie de leurs données bancaires sur le support dédié, de leur conservation par défaut et de la durée de cette conservation.

Lors de cette saisie, la personne doit également pouvoir s'opposer, simplement et discrétionnairement, par un moyen visible, explicite et ergonomique, tel qu'une case à cocher, à la

conservation de ses données bancaires. L'opposition exprimée par ce biais doit être prise en compte par le responsable du traitement, y compris lors d'achats ultérieurs.

En cas d'opposition exprimée par la personne concernée quant à la conservation de ses données bancaires, le responsable du traitement ne pourra, par la suite, pas conserver par défaut les données bancaires nouvellement saisies par le client lors d'achats ultérieurs.

L'enregistrement des données bancaires saisies ne pourra être réalisé qu'à la demande explicite de la personne concernée, exprimée ici encore par moyen visible, explicite et ergonomique, tel qu'une case à cocher.

Enfin, le responsable du traitement doit également permettre aux personnes de demander, à tout moment et de manière discrétionnaire, la suppression de leurs données bancaires.

Article 6 : Les mesures de sécurité

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 ou pour le règlement d'un abonnement 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.

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 de 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 32 du RGPD impose au responsable de traitement de prendre des mesures de sécurité (techniques et organisationnelles) 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 ;
- l'article 28 du RGPD 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 notamment de la mise en œuvre des mesures de sécurité rendues nécessaires au titre de l'article 32 du RGPD. Le responsable de traitement et le sous-traitant choisi sont tenus d'établir un contrat précisant leurs obligations respectives et reprenant les dispositions prévues à l'article 28 du RGPD.

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 du RGPD, 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 et Guide du sous-traitant sont accessibles sur le site web de la Commission ;

- le responsable de traitement et son ou ses 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 son affichage ou de son stockage) ou de remplacement du numéro de carte par un numéro non signifiant (tokenisation) doivent être mises en œuvre afin de limiter l'accès aux numéros de cartes. 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 ;

- le responsable de traitement et son ou ses sous-traitants éventuels ne procèdent en aucun cas à l'enregistrement de données relatives à la carte de paiement localement, sur l'équipement terminal de leurs clients (tels qu'ordinateurs ou ordiphones par exemple), et ne doivent pas non plus inciter ces derniers à procéder à un tel enregistrement, ces équipements n'étant pas conçus pour assurer la sécurité de ce type de données ;

- le responsable de traitement et son ou ses 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 susceptibles d'interception 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 ;

- en plus de la notification de violation qui doit être adressée à la CNIL, les personnes dont les données ont fait l'objet d'une violation de sécurité soient notifiées 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'un sel secret qui ne soit pas conservé dans le même espace de stockage ;

- des moyens d'authentification renforcée du titulaire de la carte de paiement soient mis en place, 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, 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 7

La délibération n° 2017-222 du 20 juillet 2017 est abrogée.

La présente délibération sera publiée au Journal officiel de la République française.

Le Président

Alex TURK