



# Données personnelles et publicité par voie électronique

publié le **29/06/2014**, vu **3922 fois**, Auteur : [Noé MARMONIER Avocat](#)

**L'économie numérique est source de nouvelles formes de publicité. Sites internet de vente en ligne, réseaux sociaux, applications pour smartphones et tablettes tactiles, collectent les données personnelles des consommateurs. Ces données peuvent être réutilisées à des fins de prospections commerciales. Protéger ses données personnelles est nécessaire. Décryptage.**

Afin de démarcher la clientèle, les sociétés ont aujourd'hui massivement recours à la publicité par voie électronique.

Elle opère par l'envoi de SMS, MMS ou de courriers électronique.

Le consommateur est de plus en plus souvent invité à renseigner des formulaires en ligne, notamment lorsqu'il crée une carte de fidélité, ou un compte utilisateur sur un site de e-commerce.

Ces données sont ensuite utilisées par les sociétés pour réaliser la publicité de leurs produits ou services.

Certaines sociétés se spécialisent dans la collecte de données personnelles, afin d'établir des profils de consommateurs, qui sont ensuite revendus à des sociétés publicitaires, ou à des sociétés commerciales. Autant d'atteintes potentielles aux données personnelles des consommateurs, pour lesquelles il convient d'exercer une vigilance toute particulière.

Cette prospection commerciale peut attenter à la protection des données personnelles des consommateurs.

La publicité électronique bénéficie aujourd'hui d'un régime juridique, qui demeure cependant perfectible.

Il est à la portée de chaque consommateur de veiller à la protection de ses données personnelles, à une autorisation consentie ou non de ses données, et le cas échéant, d'exercer son opposition à l'utilisation.

En vertu de l'article L34-5 du Code des postes et des communications électroniques, est interdite "*la prospection directe par l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services.*"

Mais, la publicité électronique "est autorisée si les coordonnées du destinataire ont été recueillies directement auprès de lui, dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'occasion d'une vente ou d'une prestation de services, et si le destinataire se voit offrir, de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais, hormis ceux liés à la transmission du refus, et de manière simple, à l'utilisation de ses coordonnées lorsque celles-ci sont recueillies et chaque fois qu'un courrier électronique de prospection lui est adressé."

En conséquence, le consentement aux sollicitations commerciales électroniques doit être recueilli avant l'envoi d'un tel message publicitaire.

Le consentement est généralement recueilli auprès du consommateur par le cochage d'une case par celui-ci.

Le pré-cochage est une pratique prohibée, puisqu'elle présume le consentement de la personne.

Une stipulation des conditions générales de vente ou d'utilisation d'une site ou d'une application prévoyant l'acceptation du consentement par la seule acceptation des conditions générales constitue également une pratique prohibée, qui ne souffre d'aucunes exceptions.

La norme simplifiée n°48 de la CNIL, découlant de 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, édicte des normes en matière de publicités électroniques.

La norme n°48 de la CNIL consacre un principe de conservation limitée des données.

Un principe de suppression automatique est prévue dans le cas où le consommateur ne répond à aucune sollicitations 3 ans après le dernier contact.

Les données relatives aux pièces d'identité sont conservées pendant un délai d'un an, par application de l'article 9 du Code de procédure pénale.

Les données relatives aux cartes bancaires doivent par principe être supprimées dès la finalisation de la transaction. Cependant, l'article L133-24 du Code monétaire et financier prévoit que les données peuvent être conservées pendant 13 mois suite à la transaction, à des fins probatoires en cas de litige avec le consommateur.

Il n'est pas autorisé d'utiliser des données à d'autres fins que celles pour lesquelles ces données ont été collectées.

Il n'est pas autorisé de conditionner l'accès à un service, l'achat d'un bien ou d'un service, ou le bénéfice d'une réduction à l'acceptation de recevoir des messages de sollicitations électroniques.

Dès lors, en cas de difficultés, la CNIL est compétente pour instruire les demandes de plainte en non-conformité à la norme n°48, comme le prévoit l'article L34-5 du Code des postes et des communications électroniques.

Il est aussi possible de déposer plainte, sur le fondement des articles 226-16 et suivants du Code pénal, en cas de collecte illicite des données personnelles.

Une dérive issue de la publicité électronique est particulièrement redoutable pour collecter des données personnelles, en parfaite illégalité, et susceptibles de causer un préjudice financier

substantiel pour la personne qui se laisse tromper.

Il s'agit du phishing ou hameçonnage. Cette pratique de cybercriminalité consiste à envoyer une multitude de mails à des internautes-cibles (clients d'une banque, d'un opérateur de téléphonie mobile) dans lesquels les destinataires sont invités à renseigner des données personnelles, notamment de nature bancaire, sous prétexte d'une mise à jour de celles-ci, ou suite à une prétendue perte des données causée par un faux problème technique.

Les escrocs reproduisent servilement une page internet d'une banque, d'une administration ou d'un opérateur téléphonique, afin de donner force et crédit à leurs manoeuvres frauduleuses.

Il est vivement recommandé de ne jamais répondre à ces mails, et en cas de doute, de contacter directement le service client ou le contact institutionnel afin de vérifier si cette procédure est régulière.

Si le mal est fait, et que l'internaute a subi un préjudice en renseignant ses données personnelles, il convient de déposer plainte auprès du Procureur de la République, sur le fondement de l'article 226-18 du Code pénal.

L'internaute peut se constituer partie civile afin de demander l'indemnisation du préjudice subi.

L'article 226-18 du Code pénal dispose que "*Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende*".

Ne négligez pas vos données personnelles !