Les données personnelles et la protection de la vie privée à l'heure des nouvelles technologies

Révisé le 28/03/2012, par la Rédaction de Net-iris

Plan :

Introduction

Si la notion de **données personnelles** d'un individu englobe une quantité non-négligeable et importante d'informations plus ou moins nominatives (nom, prénom, âge, sexe, lieu de résidence, loisirs préférés, pseudo, n°client, etc.), force est de constater que bon nombre de personnes ignorent précisément de quoi il s'agit, mais aussi par qui et dans quel but des **fichiers** sont créés.

S'il est aisé d'imaginer que nous sommes tous fichés par l'Etat et les organismes qui lui sont rattachés (sécurité sociale, fisc, police à travers la carte nationale d'identité, la préfecture lors de l'établissement de la carte grise, le Pôle emploi, le médecin, etc.), par son employeur, par des associations indépendantes (club de sport, association à laquelle on fait un don, forum de discussion ou chat, etc.) ou encore par des sociétés commerciales (banque, assureurs, téléphonie, fichiers clients des commerces, etc.), on imagine moins être fichés par des sociétés que l'on ne connaît pas. Et pourtant, **les données personnelles circulent facilement** soit **contre rémunération** pour le titulaire du fichier, soit de manière involontaire en cas notamment de piratage informatique ou de détournement de la finalité d'un fichier.

C'est pour cela qu'en France, la CNIL, la **Commission nationale informatique et libertés veille** à ce que loi Informatique et libertés et les autres textes qui protègent ces données personnelles, soient respectés, afin d'éviter les abus et les atteintes aux droits fondamentaux.
A l'heure d'**internet**, du **piratage informatique**, de la **traçabilité**, du **marketing-comportemental**, du **spam**, du développement de la **biométrie**, de la **vidéosurveillance**, des péages autoroutiers et d'autres technologies avancées, la préservation de sa vie privée n'est pas aisée, et il est utile de faire le point sur ce thème particulièrement important, qui d'ailleurs devrait conduire dans un avenir proche à la révision de la législation française et européenne en la matière.

Qu'est ce qu'une donnée à caractère personnel ?

Il s'agit principalement des informations qui permettent d'identifier soit directement, soit indirectement par recoupement d'informations, une personne, telles que :

- nom, prénom,
- photo,
- date de naissance,
- statut matrimonial,
- adresse postale, email, adresse IP d'ordinateur
- n° de sécurité sociale,
- n° de téléphone,
- n° de carte bancaire,

- plaque d'immatriculation du véhicule,
- empreinte génétique,
- élément d'identification biométrique,
- etc.

La définition exacte est la suivante : "*toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement ou par référence à un numéro d'identification ou à plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont disposent ou auxquels peuvent avoir accès le responsable du traitement ou toute autre personne*".

Il convient de préciser que certaines informations, qui ne sont pas des données à caractère personnel, sont considérées comme sensibles dans la mesure où elles peuvent conduire à un **comportement discriminatoire** (ex : origine raciale, opinions politiques, philosophiques ou religieuses, appartenance syndicale, information relative à la santé ou à ses orientations sexuelles). En principe, ces **données dites "sensibles"** ne peuvent être recueillies et exploitées. Toutefois, certains traitements relatifs à ces données sont possibles dans la mesure où la finalité du traitement l'exige et moyennant le respect de certaines conditions, dont le consentement explicite de la personne fichée.

A noter également que certains fichiers publics (fisc, sécurité sociale, caf, police et justice, etc.) sont constitués sans notre accord et sans possibilité d'opposition de notre part, car ils ont un but précis et souvent lié à la sécurité du territoire et au respect des principes de notre République (ex : paiement des impôts, droits aux allocations, à la protection sociale).

Pour d'autres en revanche, il est possible d'exercer son droit d'opposition à être fiché et/ou de rectification.

Ce que dit la loi

En France, c'est principalement la loi Informatique et libertés de 1978, dont la dernière révision date de 2004, qui réglemente la collecte, l'usage et la finalité de la mise en place d'un traitement automatisé ou d'un fichier manuel contenant des données personnelles.
Se trouvent soumis à la cette loi, "*les traitements de données à caractère personnel dont le responsable est soit établi sur le territoire français (c'est-à-dire y exerce une activité dans le cadre d'une installation stable, quelle que soit sa forme juridique, filiale, succursale...) ou recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne*".

Les responsables de traitements sont tenus de délivrer une information détaillée sur les conditions d'utilisation des données lors de leur collecte, que celles-ci soient recueillies de manière directe ou indirecte. Le droit d'opposition est garanti par la loi en matière de prospection commerciale, de même que les droits d'accès et de rectification sont précisés. Néanmoins, il existe des dérogations pour tenir compte en particulier des spécificités de certains traitements notamment statistiques.

Seuls sont soumis à autorisation ou avis de la CNIL, "*les traitements présentant des risques particuliers au regard des droits et libertés de personnes*". Les autres, exempts de risques, doivent seulement faire l'objet d'une déclaration de fichier quand des exonérations de déclaration ne sont pas prévues (à titre d'exemple, ne sont pas soumis à déclaration, les registres destinés exclusivement à l'information du public, ou encore les traitements de conservation d'archives).

Dans le monde du travail, il est possible et recommandé dans les grandes structures, de nommer ou plusieurs correspondants à la protection des données dans les entreprises ou les collectivités locales. C'est un décret (n°2007-451) du 25 mars 2007 qui a encadré les obligations mises à la charge du responsable du traitement, quel qu'il soit.

Pourquoi la protéger ?

Contrairement à ce que l'on pourrait croire, les **informations nominatives** en disent long sur notre vie privée puisqu'elles permettent de déterminer, par exemple, notre style de vie et nos comportements d'achat (lieu d'habitation, centre d'intérêt d'achat, loisirs), sur notre intimité (les produits que l'on affectionne le plus), ou encore sur nous-mêmes (discussions sur des forums, adhésion à un syndicat ou à un parti politique). Ces informations circulent librement dans un monde aujourd'hui sans frontières, ce qui peut un jour être pénalisant, dans la mesure où le droit à l'oubli n'est pas évident.
Aussi, si nous ne sommes pas vigilants, il sera aisé de porter atteinte de manière irréversible, à notre espace intime et à nos droits fondamentaux.

Mais internet n'est pas un espace de non-droit puisque le responsable d'un fichier ou d'un traitement de données personnelles d'un site web ou d'un forum de discussion, doit permettre aux internautes concernés par les informations collectées, d'exercer pleinement leurs droits.

Il doit les informer de son identité, de la finalité de son traitement (exemple : gestion clientèle, prospection commerciale, etc.), du caractère obligatoire ou facultatif des informations qu'il collecte, mais aussi des destinataires de ces informations, et de l'existence de droits pour les personnes fichées.

Cette information se fait en principe au moment où sont collectées les données (bon de commande, souscription d'un abonnement, enregistrement, etc.), et les mentions d'information à l'attention des personnes fichées doivent apparaître sur les formulaires utilisés pour collecter les données.

Quelles sont les principales obligations en cas de collecte d'informations à caractère personnel ?

Beaucoup ignorent encore que le fichage n'est pas libre et qu'il nécessite au préalable l'accomplissement de formalités déclaratives auprès de la CNIL, quand il ne s'agit pas d'obtenir une autorisation préalable, comme par exemple en cas de recours à des technologies biométriques.
Qu'il s'agisse d'établissements publics ou privés, la collecte d'informations personnelles est soumise à conditions, et la CNIL comme le juge veillent à leur respect.

En revanche, Internet ouvre la voie à la collecte d'information nominative par les traces que l'internaute laisse en surfant sur le web, sans que la collecte ne puisse être contrôlée (cookies, adresse IP, téléchargements, ou encore participation à des forums de discussion, messagerie instantanée, ou alimentation d'un blog).

La CNIL veille à la protection des données

Par délibération du 8 septembre 2011, la Commission nationale de l'informatique et des libertés (CNIL) a modifié l'article 69 de son règlement intérieur, afin de procéder à la mise en place de cette **nouvelle procédure de labellisation**.

Valable pour une **durée de 3 ans** renouvelable, le "**label CNIL**" est délivré aux produits ou aux procédures assurant la protection des personnes à l'égard du traitement des données à caractère personnel, conformément aux dispositions de la loi du 6 janvier 1978 modifiée.
L'objectif de la CNIL est de devenir "*un véritable régulateur économique*", et va en ce sens définir des référentiels et des règles précises encadrant la délivrance d'un label. Le premiers référentiels ont été publiés début novembre 2011.

Basée sur le **volontariat**, l'obtention de ce Label CNIL permet aux **entreprises** de **valoriser la qualité de leur service et/ou ses produits**, et aux utilisateurs, de bénéficier "*d'indicateurs de confiance dans les*

produits labellisés en leur permettant aisément d'identifier et privilégier les produits garantissant un haut niveau de protection de leurs données personnelles".
Notons toutefois que l'obtention de ce label donne lieu à la perception d'un droit, dont le montant devrait varier en fonction du produit ou des services pour lesquels le label est sollicité.

Les sociétés de services et les cabinets d'avocats qui proposent actuellement des services d'audits informatique et libertés - destinés aux organismes désireux de faire un bilan de leur politique de protection des données à caractère personnel - doivent elles aussi obtenir le label de la CNIL sur leurs procédures d'audit ou les formations informatique et libertés qu'ils proposent. L'examen de la CNIL porte sur le contenu, la forme et la méthodologie.

Exemples de produits ou services qui pourront être labellisés

- un moteur de recherche sur Internet,
- un service de transaction électronique en ligne pour un site de commerce électronique,
- un logiciel de gestion de données de santé utilisé au sein d'un hôpital,
- un logiciel de gestion du parc automobile d'une entreprise,
- un logiciel utilisé en matière de publicité comportementale,
- un dispositif de caméra de surveillance,
- etc.

Un constat : les français ont peur des fichiers

Selon une **étude d'octobre 2008** réalisée par l'institut de sondage Ipso à la demande de la CNIL, pour 61% des Français, l'existence de fichiers est perçue comme une atteinte à la vie privée. Ils sont mêmes un sur deux à éprouver des craintes concernant l'utilisation des fichiers. Leur inquiétude porte autant sur les fichiers d'Etat que sur les fichiers privés.

On remarque également que c'est la collecte d'informations personnelles sur Internet qui suscite le plus de crainte : 71% des personnes jugeant la protection de leur vie privée sur internet insuffisante, voire même "pas du tout satisfaisante" pour 37% d'entre eux.

C'est la tranche d'âge des 18-24 ans, c'est-à-dire les plus "gros consommateurs d'Internet", qui semble être la plus soucieuse dans ce domaine, puisque 78% des internautes de cette catégorie d'âge estiment que leur vie privée est insuffisamment protégée sur Internet. Néanmoins, ils n'entendent pas se détourner d'internet ou des nouveaux outils de communication.

De quoi avons-nous le plus peur ?

Sans avoir à faire référence aux films d'anticipation, certaines technologies qui s'avèrent particulières utiles, se révèlent aussi potentiellement dangereuses pour notre vie privée, que l'on en soit conscient ou pas. Il s'agit par exemple :

- des **traces** que l'on laisse sur le net, qui peuvent se retourner contre nous (à titre d'exemple, certains salariés qui critiquaient nominativement leur employeur et les pratiques de leur entreprise sur leur blog, ont été licenciés pour faute) ;
- des systèmes de **géolocalisation** : GPS des voitures, relais satellites des téléphones portables, bracelets électroniques (tant pour les détenus à la sortie de prison que pour les personnes âgées atteintes de la maladie d'Alzheimer, ou encore les bracelets équipant les nouveaux nés dans les cliniques) ;
- des **puces** de géolocalisation personnelles : implantées sous la peau, elles permettent de déterminer le lieu où se trouve une personne sur le globe ;

- des dispositifs de reconnaissance **biométrique** : ouverture ou accès contrôlés par la voix, les empreintes digitales, l'iris de l'oeil, biométrie comportementale ;
- des **codes d'accès** : qui n'a pas aujourd'hui peur de se faire pirater les codes d'accès à sa banque en ligne et se faire vider son compte en banque, ou encore pirater le numéro de sa carte bancaire ?
- des systèmes d'**enregistrement vidéo** : s'ils sont là pour nous protéger, l'exploitation des systèmes de vidéosurveillance à mauvais escient peut s'avérer extrêmement attentatoire à la vie privée ;
- des systèmes de **publicité ciblée** que ce soit sur internet ou dans certaines enseignes commerciales...

Quelles solutions pour l'avenir ?

Conscients de l'importance de la question de la protection des données personnelles, la CNIL a organisé à la mi-octobre 2008 avec son homologue allemand, une conférence mondiale sur la protection de la vie privée dans un monde sans frontières, au cours de laquelle elle est revenue sur le développement de la protection des données ces 30 dernières années. Elle a aussi présenté ce qu'elle estime être "*les défis auxquels nous devons faire face ensemble*" dans les années à venir. Bref, la CNIL espère faire évoluer la législation en la matière avant que la protection de la vie privée ne puisse plus être garantie.

Comment protéger les données personnelles figurant dans un Smartphone ?

La CNIL recommande aux utilisateurs de Smartphones d'être davantage vigilants à la **protection** de leurs **données personnelles**, et de suivre certains conseils pour maîtriser les données enregistrées dans le téléphone et **renforcer** sa **sécurité**.

Bonnes pratiques vis-à-vis des Smartphones :

- **ne pas enregistrer** dans le smartphone, des informations confidentielles telles que des codes secrets (ex : accès à la banque en ligne), des codes d'accès (travail, ordinateur portable) afin de limiter les risques en cas de vol, piratage, ou usurpation d'identité ;
- ne pas désactiver le **code PIN** et changer celui proposé par défaut par le constructeur en préférant un code compliqué (éviter de choisir sa date de naissance) ;
- mettre en place un délai de **verrouillage** automatique du téléphone en veille. En effet, en plus du code PIN, ce dispositif permet de rendre inactif (verrouiller) le téléphone au bout d'un certain temps, ce qui empêche la consultation des informations contenues dans le téléphone en cas de perte ou de vol ;
- activer si possible le **chiffrement des sauvegardes** du téléphone en utilisant les réglages de la plate-forme avec laquelle le téléphone se connecte. Cette manipulation garantira que personne ne sera en mesure d'utiliser les données figurant dans le smartphone ;
- installer un **antivirus** quand cela est possible ;
- noter le **numéro IMEI** du téléphone pour le bloquer en cas de perte ou de vol. Ce numéro est communiqué par l'opérateur, mais il peut être relevé en tapant *#06# sur le téléphone. Il suffit alors de le conserver dans un endroit sûr ;
- **ne pas télécharger** d'application de sources inconnues en privilégiant les plates-formes officielles ;
- vérifier à quelles données contenues dans le smartphone **l'application** installée va avoir accès ;
- lire les **conditions d'utilisation d'un service** avant de l'installer, et ne pas hésiter à consulter l'avis des autres utilisateurs ;
- régler les paramètres au sein du téléphone ou dans les applications de **géolocalisation** (Twitter, Foursquare, Plyce...) afin de toujours contrôler quand et par qui l'appareil peut être géolocalisé ;
- **désactiver** le GPS ou le WIFI après utilisation de l'application de géolocalisation ;
- et pour la santé (limiter l'exposition aux radiofréquences), éteindre le smartphone la nuit, ne pas le laisser de manière continue près de soi, ne pas le porter en permanence à la ceinture ou dans une poche.