# Modifications substantielles de la loi Informatique et libertés

publié le **14/10/2011**, vu **4499 fois**, Auteur : Murielle Cahen

**En quoi la réforme de la loi Informatique et libertés contribue à la protection des internautes ? En quoi consiste le recueil préalable obligatoire de l'autorisation des cookies par l'utilisateur ? Qu'apporte l'ajout d'une obligation de notification à la Cnil des violations da la sécurité des données?**

## I – La gestion des cookies : l'obligation d'obtenir le consentement préalable de l'utilisateur

### A/ Le principe d'une exigence d'autorisation préalable à l'installation des cookies

Parmi les mesures préconisées par l'ordonnance du 24 août 2011, il convient dans un premier temps de préciser celle relative aux cookies, modifiant l'article 32 II de la loi Informatique et libertés.

Les cookies sont des petits fichiers « .txt » installés sur le disque dur du terminal de connexion, à la demande du site consulté par un navigateur. Ils permettent au site de déterminer si l'utilisateur du même navigateur s'est déjà connecté auparavant. Si la plupart des navigateurs sont configurés pour accepter les cookies, il est possible de les reconfigurer pour qu'ils les refusent.

Ainsi, même avant l'ordonnance du 24 août 2011, les utilisateurs pouvaient tout à fait s'opposer aux cookies en reconfigurant leur navigateur, mais ils ne pouvaient les refuser que postérieurement à l'installation desdits cookies, selon un système d' « opt out ».

La jurisprudence veillait à garantir le respect de cette faculté de refus, comme en témoigne un jugement récent rendu par le Tribunal de grande instance de Montpellier, le 28 octobre 2010, pour l'affaire M$^{me}$ C. c/ Google France et Inc. Les juges du fond y affirment qu'il incombe aux moteurs de recherche « d'aménager la possibilité d'un retrait a posteriori des données à caractère personnel ».

Désormais, depuis le 24 août, l'utilisation de cookies doit être préalablement soumise à l'acceptation de l'utilisateur, selon un système d'« opt in ». De même, il est imposé aux responsables du traitement de données personnelles de fournir des informations « claires et complètes », quant à la finalité des cookies et aux moyens de s'y opposer, avant de recueillir le consentement de l'utilisateur.

Ce nouvel article 32 II de la loi Informatique et libertés apparaît comme la transposition directe du Paquet Télécom de 2009, qui modifiait lui-même la directive européenne du 7 mars 2002 sur le service universel et les droits des utilisateurs au regard des réseaux et des services de

communications électroniques ; et celle du 12 juillet 2002 sur le traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des communications électroniques.

### B/ Les limites de l’exigence d’autorisation préalable aux cookies

Il convient, tout d’abord, d’observer que les exceptions à l'obligation de recueillir un accord préalable, déjà présentes dans l'ancien article 32 de la loi Informatique et libertés, sont maintenues pour certains cookies. En effet, sont exclus du champ de l’obligation d’obtention du consentement préalable de l’utilisateur, les cookies qui ont pour « finalité exclusive de permettre ou faciliter la communication par voie électronique » d’une part, ainsi que les cookies qui sont « strictement nécessaires à la fourniture d'un service expressément demandé par l'internaute ».

Deuxièmement, les moyens techniques permettant de satisfaire à ces obligations d’autorisation préalable semblent restés à déterminer. Le texte précise seulement que l'accord « peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif sous son contrôle ».

L'opérateur doit alors modifier les conditions d'utilisation de son site, puis une fois ces modifications portées à l'attention de l'internaute, elles devront expressément être acceptées par lui.

En pratique, il est d’ores et déjà  possible de penser que seules deux solutions permettent au responsable du traitement de recueillir ce consentement. L’installation  de cookies peut être soumise à un mécanisme systématique de « pops up », où chaque connexion à un site serait conditionnée à l’acceptation ou non par l’utilisateur de l’installation de cookies par l’exploitant. Toutefois, l’impératif de fluidité de la navigation conduit à  préférer une seconde solution de configuration du navigateur par l’utilisateur, en responsabilisant ce dernier face à la gestion de ses données privées.

## II – Les failles de sécurité : l’obligation de notification de la violation des données de l’utilisateur

### A/ Le principe d’une obligation de notification des violations de la sécurité des données

L'ordonnance du 24 août 2011 ajoute, dans un second temps, un article 34 bis dans la Loi Informatique et libertés, instituant une obligation de notification à la CNIL des cas de violation de la sécurité des données personnelles (« Data Security Breach »).

La violation de données personnelles est constituée par toute faille de sécurité du système d'information entraînant, de façon accidentelle ou illicite, l’altération, la destruction, la perte, la divulgation, ou encore l'accès non autorisé à des données personnelles par un tiers.

Jusqu’à maintenant, le responsable du traitement était tenu de prendre « toutes précautions utiles » pour garantir la sécurité et la confidentialité des données.

Avec l’ordonnance du 24 août 2011, cette mention est remplacée par celle plus précise de « mesures adéquates », qui implique d’adapter les mesures de sécurité selon le type de données.

De plus, s’inspirant des dispositions du Paquet Télécom qu’elle transpose, l’ordonnance introduit la notion de « violation des données » dans la loi Informatique et libertés.

Ainsi, en cas d’atteinte aux données à caractère personnel, le responsable du traitement a dorénavant l’obligation d’avertir « sans délai » la CNIL. Dans l’hypothèse où cette atteinte est susceptible d’affecter les données d’une ou de plusieurs personnes physiques, la CNIL pourrait également exiger du responsable du traitement qu’il en avertisse ces personnes.

La mesure de l’ordonnance vise à obliger  les responsables du traitement des données personnelles, dans le cadre de leur « fourniture de services de communications électroniques ouverts au public ». Le terme de « services de communications électroniques » s’entend des prestations  qui consistent principalement en la fourniture de ces services, et non leur édition ou encore leur distribution.

En pratique, le fournisseur doit donc établir un inventaire des violations constatées qu'il tient à disposition de la CNIL. Il est alors tenu d’y soulever les modalités des violations constatées, les effets provoqués par cette violation et les mesures entreprises pour y remédier.

En cas de méconnaissance de l’obligation de notification à la CNIL ou à l’intéressé, la sanction du responsable de traitement est fixée à une peine pouvant aller jusqu'à cinq ans d’emprisonnement et à 300 000 euros d'amende, conformément à l’article 226-17-1 du Code pénal.

## B/ Les limites à l’obligation de notification des violations de la sécurité des données

L’ordonnance du 24 août pose toutefois une exception à l'obligation de notification à l'intéressé de la violation de la sécurité de ses données. En effet, elle n’est pas réputée nécessaire si la CNIL a constaté que des remèdes appropriés ont été mis en œuvre par le fournisseur. Il peut notamment s’agir de cryptage des données  qui ont pour finalité de rendre les données incompréhensibles.

De plus, au regard du texte même de l’ordonnance, celui-ci ne semble pas préciser les modalités de notification. Seule la directive européenne précitée du 12 juillet 2002 fait encore figure de référence sur ce point. Selon elle, la notification faite à l'abonné ou à la personne physique doit au minimum mentionner la nature de la violation de données personnelles, les points de contact auprès desquels des informations supplémentaires peuvent être obtenues, ainsi qu’une recommandation des mesures à adopter afin d'atténuer les conséquences de la violation de données personnelles.

Cette directive apparaît alors encore comme la seule garantie d’une description des conséquences de la violation de données personnelles, et des mesures proposées ou prises pour y remédier, assurant alors à l’obligation de notification des failles de sécurité à la CNIL une réelle efficacité.