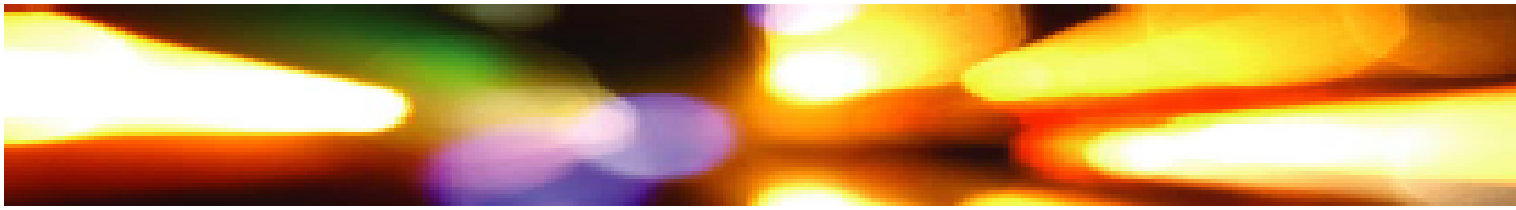
Flash IT
Décembre 2011

Stehlin & Associés
Association d'avocats au barreau de Paris



A La Une: transposition en droit français du « Paquet Télécom » : Ordonnance n°2011-1012 du 24 août 2011 relative aux communications électroniques : renforcement de la protection des consommateurs et de leurs données personnelles

Par une ordonnance en date du 24 août 2011, les directives européennes dites « Paquet Télécom » n°2009/136/CE et n°2009/140/CE, ont été transposées en droit français.

Cette Ordonnance contient diverses mesures modifiant le Code des postes et des communications électroniques, le Code de la consommation, le Code pénal et la Loi Informatique et Libertés en date du 6 janvier 1978, telle que modifiée.

Les modifications portent notamment sur le renforcement des obligations des fournisseurs de services de communications électroniques, le renforcement de l'information des abonnés ou utilisateurs d'un service de communications électronique en cas d'utilisation de cookies, la lutte contre les atteintes à la vie privée, au secret des correspondances et à la sécurité des systèmes d'information dans le domaine des communications électroniques ou encore sur une meilleure gestion des fréquences radioélectriques.

Le présent Flash n'a pas pour objet de faire une étude exhaustive de l'Ordonnance mais se limite à des observations sur deux questions essentielles relatives au renforcement de la protection des données personnelles.

1. **Utilisation de cookies[1] : l'introduction de l'opt-in**

Par cette Ordonnance, la France reteint pour les cookies le système de l'opt-in jusque là seulement réservé à la prospection commerciale « *au moyen d'automates d'appel, d'un télécopieur ou de courriers électroniques*[2] ». Désormais, l'utilisation de cookies sera soumise au consentement préalable de l'utilisateur ou de l'abonné en ligne.

[1] Il s'agit des informations qui sont déposées par un site Internet sur le terminal d'un utilisateur pour différentes finalités dont l'observation de la navigations des utilisateurs.
[2] Ancienne rédaction de l'article L. 34-5 du Code des Postes et des Communications électroniques

Stehlin & Associés
48, avenue Victor Hugo
75116 Paris
+33 1 44 17 07 70
Contact : Frédéric Lecomte
f.lecomte@stehlin-legal.com

La rédaction de l'article 32 II de la Loi Informatique et Libertés a ainsi été modifiée : « *ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son accord qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle* ».

L'accord préalable doit être spécifique et ne peut porter que sur un traitement précis et une finalité déterminée (nouvel article 32 II de la Loi Informatique et Libertés). Il ne peut dès lors être global pour tous les cookies à venir.

Le mécanisme de recueil de l'accord de l'utilisateur peut prendre plusieurs formes sur le site concerné :

- L'apparition d'une bannière en haut de la page du site ;
- zone de demande de consentement en surimpression (pop up) sur la page ;
- ou encore case à cocher lors de l'inscription à un service en ligne[3].

Cette acceptation doit être accompagnée de l'information de l'abonné ou utilisateur que ce dernier peut exercer postérieurement son droit d'opposition à cette utilisation. Ainsi, la CNIL a précisé qu'un paramétrage général autorisant tous les cookies ne pourra constituer une acceptation valable de la part de l'abonné ou de l'utilisateur. Ne sont néanmoins pas concernés les cookies qui :

- ont « *pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;*
- *ou qui sont strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur*[4]. »

Il s'agit notamment :

- des cookies utilisés comme « panier d'achat » sur un site marchand ;
- des cookies de « session utilisateur » permettant de lier les actions d'un utilisateur lorsque cela est nécessaire pour lui fournir le service qu'il demande ;
- des cookies qui ont pour unique finalité de contribuer à la sécurité du service demandé par l'utilisateur ;
- ou encore des cookies permettant d'utiliser la langue parlée par l'utilisateur ou autres préférences nécessaires à la fourniture du service demandé[5].

Par conséquent, dès lors que sont utilisés des cookies autres que ceux mentionnés ci-dessus, une simple mention dans les Conditions Générales d'Utilisation d'un site Internet de l'existence de ces cookies et du droit pour l'utilisateur de s'y opposer n'est plus suffisante. Ces Conditions Générales ne permettent pas d'obtenir le consentement préalable des utilisateurs à l'installation de cookies. Les sociétés utilisatrices de cookies devront ainsi et désormais se conformer aux nouvelles obligations imposées par le Code des postes et des communications électroniques et la Loi Informatique et Libertés et organiser la collecte des consentements de manière éclairée.

***

[3] Notice explicative disponible sur le site de la CNIL relative à la transposition du « Paquet Télécom » et les modifications apportées à l'utilisation de cookies

[4] Article 32 II de la Loi Informatique et Libertés

[5] Notice explicative disponible sur le site de la CNIL relative à la transposition du « Paquet Télécom » et les modifications apportées à l'utilisation de cookies

Stehlin & Associés
48, avenue Victor Hugo
75116 Paris
+33 1 44 17 07 70
Contact : Frédéric Lecomte
f.lecomte@stehlin-legal.com

2. Obligation de notification en cas de pertes de données pour les fournisseurs de services de communications électroniques au public

L'Ordonnance modifie également l'article 34 de la Loi Informatique et Libertés et ajoute un nouvel article 34 bis. Cet article crée une nouvelle obligation de notification à la charge des fournisseurs de services de communications électroniques (essentiellement opérateurs déclarés auprès de l'ARCEP) en cas de violation de données personnelles, notamment en cas de faille de sécurité ayant entraîné de manière accidentelle, l'atteinte, la perte ou l'accès non autorisé aux données personnelles des abonnés ou utilisateurs.

Cette violation est définie comme « *toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques* ». En cas de violation de ces données, le fournisseur devra en informer la CNIL sans délai.

Cette nouvelle obligation implique pour les fournisseurs une obligation de tenir un registre récapitulant les violations de données personnelles et les solutions mises en place pour y remédier. Ce registre doit être mis à la disposition de la CNIL (article 34 bis III de la Loi Informatique et Libertés).

L'article 34 bis prévoit également une obligation de notification aux personnes physiques concernées lorsque cette violation « *peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique* ».

Néanmoins les fournisseurs peuvent s'exonérer de cette notification à l'intéressé lorsque la CNIL constate que « *des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation* ».

En cas de violation de ces obligations, le fournisseur peut faire l'objet d'une amende de 300.000 euros (1.500.000 euros pour une personne morale) et de cinq ans d'emprisonnement (article 226-17-1 du Code pénal) ainsi que de sanctions administratives. Cette obligation de notification peut par ailleurs être lourde de conséquences pour les fournisseurs, notamment en termes de réputation.

Les fournisseurs devront ainsi prendre les mesures adéquates en interne (notamment audits internes) pour renforcer la sécurité des données et adopter des mesures de protection « appropriées » pour rendre les données « *incompréhensibles à toute personne non autorisée à y avoir accès* ».

Nous pouvons, néanmoins, nous interroger sur l'efficacité de ces mesures et sur la définition de « mesure appropriée » alors que les pirates aguerris disposent la plupart du temps d'un temps d'avance technologique leur permettant de contourner les systèmes de cryptage utilisés par les fournisseurs.

Seule l'analyse des futures décisions de la CNIL sanctionnant des prestataires de services de communications électroniques au public n'ayant pas respecté les nouvelles dispositions de la Loi Informatique et Libertés, permettra de déterminer avec plus de précisions la définition de « mesures appropriées » et l'étendue de ces nouvelles obligations.

***

Stehlin & Associés
48, avenue Victor Hugo
75116 Paris
+33 1 44 17 07 70
Contact : Frédéric Lecomte
f.lecomte@stehlin-legal.com