

Internet : Des modifications substantielles de la loi Informatique et libert s
Internet

PostÃ© par : JulieM

Publié le : 21/9/2011 13:30:00

La France a transposé le « le Paquet Telecom » (directive 2009/136 du 25 novembre 2009) par ordonnance 2011-1012 du 24 août 2011 publiée au journal officiel le 26 août 2011.

Hervé Gadabou, avocat associé chez Courtois Lebel, explique comment cette ordonnance du 24 août 2011 modifie notamment certaines dispositions de la loi n°78-17 du 6 janvier 1978 Informatiques, Fichiers et Libertés.

Les cookies : l'acceptation préalable de l'utilisateur

L'ordonnance du 24 août 2011 relative aux communications électroniques modifie l'article 32 II de la Loi n°78-17 du 6 janvier 1978. Cet article impose de nouvelles contraintes aux responsables de traitement de données personnelles, s'agissant des cookies.

D'ailleurs, l'utilisation de cookies doit être préalablement soumise à l'acceptation de l'utilisateur (système dit de l'« opt in »). En d'autres termes, les opérateurs internet responsables de traitement de données personnelles doivent obtenir le consentement des internautes, après leur avoir donné des informations « claires et complètes » (finalité des cookies et description des moyens pour s'y opposer), avant d'implanter des cookies dans leurs systèmes.



Pour rappel, jusqu'À la publication de l'ordonnance du 24 aoÃ«t 2011, les utilisateurs pouvaient s'y opposer, mais postÃ©rieurement À l'installation dudit cookie (systÃ«me dit de l' « opt out »).

Les exceptions à l'obligation d'obtenir l'accord préalable de l'intéressé, d'aj
prévoies dans l'ancien article 32, sont maintenues pour :

Les cookies qui ont pour finalit  exclusive de permettre ou faciliter la communication par voie  lectronique et

Les cookies qui sont « strictement nécessaires » à la fourniture d'un service immédiatement

demandé par l'internaute ».

Les moyens techniques permettant de satisfaire à ces obligations restent à déterminer. En effet, le texte précise seulement que l'accord « peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle ».

L'opérateur doit en tout état de cause modifier les conditions d'utilisation de son site pour remplir son devoir d'information, en intégrant les nouvelles dispositions imposées par l'ordonnance. Ces modifications devront être portées à l'attention de l'internaute et expressément acceptées par ce dernier (et non tacitement), et ce avant même « toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ».

Il conviendra de suivre l'évolution des recommandations techniques, conseils et mentions d'informations types publiées par la CNIL, laquelle ne semble pas encore avoir mis à jour son site internet.

L'obligation de notification

L'article 38 de l'ordonnance du 24 août 2011 intègre un article 34 bis dans la Loi n°78-17 du 6 janvier 1978 qui institue une obligation de notification en cas de violations de données personnelles (Data Security Breach).

⚡ Qui est concerné ?

L'obligation de notification concerne les données traitées dans le cadre de la « fourniture de services de communications électroniques ouverts au public », ce incluant également les fournisseurs « prenant en charge les dispositifs de collecte de données et d'identification ».

Pour rappel, on entend par « services de communications électroniques » les prestations consistant entièrement ou principalement en la fourniture de communications électroniques. Ne sont pas visés les services consistant à éditer ou à distribuer des services de communication au public par voie électronique.

⚡ Que recouvre la notion de « violation de données personnelles » ?

Selon l'ordonnance, la violation de données personnelles constitue toute situation de violation de la sécurité du système d'information entraînant, de façon accidentelle ou illicite :

- la destruction,
- la perte,
- l'altération,
- la divulgation, ou encore
- l'accès non autorisé à des données personnelles par un tiers.

Ces éléments ne sont pas cumulatifs.

¶ Quand notifier ?

L'obligation de notification doit être faite « sans délai ».

¶ A qui notifier ?

En cas de violation, l'ordonnance prévoit une notification sans délai :

- la CNIL
- aux intéressés

L'obligation sans délai de notification aux intéressés par le fournisseur est obligatoire dès lors que cette violation est susceptible de porter atteinte aux données personnelles ou à la vie privée de l'abonné ou d'une autre personne physique.

Exceptions :

L'obligation de notification à l'intéressé n'est pas nécessaire si la CNIL a constaté que des mesures de protections appropriées ont été mises en œuvre par le fournisseur (cryptage des données par exemple, rendant les données incompréhensibles).

À défaut de telles mesures, la CNIL peut mettre en demeure le fournisseur d'informer également le ou les intéressés de la violation constatée.

¶ Quelles sont les modalités de forme et de fond des notifications ?

Le texte de l'ordonnance ne précise pas les modalités de la notification.

Il convient donc de se référer à l'article 3 de la directive 2002/58/CE du 12 juillet 2002, sur ce point plus précis :

La notification faite à l'abonné ou à la personne physique doit indiquer, au minimum :

- la nature de la violation de données personnelles
- les points de contact auprès desquels des informations supplémentaires peuvent être obtenues
- une recommandation des mesures à adopter afin d'atténuer les conséquences négatives éventuelles de la violation de données personnelles.

La notification faite à la CNIL doit, selon la directive, décrire les conséquences de la violation de données personnelles, et les mesures proposées ou prises pour y remédier.

¶ Quelles obligations associées ?

Le fournisseur doit désormais établir un inventaire des violations constatées qu'il tient à disposition de la CNIL.

Cet inventaire doit comprendre :

- les modalités des violations constatées ;

- les effets provoqu s par cette violation ;
- les mesures entreprises pour y rem dier.

   Quelles sanctions en cas de d faut de notification ?

L'absence de notification est punie d'une peine pouvant aller jusqu'  5 ans de prison et 300.000 euros d'amende (insertion d'un nouvel alin a   l'article 226-17 du code p nal).