ASSEMBLÉE NATIONALE

9 février 2013

SÉPARATION ET RÉGULATION DES ACTIVITÉS BANCAIRES - (N° 707)

Commission	
Gouvernement	

Rejeté

AMENDEMENT

N º 278

présenté par
M. Thévenoud, M. Hammadi, M. Guillaume Bachelay, M. Franqueville, Mme Got, Mme Maquet, Mme Marcel, Mme Mazetier, M. Pellois et M. Villaumé

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 18 , insérer l'article suivant:

La section 4 du chapitre IV du titre I^{er} du Livre III du code monétaire et financier est complétée par une sous-section 6 ainsi rédigée :

« Sous-section 6

« Intrusions malveillantes dans les serveurs contenant des données à caractère personnel bancaires ou de carte bancaire

« *Art. L. 314-17.* – I. – Pour l'application du présent article, on entend par violation de données à caractère personnel bancaires ou de carte bancaire 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 ces données.

« II. – En cas de violation de données à caractère personnel bancaires ou de carte bancaire, le professionnel avertit, au plus tard sous vingt-quatre heures, la Commission nationale de l'informatique et des libertés. Lorsque cette violation peut porter atteinte aux données à caractère personnel bancaires ou de carte bancaire d'une personne physique, le professionnel avertit également l'intéressé, au plus tard sous vingt-quatre heures.

« III. – Chaque professionnel tient à jour un inventaire des violations de données à caractère personnel bancaires ou de carte bancaire, notamment de leurs modalités, de leur effet et des mesures prises pour y remédier et le conserve à la disposition de la Commission nationale de l'informatique et des libertés. »

EXPOSÉ SOMMAIRE

Cet amendement tend à instaurer une obligation pour tous les professionnels d'informer leurs clients de toute attaque réussie de pirates informatiques visant leurs données bancaires ou de carte bancaire.

L'Observatoire national de la délinquance et des réponses pénales a publié en janvier 2013 un rapport accablant sur la hausse des fraudes à la carte bancaire sur internet. Fin 2012, un autre organisme, l'Observatoire de la sécurité des cartes de paiement, indiquait que le commerce à distance représentait 61 % de la fraude pour seulement 8,4 % des transactions. Or, dans 70 % des cas, ce sont les consommateurs qui ont détecté la fraude, les banques n'ayant prévenu les clients que dans 22 % des cas. Il est crucial de prendre des mesures contre ce phénomène qui met en danger les consommateurs, mais aussi leur confiance dans le commerce en ligne.

Une part des détournements de données de cartes bancaires à des fins de fraude est due aux attaques de serveurs informatiques stockant les données bancaires ou de carte bancaire. Cependant, les gestionnaires des serveurs attaqués n'ont aujourd'hui aucune obligation d'informer les clients touchés, les empêchant de prendre les mesures de précaution nécessaires (surveillance de leurs comptes, opposition et remplacement de la carte, etc.). Il convient donc d'instaurer une telle obligation afin que les clients, alertés, puissent prendre leurs dispositions. Pour être plus efficaces, ces alertes doivent être personnalisées (envoi de SMS, de mails) et non pas constituer une simple information sur le site du professionnel, consulté très aléatoirement par les consommateurs.

Cette mesure s'inscrit dans la droite ligne des propositions de la Commission européenne en matière de protection des données.