ASSEMBLÉE NATIONALE

14ème législature

commerce électronique

Question écrite n° 32196

Texte de la question

M. Arnaud Robinet attire l'attention de M. le ministre de l'intérieur sur les chiffres révélés par le rapport de l'Observatoire de la sécurité des cartes de paiement, présidé par Christophe Noyer, également gouverneur de la Banque de France. Il apparaît que le taux de fraude sur les paiements et les retraits par carte bancaire a de nouveau légèrement augmenté en France, atteignant 0,080 % du montant des transactions effectuées, soit 450,7 millions d'euros, contre 0,077 % en 2011. Ainsi, 650 000 Français ont été victimes de fraudes à la carte bancaire, soit 2,5 % des ménages, selon une étude de l'Observatoire national de la délinquance et des réponses pénales. Il souhaiterait connaître les actions engagées par le Gouvernement pour garantir une meilleure sécurité lors des paiements sur internet.

Texte de la réponse

La sécurisation des transactions par carte bancaire est une préoccupation constante des pouvoirs publics, notamment de la Banque de France qui est chargée « d'assurer la sécurité des moyens de paiement » en application de la loi du 15 novembre 2001 relative à la sécurité quotidienne. Il y a lieu de rappeler que le cadre juridique du code monétaire et financier permet au porteur de la carte de ne pas voir sa responsabilité engagée en cas d'opération frauduleuse sur celle-ci. Les forces de sécurité de l'Etat sont engagées dans la lutte contre les opérations frauduleuses sur ces instruments de paiement (falsification, contrefaçon...), qui affectent nos concitoyens dans leur vie quotidienne. Le développement d'Internet s'accompagne en effet de nouvelles méthodes de délinquance, en particulier par l'appropriation frauduleuse des données confidentielles de personnes effectuant des achats en ligne. Diverses actions sont menées. Une plate-forme téléphonique d'information et de prévention sur les escroqueries, dénommée « Info-escroqueries », est à la disposition du public pour répondre aux interrogations des victimes et les guider dans leurs démarches. Un site (www. internet-signalement. gouv. fr) est à la disposition des particuliers et des professionnels pour signaler tout contenu illicite de l'Internet et diffuser des messages de prévention. Ces signalements, qui peuvent être le point de départ d'enquêtes pénales, sont traités par la plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS), placée au sein de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de la direction centrale de la police judiciaire. Cet office central dispose d'un groupe opérationnel d'enquête chargé de lutter contre les escroqueries sur Internet (fraude à la carte de paiement utilisée pour les ventes à distance par exemple). Au regard du caractère transnational des affaires, la lutte contre cette délinquance fait l'objet d'une coopération avec différents pays, par exemple dans le cadre d'Europol. Sur le plan juridique, la répression de l'infraction d'utilisation d'instruments de paiement falsifiés (cartes de paiement, etc.), si elle est commise en bande organisée, est plus sévère (dix ans d'emprisonnement et un million d'euros d'amende) depuis la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, qui a par ailleurs créé une incrimination relative à l'utilisation frauduleuse de données à caractère personnel de tiers sur Internet. En matière de prévention, l'OCLCTIC a renforcé son partenariat avec les professionnels chargés de la production d'automates de paiement, la fédération bancaire française et le groupement d'intérêt économique des cartes bancaires.

L'OCLCTIC siège, en outre, au sein de l'Observatoire de la sécurité des cartes de paiement. La prévention, notamment technique, est essentielle et le dernier rapport de l'Observatoire de la sécurité des cartes de paiement fait état de réelles avancées en matière de sécurisation des opérations de paiement par carte bancaire via Internet mais constate que seulement 23 % des transactions de paiement par ce vecteur sont sécurisées par des dispositifs d'authentification « non rejouable » et partant, de la technologie « 3D-Secure ». Le déploiement croissant de ce procédé auprès des e-commerçants reste donc une priorité pour l'Observatoire de la sécurité des cartes de paiement. Une sécurisation croissante exige aussi une poursuite des actions engagées en sensibilisant encore davantage le porteur de carte, les banques, les e-commerçants et commerçants afin d'accroître le niveau de coopération entre ces acteurs. Les axes d'amélioration reposent également sur une harmonisation des exigences sécuritaires par les autorités de régulation bancaire aux niveaux européen et international. Soucieux de développer un espace de confiance sur Internet, le Gouvernement a, par ailleurs, engagé une adaptation du dispositif de lutte contre la cybercriminalité. A la suite du séminaire gouvernemental sur le numérique du 28 février dernier, il a décidé de mettre en place un groupe de travail interministériel (Justice/Economie et Finances/ Intérieur/ Economie numérique) chargé d'élaborer une stratégie globale de lutte contre la cybercriminalité, prenant en compte la dimension internationale et européenne du phénomène, et portant notamment sur le développement des dispositifs d'aide aux victimes et de sensibilisation des publics. Ce groupe de travail a commencé à se réunir en juillet et devrait rendre son rapport d'ici à la fin de l'année.

Données clés

Auteur : M. Arnaud Robinet
Circonscription : Marne (1re circonscription) - Les Républicains
Type de question : Question écrite
Numéro de la question : 32196
Rubrique : Ventes et échanges
Ministère interrogé : Intérieur
Ministère attributaire : Intérieur

Date(s) clée(s)

Question publiée au JO le : 9 juillet 2013, page 7123
Réponse publiée au JO le : 17 septembre 2013, page 9737