



ASSEMBLÉE NATIONALE

13ème législature

cartes bancaires

Question écrite n° 98041

Texte de la question

M. Bernard Perrut appelle l'attention de M. le ministre de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration sur la progression dans l'utilisation des cartes bancaires par Internet par l'abus de la transmission de renseignements confidentiels qui figurent sur la carte elle-même et permettent ainsi de s'en servir pour effectuer des achats impunément. Les fraudes se multiplient sans contrôle. Il lui demande si des mesures peuvent être imaginées et multipliées pour assurer une plus grande sécurité dans ce domaine.

Texte de la réponse

Le développement de l'Internet offre des opportunités à une criminalité en constante évolution. De nouvelles formes de délinquance affectent ainsi les transactions par carte bancaire, par exemple l'appropriation frauduleuse des données confidentielles des personnes effectuant en ligne des achats ou des vérifications sur leur compte bancaire. Pour y répondre, les moyens humains et juridiques des forces de sécurité sont renforcés et leurs méthodes d'investigation modernisées. Un plan d'action de lutte contre la cybercriminalité, qui incombe à titre principal à 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, a été engagé dès 2008 et vise notamment à combattre les escroqueries sur l'Internet. Plusieurs structures ont été mises en place au sein de cet office. Un groupe d'enquête spécifiquement chargé de lutter contre les escroqueries sur l'Internet et le « carding » (trafic de données bancaires sur l'Internet) a été institué pour assurer une centralisation opérationnelle des affaires, identifier les groupes criminels et diligenter des procédures poursuivies le cas échéant dans le cadre de l'entraide judiciaire. Depuis 2009, une plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) permet aux internautes et aux professionnels de l'Internet de signaler (sur le site www.internet-signalement.gouv.fr) tout contenu illicite sur le Web (notamment les sites de « carding »). En 2010, la plate-forme a traité près de 78 000 signalements, dont 56 % concernant des escroqueries commises sur l'Internet. Les policiers et les gendarmes travaillant au sein de PHAROS vérifient et recoupent les signalements, dont ceux portant sur des escroqueries, puis, s'ils sont caractérisés, les adressent pour enquête à un service de police ou de gendarmerie. La plate-forme diffuse, par ailleurs, des messages de conseils et de prévention aux internautes. L'exploitation de ces signalements a permis d'engager, en 2010, plus de 700 enquêtes sur le territoire français et près de 2 000 signalements ont été adressés à des États étrangers, par le canal d'Interpol, afin de solliciter la fermeture de sites illicites ou la suppression de contenus. Une plate-forme téléphonique « Info escroqueries », composée de policiers et de gendarmes, a également été créée, avec pour mission la prévention et l'information du public sur toutes les formes d'escroquerie. En 2010, elle a traité 15 000 appels. Ce dispositif a permis de faire connaître à la population les principaux modes opératoires utilisés par les malfaiteurs ainsi que les moyens de s'en prémunir et facilite les investigations des forces de sécurité. Un partenariat a également été développé entre le ministère de l'intérieur et l'association « Signal Spam », qui regroupe des acteurs publics et privés, afin d'améliorer la lutte contre les « spams », vecteurs majeurs de propagation d'infractions sur le Web. Le site www.signal-spam.fr met notamment à la disposition des internautes un guide de bonnes pratiques. Au-delà, la lutte contre la cybercriminalité exige une approche globale. À

l'initiative de la France, il a par exemple été décidé de créer dans le cadre de l'Union européenne une plateforme européenne de signalement des infractions relevées sur l'Internet (Internet Crime Reporting Online System), programmée pour 2013. Limitée au départ aux contenus pédopornographiques, elle devrait être élargie à d'autres infractions. Une active coopération internationale est également menée par le canal d'Interpol ou dans le cadre de relations bilatérales. Ce dispositif global a permis une diminution de 6,58 % du nombre de falsifications et d'usages frauduleux de cartes de crédit constatés par les services de police et de gendarmerie en 2009 et de 7,34 % en 2010. S'agissant des escroqueries commises sur l'Internet, les données disponibles à ce jour (concernant la police nationale) font apparaître une baisse de 16,79 % des faits constatés au cours des neuf premiers mois de l'année 2010 (8 219 faits constatés, contre 9 878 au cours de la même période 2009). Déterminé à ce que l'Internet ne devienne pas un espace de non-droit, le ministre de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration a fait inscrire dans la loi d'orientation et de programmation pour la performance de la sécurité intérieure, adoptée par le Parlement le 8 février 2011, de nouvelles dispositions qui permettront de mieux lutter contre les cyber-escroqueries, avec la création d'une incrimination d'utilisation frauduleuse de données à caractère personnel de tiers sur l'Internet et la possibilité pour les enquêteurs de capter à distance et hors consentement du titulaire des données numériques trouvant dans un ordinateur ou transitant par celui-ci.

Données clés

Auteur : [M. Bernard Perrut](#)

Circonscription : Rhône (9^e circonscription) - Union pour un Mouvement Populaire

Type de question : Question écrite

Numéro de la question : 98041

Rubrique : Moyens de paiement

Ministère interrogé : Intérieur, outre-mer, collectivités territoriales et immigration

Ministère attributaire : Intérieur, outre-mer, collectivités territoriales et immigration

Date(s) clé(s)

Question publiée le : 18 janvier 2011, page 398

Réponse publiée le : 3 mai 2011, page 4549