



ASSEMBLÉE NATIONALE

14ème législature

cartes bancaires

Question écrite n° 4731

Texte de la question

M. Philippe Meunier attire l'attention de M. le ministre de l'intérieur sur l'augmentation de l'utilisation frauduleuse des cartes bancaires sur internet. Aussi, il lui demande quels dispositifs sont aujourd'hui mis en œuvre par l'État afin de lutter contre cette fraude ainsi que les mesures que le Gouvernement entend prendre afin d'assurer une plus grande sécurité dans les transactions en ligne.

Texte de la réponse

Le développement d'Internet offre des opportunités à une criminalité en constante évolution, qui recourt à des technologies sophistiquées et diversifie ses modes opératoires. De nouvelles formes de délinquance affectent ainsi les transactions par carte de paiement, par exemple l'appropriation frauduleuse des données confidentielles des personnes effectuant en ligne des achats ou des vérifications sur leur compte bancaire. L'action des services de police et de gendarmerie en la matière s'inscrit dans le cadre d'un plan de lutte contre la cybercriminalité, dont la mise en œuvre 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 ce titre, plusieurs structures ont été mises en place au sein de l'OCLCTIC. Un site internet (www.internet-signalement.gouv.fr) est à la disposition des particuliers et des professionnels pour signaler tout contenu illicite découvert sur le web. Ces signalements sont traités par une plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS), qui diffuse également des messages de prévention aux internautes. 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. Une plate-forme téléphonique d'information et de prévention sur les escroqueries, nommée « info-escroqueries », est également à la disposition du public, pour répondre aux interrogations des victimes et les guider dans leurs démarches. Par ailleurs, l'OCLCTIC s'est doté de groupes opérationnels d'enquête, chargés d'assurer une centralisation opérationnelle des affaires, d'identifier les groupes criminels et de diligenter des procédures, poursuivies le cas échéant dans le cadre de l'entraide judiciaire. L'un de ces groupes opérationnels est spécifiquement chargé de lutter contre les fraudes affectant les cartes de paiement et notamment le « carding » (trafic de données bancaires sur Internet). La cybercriminalité étant essentiellement un phénomène transnational, les coopérations bilatérales avec les pays « sources » sont également renforcées et la coopération opérationnelle internationale se développe, dans le cadre en particulier d'Europol et d'Interpol. Enfin, la prévention constitue un élément important de la lutte contre les escroqueries commises sur internet. Elle se traduit, par exemple, par diverses actions de prévention et d'information du public sur les risques de l'internet et par le développement de partenariats public/privé.

Données clés

Auteur : [M. Philippe Meunier](#)

Circonscription : Rhône (13^e circonscription) - Les Républicains

Type de question : Question écrite

Numéro de la question : 4731

Rubrique : Moyens de paiement

Ministère interrogé : Intérieur

Ministère attributaire : Intérieur

Date(s) clé(s)

Question publiée au JO le : [18 septembre 2012](#), page 5099

Réponse publiée au JO le : [30 octobre 2012](#), page 6170