



ASSEMBLÉE NATIONALE

13ème législature

cartes bancaires

Question écrite n° 117759

Texte de la question

M. Christian Vanneste attire l'attention de M. le ministre de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration sur l'utilisation frauduleuse de cartes de crédits. De nombreuses fraudes à la carte bancaire sont à déplorer. Mais désormais les fraudes ont lieu alors même que la victime est en possession de sa carte bancaire (retraits illégaux, achats sur internet). Il semblerait que ses vols sont à l'initiative d'informaticiens très pointus en Roumanie. Il souhaiterait avoir davantage de précisions sur ce sujet.

Texte de la réponse

Diverses formes de fraude affectent les transactions par carte bancaire, liées soit à la capture de données sur l'internet, soit à la falsification et à la contrefaçon des cartes de paiement. S'agissant des premières, les délinquants ont mis au point diverses techniques visant à s'approprier les données bancaires confidentielles des personnes effectuant des achats ou des vérifications sur leur compte bancaire. Pour répondre à cette délinquance, largement internationale, un plan de lutte contre la cybercriminalité, destiné notamment à lutter contre les escroqueries, a été engagé dès 2008. Sa mise en oeuvre 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. Plusieurs structures ont été mises en place au sein de l'OCLCTIC. Deux groupes d'enquête sont spécifiquement chargés de la lutte contre les escroqueries sur internet, l'un étant spécialisé dans le « carding » (trafic de données bancaires sur l'internet visant à la fabrication de fausses cartes de crédit), l'autre dans le « skimming » (piratage de données bancaires par copie des informations d'une piste magnétique d'une carte valide vers une autre carte). Une plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) permet depuis 2009 aux internautes et aux professionnels de signaler tout contenu illicite. Une plate-forme téléphonique d'information et de prévention sur les escroqueries, nommé « info-escroqueries », a également été créée en 2009. S'agissant de la falsification et de la contrefaçon des cartes de paiement, la principale technique des malfaiteurs pour la fabrication de cartes de paiement falsifiées est le « skimming ». Elle consiste à fabriquer des systèmes de piratage de distributeurs automatiques de billets, de distributeurs automatiques de carburant, de points de vente et de terminaux de paiement électroniques pour capturer les pistes magnétiques et les codes secrets des clients. La lutte contre cette criminalité est particulièrement difficile en raison de l'extrême mobilité des équipes de malfaiteurs chargés de la pose des matériels de piratage et de l'utilisation des cartes contrefaites dans des pays lointains. Face à cette menace en constante évolution, les enquêteurs spécialisés de l'OCLCTIC agissent dans le cadre du plan d'action de lutte contre la cybercriminalité lancé en 2008. Des documents techniques ont été diffusés aux services de police, de gendarmerie et des douanes, des actions de sensibilisation ont été menées, notamment auprès des services du ministère de la justice, et la formation des enquêteurs spécialisés (« investigateurs en cybercriminalité ») s'est renforcée dans les services de police et de gendarmerie. En matière de prévention, l'OCLCTIC a renforcé son partenariat avec la fédération bancaire française et le groupement d'intérêt économique des cartes bancaires en vue d'améliorer l'échange d'informations opérationnelles. La loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure renforce à cet égard les moyens de prévention et

de répression contre cette délinquance. L'utilisation d'instruments de paiement falsifiés comme les cartes de paiement, si elle est commise en bande organisée, est désormais plus sévèrement sanctionnée (dix ans d'emprisonnement et un million d'euros d'amende). La loi du 14 mars 2011 a par ailleurs créé une nouvelle incrimination relative à l'utilisation frauduleuse de données à caractère personnel de tiers sur l'internet et permet aux enquêteurs de capter à distance des données numériques se trouvant dans un ordinateur ou transitant par lui. Comme le relève le parlementaire, la Roumanie est, avec d'autres pays, par exemple d'Afrique, un des « pays sources » de cette criminalité. C'est la raison pour laquelle la France et la Roumanie ont engagé une coopération renforcée dans ce domaine, visant notamment à améliorer la réactivité des autorités judiciaires et policières roumaines, par le canal d'Interpol, dans le cadre de relations bilatérales ou au sein de l'Union européenne. Cette étroite coopération est déjà manifeste dans le cadre des procédures d'entraide judiciaire (plusieurs commissions rogatoires ont pu être exécutées en Roumanie en présence de policiers français) et a été renforcée par le détachement d'un policier roumain au sein de l'OCLCTIC.

Données clés

Auteur : [M. Christian Vanneste](#)

Circonscription : Nord (10^e circonscription) - Union pour un Mouvement Populaire

Type de question : Question écrite

Numéro de la question : 117759

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 : 13 septembre 2011, page 9713

Réponse publiée le : 14 février 2012, page 1393