ASSEMBLÉE NATIONALE

13ème législature

cartes bancaires

Question écrite n° 103700

Texte de la question

M. Francis Saint-Léger attire l'attention de M. le ministre de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration sur la fraude liée aux cartes de crédit. Il désire connaître les mesures de sécurité qu'il entend mettre en oeuvre afin de limiter cette fraude.

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 (par exemple, les sites de « phishing » ou de « carding »). La plate-forme, adossée au portail www.Internet-signalement.gouv.fr, est composée de cinq fonctionnaires de police et de cinq militaires de la gendarmerie. En 2010, elle a traité 77 646 signalements, dont 56 % concernant des escroqueries commises sur l'Internet (2 877 signalements pour des escroqueries de type « phishing »). Une plate-forme téléphonique d'information et de prévention sur les escroqueries, nommé « info-escroqueries », a également été créée en 2009. En 2010, elle a reçu 23 695 signalements, dont 321 pour des escroqueries à la carte bancaire et 1 021 pour des escroqueries de type « phishing ». Ce dispositif a permis de faire connaître à la population les principaux modes opératoires utilisés par les fraudeurs ainsi que les moyens de s'en prémunir. Sur le plan de la coopération internationale, la France a proposé, à l'occasion de sa présidence du Conseil de l'Union européenne en 2008, la création d'une plate-forme européenne de signalement des contenus illicites sur l'Internet (Internet Crime Reporting Online System), qui devrait être intégrée dans le cadre plùs large du futur « Centre européen de la cybercriminalité ». 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 (DAB), de distributeurs automatiques de carburant (DAC), 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. Selon le

groupement d'intérêt économique des cartes bancaires, le nombre de piratages de DAB et de points de vente est cependant stable en 2010. 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. L'OCLCTIC siège, en outre, au sein de l'Observatoire de la sécurité des cartes de paiement aux côtés des représentants des administrations concernées, du secteur bancaire et des associations de défense des consommateurs. Par ailleurs, le directeur général de la police nationale organise, en liaison avec la Fédération bancaire française et le groupement d'intérêt économique des cartes bancaires, une réunion semestrielle de coordination et d'échange d'informations. Ce partenariat concerne également les professionnels chargés de la production d'automates de paiement, afin d'améliorer la protection des distributeurs automatiques de billets de banques ou de carburant, la détection des dispositifs de captation et la diffusion de l'information vers les services de police. S'agissant des DAC, il convient de relever les progrès réalisés par les fournisseurs de modules de paiement, qui proposent désormais des modèles particulièrement sécurisés, rendant plus difficile, voire impossible, ce type de piratage (aucun piratage de DAC n'a été signalé en 2010). Dans sa dimension internationale, la lutte contre cette criminalité fait l'objet d'une coopération renforcée, en particulier avec la Roumanie. La France participe également à l'alimentation du fichier d'Europol consacré au « skimming » (AWF Terminal). Ce dispositif global a permis une diminution de 7,34 % du nombre de falsifications et d'usages frauduleux de cartes de crédit constatés par les services de police et de gendarmerie en 2010. La mobilisation des pouvoirs publics a par exemple largement contribué à l'éradication récente, en France, des escroqueries à la « Yes Card » (carte à puce, vierge à l'origine, dans laquelle des données spécifiques sont générées par calcul ou programmées par un « pirate », à partir du contenu d'une carte bancaire trouvée ou périmée). La mobilisation doit cependant rester totale, au regard des tendances négatives observées au cours du premier trimestre 2011. 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 1 Meuros 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.

Données clés

Auteur : M. Francis Saint-Léger
Circonscription : Lozère (1re circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 103700
Rubrique : Moyens de paiement
Ministère interrogé : Intérieur, outre-mer, collectivités territoriales et immigration
Ministère attributaire : Intérieur, outre-mer, collectivités territoriales et immigration

Date(s) clée(s)

Question publiée le : 29 mars 2011, page 3010
Réponse publiée le : 12 juillet 2011, page 7634