ASSEMBLÉE NATIONALE

14ème législature

commerce électronique

Question écrite n° 25258

Texte de la question

M. Édouard Courtial attire l'attention de Mme la garde des sceaux, ministre de la justice, sur les fraudes à la carte bancaire dans les ventes en ligne. En effet, ces dernières années, internet enregistre une augmentation du risque de fraude. Selon une récente étude, les tentatives de fraude à la carte bancaire représentent près de 3 % des 26 millions de transactions réalisées sur internet en France en 2012, et ce principalement dans les secteurs de l'électroménager, de la téléphonie et de la parfumerie. Le produit de ces fraudes atteindrait 1,7 milliard d'euros. La fraude à la carte bancaire s'est professionnalisée et industrialisée, les fraudeurs agissant souvent au sein d'organisations criminelles. C'est pourquoi il souhaite connaître les mesures prises par le Gouvernement pour lutter contre les grands réseaux de fraude en ligne.

Texte de la réponse

La multiplication des échanges commerciaux sur Internet a donné à certains réseaux criminels l'occasion de commettre des escroqueries à grande échelle. En effet, l'utilisation d'Internet permet à la fois de préserver l'anonymat et de toucher un très grand nombre de victimes en France et dans le monde entier. Il existe ainsi plusieurs types d'escroquerie par internet : - l'escroquerie commise à l'occasion d'une transaction bancaire en ligne à un prix onéreux sans obtention du bien acheté ; - l'escroquerie qui consiste à obtenir le versement d'une somme d'argent en abusant les victimes avec de faux courriels d'appel au secours émis à partir d'adresses piratées de leurs contacts ; - l'escroquerie par « skimming » (de l'anglais : « écrémage ») qui consiste à manipuler les automates et terminaux de paiement avec un équipement spécial qui copie les données contenues sur la piste magnétique de la carte bancaire ; - le « phishing » (de l'anglais : « hameçonnage ») qui consiste à se faire passer pour un organisme connu (banque, administration fiscale, caisse de sécurité sociale, fournisseur d'accès à internet...) et à demander à la victime de « mettre à jour » ou de « confirmer suite à un incident technique » ses données bancaires. Face à ces nouveaux modes opératoires, plusieurs dispositions ont été prises afin de mieux cerner le phénomène et de lutter plus efficacement contre cette délinquance. Ainsi, lorsqu'un particulier découvre un site lui laissant suspecter ce type d'escroquerie, il peut désormais très facilement le signaler sur le site https ://www. internet-signalement. gouv. fr/. Il s'agit d'une plateforme qui permet de répertorier les sites internet dont le contenu est illicite. Les signalements sont traités par un service d'enquête spécialisé en matière d'escroquerie par utilisation des nouveaux moyens de communication, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Ils peuvent être le point de départ de l'ouverture d'une enquête pénale. Par ailleurs, dans le but de limiter le préjudice matériel des victimes, l'article L 133-18 alinéa 1 du code monétaire et financier prévoit qu' « En cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues à l'article L. 133-24 [signalement sans tarder et au plus tard dans un délai de 13 mois à compter du débit, sauf disposition contraire], le prestataire de services de paiement du payeur rembourse immédiatement au payeur le montant de l'opération non autorisée et, le cas échéant, rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu. ». En outre, l'article 15-3 alinéa 1 du code de procédure pénale dispose que « La police judiciaire est tenue de recevoir les plaintes déposées par les victimes d'infractions à la loi pénale et de

les transmettre, le cas échéant, au service ou à l'unité de police judiciaire territorialement compétent. ». Les fournisseurs d'accès à internet et les opérateurs en téléphonie mobile sont systématiquement requis par les officiers de police judiciaire, sur autorisation du procureur de la République dans le cadre d'une enquête préliminaire ou sur commission rogatoire du juge d'instruction dans le cadre d'une information judiciaire, pour transmettre toute information utile à l'identification du ou des titulaires de la ligne téléphonique, du courriel ou de l'adresse IP à l'origine de l'escroquerie. Enfin, le ministère de la justice porte une attention toute particulière à ce type de faits et participe activement aux réunions et travaux de l'Observatoire à la Sécurité des Cartes de Paiement (OSCP) qui réunit les représentants des principales administrations concernées par cette question (ministère de la justice, ministère de l'économie et desfFinances, OCLCTIC, ministère de l'intérieur, Agence nationale de la sécurité des systèmes d'information), les représentants des émetteurs de cartes de paiement et du secteur bancaire, les représentants des consommateurs ainsi que les représentants des commerçants, en vue de coordonner en amont des actions efficaces de prévention et de lutter ensemble contre ce type d'escroquerie.

Données clés

Auteur : M. Édouard Courtial
Circonscription : Oise (7e circonscription) - Les Républicains
Type de question : Question écrite
Numéro de la question : 25258
Rubrique : Ventes et échanges
Ministère interrogé : Justice
Ministère attributaire : Justice

Date(s) clée(s)

Question publiée au JO le : 23 avril 2013, page 4363
Réponse publiée au JO le : 13 août 2013, page 8787