ASSEMBLÉE NATIONALE

# 14ème legislature

| | | |
|---|---|---|
| **Question N° : 9279** | De **M. Jacques Myard** ( Union pour un Mouvement Populaire - Yvelines ) | **Question écrite** |

| | |
|---|---|
| **Ministère interrogé** > Justice | **Ministère attributaire** > Justice |

| | | |
|---|---|---|
| **Rubrique** >télécommunications | **Tête d'analyse** >Internet | **Analyse** > cybercriminalité. lutte et prévention. |

Question publiée au JO le : **06/11/2012**
Réponse publiée au JO le : **11/06/2013** page : **6172**
Date de renouvellement : **26/03/2013**

## Texte de la question

M. Jacques Myard appelle l'attention de Mme la garde des sceaux, ministre de la justice, sur les escroqueries dont est victime un nombre croissant de nos concitoyens sur les nouveaux moyens de communication, internet et téléphone portable. Les premiers prennent la forme de courriels envoyés sur la messagerie des particuliers les incitant à révéler des données confidentielles et notamment des informations bancaires. En particulier, la contrefaçon de sites connus et ayant de nombreux abonnés, comme les fournisseurs d'accès à internet (FAI) ou encore des sites de transaction en ligne, incite en signalant de faux problèmes à se connecter sur un site contrefait pour y entrer ses identifiants et codes d'accès. Les seconds prennent la forme d'appels anonymes ou de textos incitant à rappeler un numéro surtaxé offrant un pseudo service non désiré. Compte tenu du nombre d'utilisateurs de ces services, soit près de 60 millions de Français, le taux potentiel de réponse, aussi faible soit-il, n'en permet pas moins à ces escrocs d'espérer des profits importants. Aussi, la lutte contre ces agissements passe avant tout par une prévention de très large envergure développant la connaissance et la vigilance de tous les utilisateurs. En janvier 2009 a été présenté un plan de lutte contre les escroqueries sur internet, avec la création d'une plateforme d'agents de police dédiée à ce type de fraudes, la désignation d'un référent dans les commissariats de police, et un standard téléphonique ainsi qu'un site internet permettant aux utilisateurs le signalement de ces agissements. Il n'en demeure pas moins que ces escroqueries continuent de se développer, et que nous recevons tous des courriels ou des appels de ce type. Les utilisateurs prudents ou avertis se contentent pour la plupart de les ignorer, mais beaucoup d'autres se laissent abuser. Force est de constater aussi que ceux qui souhaitent dénoncer ces agissements se heurtent souvent à un mur des FAI ou des opérateurs qui estiment que ce n'est pas leur problème, d'autre part à la difficulté de trouver les informations nécessaires au signalement sur internet ou aux démarches à suivre en général. Enfin, compte tenu du caractère mondial des technologies de l'information, les auteurs de ces délits se trouvent souvent hors du pays et donc hors d'atteinte des services de police français. Il va de soi que la lutte contre cette nouvelle délinquance passe par une forte coopération internationale. Il lui demande en conséquence comment il compte enrayer les escroqueries dans les nouvelles technologies, responsabiliser davantage les FAI et opérateurs, et surtout donner une meilleure information à nos concitoyens pour prévenir ces agissements.

## Texte de la réponse

Il existe en effet plusieurs types d'escroqueries par internet : 1) L'escroquerie commise à l'occasion d'une transaction bancaire en ligne à un prix onéreux sans retour du bien acheté ; 2) L'escroquerie qui consiste à bénéficier du versement d'une somme d'argent en abusant les victimes via de faux courriels d'appel au secours émis à partir des adresses piratées de leurs contacts ; 3) 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 ; 4) Le « phishing » (de l'anglais : « hameçonnage ») qui consiste pour l'escroc à se faire passer pour un organisme familier (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. Lorsqu'un particulier constate 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/. Cette plateforme permet ainsi de répertorier les sites internet dont le contenu est illicite. Ces 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). Ces signalements 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, en vue de 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 des finances, 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.