ASSEMBLÉE NATIONALE

# 14ème legislature

| | | |
|---|---|---|
| **Question N° : 51359** | De **M. André Chassaigne** ( Gauche démocrate et républicaine - Puy-de-Dôme ) | **Question écrite** |

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

Question publiée au JO le : **04/03/2014**
Réponse publiée au JO le : **20/05/2014** page : **4099**
Date de changement d'attribution : **03/04/2014**

## Texte de la question

M. André Chassaigne attire l'attention de M. le ministre de l'intérieur sur les mesures de lutte contre le piratage des boîtes électroniques. Malgré les reportages et informations diffusées dans les médias et certaines mesures de prévention à l'attention des particuliers, beaucoup sont victimes de pirates informatiques essentiellement basés à l'étranger. Utilisant les informations communiquées notamment dans les réseaux sociaux, ou par la méthode du *phishing*, les pirates arrivent à retrouver le nom puis le mot de passe permettant d'accéder aux boîtes électroniques. Ils usent ensuite de subterfuges permettant d'abuser de la crédulité ou de l'ignorance des personnes en contact avec le titulaire de la boîte électronique piratée. En délivrant un message de demande d'aide urgente, ils arrivent ainsi à obtenir le versement à l'étranger de sommes importantes *via* des sociétés internationales de transfert d'argent. Il existe alors peu de chances de retrouver les responsables et les fonds extorqués. La situation est difficile à vivre pour la victime, en raison des sommes perdues, mais aussi pour le titulaire de la boîte électronique, qui peut s'estimer redevable, sans pour autant être responsable. Au regard du nombre important de ces affaires et des conséquences personnelles pour les victimes, des actions ne pourraient-elles pas être mises en place auprès des sociétés impliquées (opérateurs internet ou de transfert de fonds) afin de limiter le piratage ou d'en limiter les conséquences ? Par ailleurs, les assurances ne peuvent-elles pas couvrir ce type d'escroquerie, à l'instar de ce qui existe déjà pour les moyens de paiement ? Il lui demande de bien vouloir répondre à ces questions et de lui communiquer les statistiques sur le niveau actuel de ces escroqueries et les mesures qu'il envisage pour renforcer la lutte contre ces pratiques.

## Texte de la réponse

Le développement d'Internet et des réseaux offre un nouveau champ d'action à différentes formes de délinquance, qui tirent profit de la vitesse et de la puissance de propagation d'Internet et de l'anonymat qu'il procure. Dans nos sociétés où Internet et les systèmes d'information occupent une place sans cesse croissante, la sécurité numérique constitue pour la société et pour l'Etat un enjeu majeur. Comme dans la vie quotidienne, l'Etat doit en effet assumer son rôle pour assurer la sécurité de nos concitoyens et celle des entreprises dans l'espace numérique, face à des menaces diverses et mouvantes (atteintes aux systèmes d'information, cyberdélinquance crapuleuse, cyberdélinquance idéologique...). Parmi les manifestations les plus visibles de cette délinquance figure le « phishing », qui vise à recueillir des informations personnelles confidentielles par des envois de mels falsifiés qui se présentent comme des messages provenant d'organismes familiers. Comme d'autres acteurs publics et privés, les forces de sécurité de l'Etat consacrent d'importants moyens, humains et techniques, à la lutte contre la cybercriminalité sous toutes ses formes. Au sein du ministère de l'intérieur, cette mission 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. Composé de policiers et de gendarmes, cet office central anime et coordonne l'action des services centraux et territoriaux de la police judiciaire, conduit des actes d'enquête et des travaux techniques d'investigation en appui de nombreux services, aussi bien de police et de gendarmerie que d'autres administrations (direction générale des douanes et droits indirects, etc.). L'OCLCTIC dispose aussi d'un groupe d'enquête mixte police-gendarmerie spécialisé dans la répression des principales infractions de cybercriminalité (fraude aux cartes de paiement pour les ventes à distance, fausses annonces, escroqueries à la nigériane, à la fausse loterie...) et notamment dans l'identification des réseaux criminels. La collaboration est particulièrement développée avec la gendarmerie nationale. La cybercriminalité étant largement un phénomène transnational, les coopérations bilatérales avec les pays « sources » sont également renforcées et la coopération se développe dans les enceintes européennes et internationales (Union européenne, Conseil de l'Europe, G8, Interpol...). Une plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) a été mise en place en 2009 pour exploiter le site www. internet-signalement. gouv. fr, qui offre des conseils de prévention et permet aux internautes et aux professionnels de signaler, de manière simple, tout contenu illicite de l'Internet. Ces signalements peuvent être le point de départ de l'ouverture d'une enquête pénale. La plate-forme, composée de policiers et de gendarmes et placée au sein de l'OCLCTIC, a reçu en 2012 près de 120 000 signalements, dont des milliers ont été transmis pour enquête aux services répressifs français et à Interpol. 60 % de ces signalements concernent des escroqueries commises sur Internet. En 2013, PHAROS a reçu 123 987 signalements, dont près de 25 000 concernaient des faits de « phishing ». Le nombre de signalements reçus par PHAROS témoigne d'une réelle visibilité du site www. internet-signalement. gouv. fr, dont l'existence est signalée sur de nombreux sites publics ou privés, et qui est immédiatement identifiable via les grands moteurs de recherche. Une plate-forme téléphonique d'information et de prévention du public sur toutes les formes d'escroqueries existe également. Appelée « Info escroqueries » et composée de policiers et de gendarmes, elle reçoit plus de 20 000 appels par an. De nombreux organismes publics et privés mènent des campagnes de sensibilisation face aux risques du « phishing » et certains ont mis en place un dispositif de signalement. PHAROS demeure toutefois le point central national unique de recueil des signalements. Il convient de souligner que PHAROS a parmi ses partenaires privés l'association Phishing Initiative, qui assure un traitement efficace des signalements de « phishing », mettant à la disposition des internautes un formulaire en ligne spécifique. Les adresses signalées sont répercutées vers les éditeurs de logiciels de navigation sur Internet, afin que leurs utilisateurs soient automatiquement alertés lorsqu'ils sont confrontés à des sites de « phishing ». Il est à ce jour difficile de quantifier le phénomène de « phishing », qui ne fait pas l'objet d'un recensement statistique spécifique, même si le nombre de signalements reçus par PHAROS donne un aperçu de la réalité. Le nouveau système de la statistique publique de la délinquance, conçu en concertation avec l'Observatoire national de la délinquance et des réponses pénales (ONDRP), va toutefois permettre de rendre compte de certaines réalités, notamment de la cybercriminalité, que les indicateurs de la délinquance ne permettaient pas jusqu'à présent d'appréhender. La nouvelle architecture statistique comporte un agrégat relatif à la cybercriminalité, qui n'est toutefois pas encore opérationnel en raison de préalables techniques. Ce nouvel agrégat permettra de recenser précisément les infractions liées aux technologies de l'information et de la communication. Il doit être souligné qu'une prévention efficace de la cyberdélinquance passe en tout état de cause d'abord par une sensibilisation des internautes, qui doivent, au quotidien, faire preuve de vigilance. S'agissant de l'interrogation, soulevée dans la question écrite, relative aux « assurances » face à ce type d'escroqueries, il s'agit d'un sujet qui ne relève pas de la compétence du ministre de l'intérieur. Enfin, et de manière plus générale, il doit être souligné que, prenant en compte l'augmentation des menaces, et les difficultés qui peuvent se rencontrer pour y répondre (caractère transnational des réseaux, application du droit national à des opérateurs étrangers...), le Gouvernement a engagé une adaptation du dispositif de lutte contre la cybercriminalité. Il est en effet indispensable de « monter en gamme », de renforcer l'arsenal juridique et de faire évoluer les organisations. A la suite du séminaire gouvernemental sur le numérique du 28 février 2013, un groupe de travail interministériel (Justice/Economie/Intérieur/Economie numérique) a été institué. Ce groupe de travail a commencé à se réunir en juillet 2013 pour élaborer une stratégie globale de lutte contre la cybercriminalité, prenant en compte la dimension internationale et européenne du phénomène, et portant notamment sur le développement des dispositifs d'aide aux victimes et de sensibilisation des publics. Ses travaux sont achevés et son rapport devrait prochainement être remis. Par ailleurs, le ministre de l'intérieur a demandé début 2014 aux directeurs généraux de la police nationale et de la

gendarmerie nationale de définir un Plan d'action ministériel permettant de franchir de nouvelles étapes en matière de capacités de réponse aux cybermenaces, tant préventives qu'administratives ou de police judiciaire. L'objectif est, notamment, d'optimiser les organisations internes au ministère et de développer une action tout à la fois transverse, globale et lisible, intégrant une politique de prévention, des dispositifs de répression et des capacités d'anticipation. Le rapport final devrait être remis au ministre à la fin du mois de mai. Au-delà, une action globale est engagée par le Gouvernement pour renforcer les capacités nationales de cybersécurité (sécurité des systèmes d'information...), dans le cadre notamment du travail accompli par l'Agence nationale de sécurité des systèmes d'information (ANSSI).