ASSEMBLÉE NATIONALE

14ème legislature

Question N° : 31297	De **M. Marc Le Fur** (Union pour un Mouvement Populaire - Côtes-d'Armor)	**Question écrite**

Ministère interrogé > PME, innovation et économie numérique	**Ministère attributaire** > Intérieur

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

Question publiée au JO le : **02/07/2013**
Réponse publiée au JO le : **17/09/2013** page : **9733**
Date de changement d'attribution : **06/08/2013**

Texte de la question

M. Marc Le Fur attire l'attention de Mme la ministre déléguée auprès du ministre du redressement productif, chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique, sur la lutte contre le « *phishing* ». Les internautes et entreprises sont de plus en plus fréquemment destinataires de courriels frauduleux de type hameçonnage ou « *phishing* » qui usurpent l'identité d'entreprises, d'administrations publiques ou d'organismes reconnus afin d'obtenir leurs informations personnelles et coordonnées bancaires. À première vue, il est difficile d'identifier le véritable expéditeur car les pirates informatiques utilisent les en-têtes et logos officiels de l'organisme détourné. Dans la plupart des cas, les internautes sont invités à se connecter en ligne *via* un lien hypertexte pour actualiser leurs coordonnées sur un site web factice dont la mise en page et l'URL semblent authentiques. Alors que les contribuables français sont encouragés à réaliser leur déclaration d'impôts en ligne, de faux courriels semblant provenir de l'administration fiscale circulent, profitant des victimes les moins vigilantes. Très récemment ce sont des entreprises françaises, et notamment des banques, qui ont été la cible de cyberattaques très organisées, adressant un mail personnalisé couplé avec un appel téléphonique au salarié pour gagner sa confiance. Ce type d'escroquerie s'étend également aux téléphones portables par le biais de SMS. C'est pourquoi il lui demande, d'une part, de lui fournir un état statistique précis de ce type d'acte cybercriminels et, d'autre part, de lui indiquer les mesures envisagées par le Gouvernement pour prévenir et protéger les particuliers et les entreprises de ces pratiques.

Texte de la réponse

La sécurité de l'espace numérique constitue pour la société (acteurs économiques, particuliers...) et pour l'Etat un enjeu majeur alors que le développement d'Internet et des systèmes d'information offre de nouvelles occasions à une criminalité, souvent internationale, qui sait tirer profit des structures de l'environnement numérique (anonymisation, etc.). 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. Les victimes, trompées par la qualité supposée de l'expéditeur, fournissent leurs données bancaires. Banques, grandes sociétés et organismes publics sont la cible de fréquentes campagnes de « phishing », très évolutives en fonction du contexte social et économique. 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.). La collaboration est particulièrement développée avec la gendarmerie nationale, dont le service technique de recherches judiciaires et de documentation (STRJD) est doté d'une division de lutte contre la cybercriminalité. La gendarmerie dispose aussi d'une expertise judiciaire avec son département informatique et électronique de l'institut de recherche criminelle de la gendarmerie nationale (IRCGN), à l'instar du service central de l'informatique et des technologies de la sous-direction de la police technique et scientifique de la direction centrale de la police judiciaire. La cybercriminalité étant largement un phénomène transnational, les coopérations bilatérales avec les pays « sources » sont 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. Au cours des sept premiers mois de 2013, PHAROS a reçu plus de 80 000 signalements, dont près de 20 000 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 40 000 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 et l'association Phishing Initiative préparent une convention de partenariat qui permettra une transmission réciproque des signalements pour en assurer un traitement plus efficace, avec en particulier la mise à disposition des internautes d'un formulaire en ligne permettant le signalement facile des URL qui dirigent vers des sites de phishing. Les organismes sociaux et les autres acteurs privés ciblés par des campagnes de « phishing » pourront s'associer à ce dispositif. 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. Par ailleurs, le Gouvernement a engagé une adaptation du dispositif de lutte contre la cybercriminalité, qui passe notamment par une connaissance accrue du phénomène. A la suite du séminaire gouvernemental sur le numérique du 28 février dernier, il a été décidé de mettre en place un groupe de travail interministériel (Justice/Economie et Finances/ Intérieur/ Economie numérique) chargé d'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. Ce groupe de travail a commencé à se réunir en juillet 2013 et devrait rendre son rapport d'ici à la fin de l'année.