ASSEMBLÉE NATIONALE

14ème legislature

Question N° : 23092	De **M. Pascal Popelin** (Socialiste, républicain et citoyen - Seine-Saint-Denis)	**Question écrite**
Ministère interrogé > Économie et finances	**Ministère attributaire** > Intérieur	
Rubrique >télécommunications	**Tête d'analyse** >Internet	**Analyse** > escroqueries. lutte et prévention.
Question publiée au JO le : **02/04/2013** Réponse publiée au JO le : **18/06/2013** page : **6441** Date de changement d'attribution : **16/04/2013**		

Texte de la question

M. Pascal Popelin attire l'attention de M. le ministre de l'économie et des finances sur la multiplication des courriels frauduleux émanant d'individus se faisant passer pour des opérateurs publics ou privés. Cette pratique est en effet en pleine croissance : l'usurpateur envoie à sa victime un message et récupère ses informations personnelles et bancaires ensuite utilisées pour accéder à des comptes sécurisés et effectuer des opérations sous son identité. Actuellement, si la DGCCRF (direction générale de la concurrence de la consommation et de la répression des fraudes) assure la protection économique et la sécurité des consommateurs, il n'existe aucun moyen direct de signaler la fraude à l'opérateur en question. Certains organismes, comme la CAF, ont sur leur site procédé à une campagne de sensibilisation de l'usager tendant vers l'instauration d'une procédure de signalement automatique des courriels et sites internet frauduleux. C'est pourquoi il s'interroge sur l'opportunité de généraliser cet outil, et de créer sur la page d'accueil des sites de paiement en ligne un onglet « signalement de fraudes », qui permettra au consommateur d'alerter la société de toute tentative de fraude. Il souhaiterait alors avoir connaissance de la méthode que le Gouvernement compte employer pour réduire les risques de fraudes sur la toile.

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.) et développe des techniques sans cesse plus sophistiquées. Parmi les manifestations les plus visibles de cette criminalité figure le phishing, qui vise à recueillir des informations personnelles confidentielles par des envois massifs de mels falsifiés qui se présentent comme des messages provenant d'administrations publiques, de banques, de grandes entreprises, etc. Les victimes, trompées par la qualité supposée de l'expéditeur, fournissent elles-mêmes leurs données bancaires ou d'autres données personnelles. La lutte contre la cybercriminalité sous toutes ses formes (escroqueries, utilisation frauduleuse de moyens de paiement, pédophilie, etc.) est un axe central de la politique de sécurité. La visite effectuée le 11 janvier dernier par le ministre de l'intérieur et le ministre délégué chargé de l'économie numérique dans les services spécialisés de la police et de la gendarmerie nationales, comme la clôture par le ministre de l'intérieur du forum international sur la cybersécurité qui s'est tenu à Lille les 28 et 29 janvier dernier, témoignent de l'importance que le Gouvernement accorde à cet enjeu. Les forces de sécurité de l'Etat consacrent d'importants moyens à la lutte contre cette délinquance, recourent à des méthodes d'investigation modernes et proactives (enquêtes sous pseudonyme...), développent les partenariats avec différents acteurs (universités, réseau européen des centres d'excellence en matière de lutte contre la cybercriminalité...). Au sein du ministère de l'intérieur, l'action de la police et de la gendarmerie s'appuie sur un réseau de plus de 600

enquêteurs spécialisés dans le numérique. Toutefois, la lutte contre la cybercriminalité 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 sur le plan opérationnel et technique l'action des services centraux et territoriaux de la police judiciaire. 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 et gère le centre national d'analyse des images de pédopornographie (CNAIP), commun à la police et à la gendarmerie. 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. L'OCLCTIC 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.). Une plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) a été mise en place en 2009 pour gérer le site www. internet-signalement. gouv. fr, qui offre des conseils de prévention et permet aux internautes et aux professionnels de dénoncer, de manière simple, tout contenu illicite sur Internet ou toute infraction dont ils sont victimes. La plate-forme, composée de policiers et de gendarmes, 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. Comme les banques et les grandes sociétés (ERDF...), les organismes publics, dont les caisses d'allocations familiales (CAF), sont la cible de fréquentes campagnes de phishing, très évolutives en fonction du contexte social et économique. Ces organismes mènent des campagnes de sensibilisation de leur public et certains ont mis en place un dispositif de signalement. La plate-forme PHAROS demeure toutefois le point central national unique de recueil de ces signalements. Il convient à cet égard de souligner que PHAROS et l'association Phishing Initiative préparent une convention de partenariat qui permettra de mettre à la disposition des internautes un formulaire en ligne permettant le signalement facile des URL (adresses) qui dirigent vers des sites de phishing. Ce partenariat entre PHAROS et Phishing Initiative permettra une transmission réciproque des signalements et d'en assurer un traitement plus rapide et plus efficace. Les organismes sociaux et les autres acteurs privés ciblés par des campagnes de phishing pourront s'associer à ce dispositif. 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. L'OCLCTIC dispose aussi d'un groupe d'enquête spécialisé dans la lutte contre les escroqueries sur Internet. Une vigilance particulière s'exerce également à l'égard des opérations frauduleuses affectant les transactions par carte bancaire. L'OCLCTIC a renforcé son partenariat avec la fédération bancaire française et le groupement d'intérêt économique des cartes bancaires afin d'améliorer l'échange d'informations opérationnelles et techniques. L'OCLCTIC siège, en outre, au sein de l'Observatoire de la sécurité des cartes de paiement. Ce partenariat concerne également les professionnels chargés de la production d'automates de paiement, afin d'améliorer la protection des équipements, la détection des dispositifs de captation et la remontée de l'information vers les services de police. La prévention, notamment technique, est essentielle et le dernier rapport de l'Observatoire de la sécurité des cartes de paiement fait état sur ce point de réelles avancées dans la sécurisation des opérations de paiement par carte bancaire via Internet (dispositifs d'authentification « non rejouable » tels la technologie « 3D-Secure...). Sur le plan juridique, la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure a doté les services de sécurité de moyens accrus (captation à distance des données issues de communications électroniques dans la lutte contre la criminalité organisée, obligation pour les fournisseurs d'accès à Internet de bloquer les images pédopornographiques sur des sites notifiés par le ministère de l'intérieur, "cyberpatrouilles" pour détecter les infractions d'apologie et de provocation aux actes de terrorisme). Par ailleurs, la loi précitée a introduit dans le code pénal une incrimination spécifique d'usurpation d'identité sur Internet. Le ministre de l'intérieur a annoncé la mise en place d'un groupe de travail interministériel associant les ministères de l'intérieur, de la justice et de l'économie numérique pour aller plus loin. Ce groupe proposera des mesures concrètes d'amélioration des moyens de lutte contre la cybercriminalité, notamment en matière de sensibilisation du public et de prévention. La cybercriminalité étant essentiellement un phénomène transnational, les coopérations bilatérales avec les pays "sources" sont

renforcées et la coopération opérationnelle internationale se développe dans le cadre des enceintes européennes et internationales (Union européenne, Conseil de l'Europe, G8, Interpol...). Il convient notamment de noter la mise en place en janvier dernier d'un Centre européen de lutte contre la cybercriminalité (EC3) auprès d'Europol. La France est également adhérente à la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001, première et unique convention internationale en la matière, qui favorise la coopération judiciaire et permet la mise en relation directe des services d'investigation pour répondre aux demandes urgentes de gel de données numériques. En France, l'OCLCTIC a été désigné comme point de contact.