ASSEMBLÉE NATIONALE

14ème législature

Internet

Question écrite n° 20530

Texte de la question

M. Rudy Salles attire l'attention de M. le ministre de l'intérieur sur le phénomène de la cyber-escroquerie qui touche déjà des dizaines de milliers de citoyens français. Depuis l'ouverture du réseau internet au trafic commercial au début des années 1990, les cyber-escroqueries n'ont cessé d'augmenter et sont un vrai fléau international. Les services comme paypal ou moneybookers sont régulièrement clonés pour faire de faux sites à ces enseignes. Les banques françaises et européennes font aussi l'objet d'usurpation. De faux courriels à enseigne de ces banques sont envoyés par centaines de milliers aux internautes dans le but d'obtenir l'identifiant et le mot de passe de leur compte bancaire en ligne. Des faux documents à l'enseigne de grandes banques internationales se multiplient. Il en va de même pour les abonnements des internautes. Des faux courriels à en-tête d'Orange, Free, Club internet, Alice-adsl, etc., circulent chaque jour. Très récemment, la SACEM, la CAF, mais également l'administration fiscale française faisaient l'objet d'usurpation, dans le cadre d'une tentative d'escroquerie visant à récupérer des numéros de cartes bancaires. Les internautes se voient proposer de fausses offres d'emploi ou des stages rémunérés. Les candidats sont invités à envoyer un dossier de candidature et devront s'acquitter des frais de dossier de 100 à 350 euros. Les victimes, qui bien souvent auront avisé « Pôle emploi » de ce nouvel emploi, ne sont plus indemnisées pendant un certain temps. Ce phénomène prend aussi la forme d'annonces de gain à une loterie, d'héritage ou de don *via* le courrier électronique. Se référant à l'ordonnance n° 2009-104 du 30 janvier 2009 (article 19), le Crédit agricole d'Aquitaine a récemment demandé par courrier électronique à ses clients la transmission de la copie de leur pièce d'identité et d'un justificatif de domicile, proposant de retourner les documents *scannés* par voie électronique. Il s'agissait là d'une demande réelle mais, pour le consommateur, il est de plus en plus difficile de faire la part entre le vrai et le faux, tant ils sont peu ou mal informés des risques et des pratiques. Eu égard à ces observations, il lui demande quelles mesures il compte prendre pour protéger les internautes français des cyber-escroqueries.

Texte de la réponse

La sécurité de l'espace numérique constitue pour la société et pour l'Etat un enjeu majeur alors que ledéveloppement d'Internet et des systèmes d'information a donné naissance à une nouvelle forme de criminalité, souvent internationale, qui sait tirer profit des structures de l'environnement numérique (anonymisation, etc.) et développe des techniques sans cesse plus sophistiquées. La lutte contre la cybercriminalité (escroqueries, utilisations frauduleuses de moyens de paiement, pédophilie, etc.) est donc un axe central de la politique de sécurité. Le 11 janvier dernier, la visite des services spécialisés de la police et de la gendarmerie nationales par le ministre de l'Intérieur et la ministre déléguée chargée de l'Economie Numérique, comme leur participation, ainsi que celle du ministre délégué aux Anciens Combattants, au forum international sur la cybercriminalité (FIC) 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 pseudonymes...) et développent des 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. Cependant, 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. Il 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 des droits indirects, etc.). Depuis 2008, un groupe d'enquêteurs spécialisés a été mis en place et spécialement chargé d'engager des procédures contre les réseaux utilisant Internet pour commettre des escroqueries (fraude à la carte de paiement utilisée pour les ventes à distance, faux sites, fausses annonces, etc.). A cette occasion, 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. Dans le cadre de la prévention, notamment technique, ce service a également développé des liens avec les professionnels chargés de la production d'automates de paiement, pour améliorer la protection des équipements, la détection des dispositifs de captation et la remontée de l'information vers les services de police. 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'authentifïcation « non rejouable » tels la technologie « 3D-Secure...). Parallèlement à ces groupes d'enquête, il convient de rappeler que depuis 2009, une plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS), a été mise en place pour gérer le site www. internetsignalement. gouv. fr. Cette plateforme, qui offre par ailleurs des conseils de prévention, permet aux internautes et aux professionnels de signaler des sites au contenu illégal ou des infractions dont ils ont été victimes. Près de 120 000 signalements ont été recueillis en 2012, dont des milliers ont été transmis pour enquête aux services répressifs français et à Interpol. Une plateforme 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 a reçu près de 42 000 appels en 2011. 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 récemment 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. Enfin, la cybercriminalité étant un phénomène essentiellement transnational, les coopérations bilatérales avec les pays "sources" sont renforcées et la coopération opérationnelle internationale se développe dans le cadre de diverses enceintes européennes et internationales (Union européenne, Conseil de l'Europe, G8, Interpol...). On peut 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 promeut la participation des parties au réseau d'alerte "G8/H24", qui permet la mise en relation directe des services d'investigation pour répondre aux demandes urgentes de gel de données numériques. En France, c'est l'OCLCTIC qui a été désigné comme point de contact.

Données clés

Auteur : M. Rudy Salles
Circonscription : Alpes-Maritimes (3e circonscription) - Union des démocrates et indépendants
Type de question : Question écrite
Numéro de la question : 20530
Rubrique : Télécommunications
Ministère interrogé : Intérieur

Version web : https://www.assemblee-nationale.fr/dyn/14/questions/QANR5L14QE20530

Ministère attributaire : Intérieur

Date(s) clée(s)

Question publiée au JO le : 5 mars 2013, page 2431
Réponse publiée au JO le : 11 juin 2013, page 6163