ASSEMBLÉE NATIONALE

13ème législature

Internet

Question écrite n° 130020

Texte de la question

M. Richard Mallié attire l'attention de M. le ministre de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration sur le phénomène de la cyber-escroquerie qui touche des dizaines de milliers de citoyens français. Une association de consommateur vient de nouveau d'alerter les pouvoirs publics sur un phénomène en pleine croissance : de faux courriels circulent en masse et invitent leurs destinataires à communiquer des données confidentielles. 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. 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 de différentes entreprises (Orange, Free, Club internet...) circulent chaque jour. 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

Internet offre de nouvelles occasions à une criminalité qui sait tirer profit des structures de l'environnement numérique (anonymisation, etc.) et développe des techniques de plus en plus sophistiquées, notamment en matière d'escroqueries. Pour y répondre, les moyens des forces de sécurité de l'Etat sont renforcés et leurs méthodes d'investigation modernisées. La police et la gendarmerie nationales disposent de plus de 500 enquêteurs spécialisés. Un plan d'action de lutte contre la cybercriminalité a été engagé dès 2008, qui incombe à titre principal à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), placé au sein de la direction centrale de la police judiciaire. Il a été complété en 2009 par un plan de lutte contre les escroqueries. Une plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) a été instituée pour gérer le site www. internet-signalement. gouv. fr, qui offre des conseils de préévention et permet aux internantes et aux professionnels de dénoncer, de manière simple, tout contenu illicite sur internet ou toute infraction dont ils sont victimes. En 2011, la plate-forme, composée de policiers et de gendarmes, a reçu plus de 100 000 signalements dont près de la moitié concernant des escroqueries et extorsions de fonds commises sur Internet et des milliers de signalement ont été transmis pour enquête aux services répressifs français et à Interpol. Une plate-forme téléphonique d'information et de prévention du public sur toutes les formes d'escroqueries a également été créée. Appelée « Info escroqueries » et composée de policiers et de gendarmes, elle a reçu plus de 25 000 appels en 2011. Il a également été institué dès 2008 au sein de l'OCLCTIC un groupe de lutte contre les escroqueries sur Internet. Ce groupe d'enquête, composé de policiers et de gendarmes, est 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.) et assure une centralisation opérationnelle des affaires recensées dans l'ensemble du territoire national. L'expérience acquise par ce groupe a permis de développer une connaissance précise du phénomène et de situer les principaux réseaux criminels en Afrique de l'Ouest, en Asie et en Europe orientale, particulièrement en Roumanie. Au regard du caractère transnational des affaires, le

groupe d'enquête recourt régulièrement à des demandes d'entraide judiciaire, dont l'exécution peut-être facilitée grâce à la coopération policière privilégiée instaurée avec certains pays, par exemple avec la Roumanie qui dispose depuis 2010 d'un policier détaché au sein de l'OCLCTIC. Sur le plan juridique, la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI) dote 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 LOPPSI a introduit dans le code pénal une incrimination spécifique d'usurpation d'identité sur Internet. 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 d'Europol et d'Interpol. La France est 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. 54 Etats sont membres du réseau, dont la France. Au sein de TUE, divers projets en cours vont permettre de renforcer la lutte contre la cybercriminalité, notamment la création, sur proposition française, d'une plate-forme européenne de signalement des infractions sur Internet (Internet Crime Reporting Online System), qui se traduira par l'intégration des données issues des platesformes nationales de signalement dans le système d'information d'Europol. La création d'un « centre européen du cybercrime » est également à l'étude pour identifier les nouvelles formes de criminalité sur Internet, dans le cadre d'un partenariat publicprivé. Des travaux sont également menés en matière de sécurité des systèmes d'information, avec un projet de directive visant à renforcer la coopération entre les Etats membres. Il y a lieu de rappeler que la France est dotée d'un Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (CERTA). Rattaché à TAgence nationale de la sécurité des systèmes d'information au sein du secrétariat général de la défense et de la sécurité nationale, le CERTA assure des fonctions de veille, de détection, d'alerte et de réponse opérationnelles aux attaques informatiques. Des centres similaires existent dans une vingtaine d'autres Etats européens. La protection des systèmes informatiques de grandes entreprises ou de sites d'administrations publiques constitue en effet un enjeu majeur, aussi bien cour les institutions concernées que pour les utilisateurs d'Internet et plus largement pour le public.

Données clés

Auteur : M. Richard Mallié
Circonscription : Bouches-du-Rhône (10e circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 130020
Rubrique : Télécommunications
Ministère interrogé : Intérieur, outre-mer, collectivités territoriales et immigration
Ministère attributaire : Intérieur, outre-mer, collectivités territoriales et immigration

Date(s) clée(s)

Question publiée le : 6 mars 2012, page 1992
Réponse publiée le : 8 mai 2012, page 3556