ASSEMBLÉE NATIONALE

14ème législature

Internet

Question écrite n° 55901

Texte de la question

M. Guillaume Chevrollier attire l'attention de M. le ministre de l'intérieur sur les mesures de lutte contre les arnaques à l'aide de faux messages sur les boîtes électroniques. Des personnes âgées notamment sont victimes de faux messages de détresses émanant de l'étranger de parents proches ou de messages pour réclamer un lot ou bien pour récupérer des fonds d'une assurance vie non réclamée par exemple. Ces messages n'ont qu'un seul but : inciter la victime à transférer des fonds rapidement sur des comptes à l'étranger. Ces escrocs étant essentiellement basés en dehors de l'union européenne, les enquêtes sont difficiles à mener par les services d'investigation. Il lui demande quelles mesures 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. L'Etat doit 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 (sécurité des systèmes d'information, lutte contre la cybercriminalité, cyberdéfense...). Comme d'autres acteurs publics et privés, les forces de sécurité de l'Etat, qui disposent de structures dédiées, consacrent d'importants moyens, humains et techniques, à la lutte contre la cybercriminalité sous toutes ses formes, avec notamment 600 enquêteurs spécialisés de la police et de la gendarmerie nationales. 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...). 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), placée au sein de l'OCLCTIC, exploite 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, a reçu en 2013 plus de 120 000 signalements, dont des milliers ont été transmis pour enquête aux services répressifs français et à Interpol. Une plate-forme téléphonique d'information du public et

de prévention 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. 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. 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 l'ensemble des cybermenaces. 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, 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. Son rapport sera remis au Premier ministre le 30 juin. 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 gagner en efficacité et en réactivité et de franchir de nouvelles étapes, tant préventives qu'administratives ou de police judiciaire. L'objectif est, notamment, d'optimiser les organisations internes au ministère et de développer une action à la fois transverse, globale et lisible, intégrant une politique de prévention, des dispositifs de répression et des capacités d'anticipation. Le rapport sur la lutte contre les cybermenaces en matière de sécurité intérieure a été remis au ministre de l'intérieur le 31 mai. Il propose six axes stratégiques d'action (renforcer le niveau de sécurité des systèmes d'information, promouvoir la coopération internationale, améliorer le niveau de sensibilisation et de prévention des particuliers, des acteurs économiques et des collectivités territoriales, etc.). Ces préconisations ont été validées par le ministre de l'intérieur, qui a par ailleurs décidé de nommer un délégué ministériel à la lutte contre les cybermenaces. Ce dernier sera chargé, notamment, de veiller à la mise en oeuvre effective du plan d'action. D'ores et déjà, la création d'une sous-direction dédiée à la lutte contre la cybercriminalité au sein de la direction centrale de la police judiciaire va permettre de renforcer les capacités de réponse du ministère de l'intérieur.

Données clés

Auteur : M. Guillaume Chevrollier
Circonscription : Mayenne (2e circonscription) - Les Républicains
Type de question : Question écrite
Numéro de la question : 55901
Rubrique : Télécommunications
Ministère interrogé : Intérieur
Ministère attributaire : Intérieur

Date(s) clée(s)

Question publiée au JO le : 20 mai 2014, page 3995
Réponse publiée au JO le : 29 juillet 2014, page 6524