



ASSEMBLÉE NATIONALE

14ème législature

Internet

Question écrite n° 49644

Texte de la question

M. Claude Sturni attire l'attention de M. le ministre de l'intérieur sur les « arnaques aux sentiments » qui se multiplient sur internet. Fausses propositions de rencontres, relations amoureuses fictives, identités piratées et usurpées, courriels frauduleux ont un point commun : ils viennent généralement des pays d'Afrique de l'ouest. Ces sollicitations débouchent systématiquement sur des demandes de versement d'argent, sous divers prétextes. Les scénarii les plus récurrents décrivent une situation d'urgence ou d'extrême pauvreté visant à culpabiliser ou à mettre la personne cible sous pression pour des questions « de vie ou de mort ». De ce fait, un transfert est effectué par des services comme Western union, Moneygram, BDE Ccash, Meridiana, Ria et autres agences. Les personnes escroquées se retrouvent totalement démunies, les plaintes étant généralement classées faute de pouvoir identifier les auteurs de ces arnaques. Les sommes ne sont que rarement restituées puisque transférées dans un cadre légal (sauf en cas de remboursement après contrôle des services de transferts d'argent). Il appelle donc à l'éradication de ces pratiques, notamment en développant la traque contre la cybercriminalité en collaboration avec les États concernés, dans lesquels ces activités criminelles sont perpétrées en toute impunité à une échelle industrielle. Il lui demande donc de bien vouloir lui indiquer les mesures concrètes que le Gouvernement compte entreprendre sur cette question.

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. Comme dans la vie quotidienne, l'Etat doit en effet 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 (atteintes aux systèmes d'information, cyberdélinquance crapuleuse, cyberdélinquance idéologique...). La présence du ministre de l'intérieur à la 6e édition du Forum international sur la cybersécurité (FIC), qui s'est tenue à Lille en janvier, a constitué un nouvel exemple de l'importance accordée à ces défis. Aux côtés d'autres acteurs publics et privés, les forces de sécurité de l'Etat consacrent d'importants moyens à la lutte contre la cybercriminalité sous toutes ses formes. L'action de la police et de la gendarmerie nationales s'appuie sur un réseau de plus de 600 enquêteurs spécialisés dans le numérique. 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 est doté d'une division de lutte contre la cybercriminalité. La cybercriminalité étant largement un phénomène transnational, les coopérations avec les pays « sources » et dans les enceintes

européennes et internationales (Union européenne, Conseil de l'Europe, G8, Interpol...) se développent. L'OCLCTIC dispose aussi d'un groupe d'enquête mixte police-gendarmerie spécialisé dans la répression des principales infractions de cybercriminalité. Sur le plan juridique, la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure a créé une incrimination pénale d'usurpation d'identité sur Internet. 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](http://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 d'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, reçoit plus de 100 000 signalements par an, dont des milliers sont transmis pour enquête aux services répressifs français et à Interpol. Egalement composée de policiers et de gendarmes, une plate-forme téléphonique d'information et de prévention (« Info escroqueries ») sur toutes les formes d'escroqueries est également à la disposition du public. Elle reçoit plus de 40 000 appels par an. Prenant en compte l'augmentation des menaces et les difficultés 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 la cybercriminalité. A la suite du séminaire gouvernemental sur le numérique du 28 février 2013, un groupe de travail interministériel (Justice/Economie et Finances/Intérieur/Economie numérique) a été institué. Ce groupe de travail a commencé à se réunir en juillet 2013 et devrait rendre son rapport prochainement. Il est 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. Face au phénomène, il est en effet indispensable de renforcer l'arsenal juridique et de faire évoluer les organisations. Apporter des réponses opérationnelles efficaces à cette délinquance exige de développer les coordinations entre les services, pour apporter des réponses globales à des menaces toujours plus diverses. L'année 2014 sera donc une année d'initiatives et d'avancées, avec l'élaboration en cours d'un plan d'action du ministère de l'intérieur. Il sera finalisé en lien étroit avec la réflexion que mène le ministère de la justice sur ces mêmes questions, d'ici à la fin du trimestre. Il convient également de rappeler que, pour assurer la sécurité des systèmes d'information de l'Etat et des opérateurs d'importance vitale, la France est dotée d'une Agence nationale de la sécurité des systèmes d'information (ANSSI), placée au sein du secrétariat général de la défense et de la sécurité nationale, et dont le renforcement des moyens se poursuit en application du nouveau Livre blanc sur la défense et la sécurité nationale. Enfin, une prévention efficace de la cyberdélinquance passe d'abord par une sensibilisation des internautes, qui doivent, au quotidien, faire preuve de vigilance.

Données clés

Auteur : [M. Claude Sturni](#)

Circonscription : Bas-Rhin (9^e circonscription) - Les Républicains

Type de question : Question écrite

Numéro de la question : 49644

Rubrique : Télécommunications

Ministère interrogé : Intérieur

Ministère attributaire : Intérieur

Date(s) clé(s)

Question publiée au JO le : [11 février 2014](#), page 1222

Réponse publiée au JO le : [20 mai 2014](#), page 4096