ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 23115	De **M. Frédéric Reiss** (Les Républicains - Bas-Rhin)	**Question écrite**
Ministère interrogé > Intérieur	**Ministère attributaire** > Intérieur	
Rubrique >sécurité des biens et des personnes	**Tête d'analyse** >Escroqueries sur internet	**Analyse** > Escroqueries sur internet.
Question publiée au JO le : **24/09/2019** Réponse publiée au JO le : **19/11/2019** page : **10154**		

Texte de la question

M. Frédéric Reiss interroge M. le ministre de l'intérieur au sujet des escroqueries sur internet. Avec le développement de l'utilisation d'internet et des services en ligne, il est aussi constaté un accroissement des escroqueries usant du numérique. De façon croissante, les services de police et de gendarmerie accueillent un public victime d'arnaques en ligne. Bien au-delà des simples offres d'enrichissement rapide et facile, les utilisateurs de messageries électroniques reçoivent aujourd'hui des courriels comprenant des en-têtes d'organismes bancaires ou des services fiscaux ou sociaux et se font proposer des remboursements sous réserve de fournir leurs coordonnées bancaires. Un examen très attentif de ces messages est parfois nécessaire pour s'apercevoir qu'il s'agit d'un faux. En parallèle, les tentatives de chantages basés sur des prétendues vidéos récupérées par *hacking* auprès des internautes se multiplient. Les futures victimes, souvent maîtrisant peu l'outil numérique, acceptent de s'acquitter d'une première somme par virement afin de récupérer les données, ce qui ouvre ensuite la voie à des échanges menant à des versements toujours plus importants. La gendarmerie relate aussi des exemples où les arnaqueurs sont allés jusqu'à se faire passer pour les forces de l'ordre et demandent une somme d'argent pour aider à piéger les fraudeurs, entretenant ainsi la victime dans l'erreur. Cette nouvelle forme de fraude, bien qu'en croissance permanente, est encore peu appréhendée, notamment du fait que beaucoup de victimes ne se font pas connaître par honte. La numérisation des démarches administratives imposant un recours accru à internet, ces usagers peu à l'aise sont d'autant plus confrontés à ce risque de malversations. En parallèle, malgré les efforts des forces de l'ordre locales, il faut relever qu'il s'agit d'une lutte inégale, tant ces arnaques font partie intégrante d'un large dispositif frauduleux très souvent géré depuis l'étranger afin de permettre la disparation des sommes extorquées. Face à l'ampleur de ce phénomène, il souhaite connaître les mesures spécifiques mises en place par le ministère pour lutter contre cette forme particulière d'abus de faiblesse, notamment en cherchant la coopération des États étrangers hébergeant ces malfaiteurs. En complément, il souhaite insister sur la nécessité d'accroître la communication en la matière envers le grand public.

Texte de la réponse

La lutte contre la cyberdélinquance constitue une priorité gouvernementale et du ministre de l'intérieur, qui mobilise les forces de sécurité intérieure. Police nationale et gendarmerie nationale ont structuré un dispositif national cohérent et en constante adaptation afin de faire face aux évolutions perpétuelles des cybermenaces. La spécificité du ministère repose, en outre, sur son maillage territorial et sur le travail de cohérence ministérielle que conduit le délégué aux industries de sécurité et à la lutte contre les cybermenaces, en lien étroit avec les directions générales de la police et de la gendarmerie nationales. Au sein de la police nationale, la lutte contre la

cyberdélinquance incombe à titre principal à la sous-direction de la lutte contre la cybercriminalité de la direction centrale de la police judiciaire (DCPJ), chargée du pilotage et de la coordination de la lutte contre la cybercriminalité sur le plan national. Elle s'attache à développer une réponse globale et transversale et à renforcer les partenariats avec les grandes sociétés de service de l'internet, notamment le secteur bancaire. Cette sous-direction comprend, en particulier, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), créé en 2000. L'Office abrite la plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS), qui gère le site www.internet-signalement.gouv.fr ouvert en 2009 et qui permet aux internautes et aux professionnels de signaler tout contenu illicite sur internet. Cette plate-forme, composée de 21 policiers et 8 gendarmes, prend en compte tous les contenus et usages illicites de l'internet, notamment les escroqueries. L'Office intègre également la plate-forme téléphonique d'information et de prévention sur les escroqueries (Info-Escroqueries) qui apporte, depuis sa création en 2009, une aide aux victimes. Les opérateurs d'Info-Escroqueries - soit 6 policiers, 3 réservistes de la police nationale et 2 gendarmes - ont pour mission de conseiller les victimes, sur le plan technique et juridique, de les orienter vers les services de police ou de gendarmerie et vers des services d'aide aux victimes. L'OCLCTIC coordonne au niveau national l'activité opérationnelle et judiciaire des services de police et de gendarmerie en matière de lutte contre la cybercriminalité. L'Office inclut dans ses structures une brigade à compétence nationale spécialisée qui diligente des enquêtes de fond et de portée internationale pour démanteler des réseaux d'escrocs organisés. A titre d'exemple, la plate-forme PHAROS et Ie service Info-Escroqueries ont reçu début 2019 de nombreux appels et signalements relatifs à des mels d'escroqueries par chantage aux vidéos pornographiques. L'OCLCTIC, chargé de cette affaire, a, par le biais du site www.cybermalveillance.gouv.fr, mis à la disposition des victimes un modèle de lettre-plainte ainsi qu'une messagerie fonctionnelle afin de les accompagner et de simplifier la procédure à suivre pour porter les faits à la connaissance des services de police. Ce dispositif a permis de récupérer de manière dématérialisée et centralisée les signalements afin de procéder à des rapprochements et déboucher sur une interpellation. Sur le plan de la formation, la DCPJ a mis en place avec les services de formation de la police nationale un dispositif pyramidal qui répond au besoin massif de l'ensemble des services de police de disposer de compétences en matière d'administration de la preuve numérique, notamment dans le cadre des enquêtes diligentées en matière d'escroqueries sur internet. Le dispositif de la police nationale s'appuie ainsi, au niveau territorial, sur des enquêteurs dénommés « primo-intervenants en cybercriminalité » et « investigateurs en cybercriminalité ». 15 laboratoires d'investigation opérationnelle du numérique, déployés dans les services territoriaux de la DCPJ et au sein de la préfecture de police, structurent le dispositif local et permettent la mutualisation d'outils et de compétences expertes. Leur déploiement se poursuit au niveau des services territoriaux de la police judiciaire. Afin d'offrir à nos concitoyens des moyens adaptés à l'ère numérique pour faciliter leurs démarches, et conformément à l'ambition de la police de sécurité du quotidien, le ministère de l'intérieur développe en outre des télé-services innovants. L'OCLCTIC de la DCPJ pilote ainsi un projet de plate-forme centralisée de prise de plainte en ligne pour les faits d'escroqueries commises sur internet. Cette plate-forme, dénommée THESEE, sera prochainement opérationnelle. Elle vise notamment à améliorer le service rendu aux victimes et à améliorer la lutte contre les escroqueries par la centralisation, l'analyse et le regroupement des plaintes et signalements. Son champ de compétence englobera notamment les escroqueries à la romance, les chantages à la webcam (« sextorsions »), les fausses annonces de vente ou de location et les rançongiciels (ou « ransomwares »). Il convient enfin de rappeler que les actions de prévention, d'assistance et d'information des victimes constituent des aspects essentiels à une véritable cybersécurité du quotidien. Le Gouvernement a ainsi lancé en octobre 2017 une plate-forme pour guider et accompagner les victimes de cybermalveillance (www.cybermalveillance.gouv.fr).