ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 8419	De **M. Vincent Ledoux** (UDI, Agir et Indépendants - Nord)	**Question écrite**

Ministère interrogé > Intérieur	**Ministère attributaire** > Intérieur

Rubrique >banques et établissements financiers	**Tête d'analyse** >Les moyens mis en œuvre pour lutter contre les escroqueries bancaires	**Analyse** > Les moyens mis en œuvre pour lutter contre les escroqueries bancaires.

Question publiée au JO le : **22/05/2018**
Réponse publiée au JO le : **20/11/2018** page : **10468**
Date de changement d'attribution : **16/10/2018**

Texte de la question

M. Vincent Ledoux appelle l'attention de M. le ministre d'État, ministre de l'intérieur, sur les débits frauduleux sur compte bancaire. L'Observatoire national de la délinquance et des réponses pénales (ONDRP) observe une forte hausse du nombre de ménages victimes d'au moins un retrait frauduleux, les déclarations enregistrées étant passé de 500 000 en 2010 à 1,2 million en 2017 - rien moins qu'un doublement en 6 ans. Un tiers des ménages se déclarent victimes d'escroqueries multiples, deux tiers d'entre elles pour un préjudice inférieur à 300 euros et 70 % découvrent la fraude en consultant leur relevé d'opération. La dernière note de l'Observatoire national de la délinquance et des réponses pénales, indique que près des deux tiers des ménages victimes en 2016 ignorent totalement comment l'auteur a procédé pour obtenir leurs coordonnées bancaires et que les sommes dérobées sont majoritairement utilisées pour effectuer des achats en ligne. De plus, on constate que la part des achats effectués à partir d'un site étranger augmente, passant de 16 % en 2014 à 24 % en 2016. Il lui demande donc de bien vouloir lui préciser les modalités mises en œuvre pour lutter contre les escroqueries bancaires et sensibiliser les clients.

Texte de la réponse

Les débits frauduleux sur compte bancaire constituent une part importante de la cybercriminalité. Selon le groupement d'intérêt économique (GIE) « cartes bancaires », le montant global de la fraude à la carte de paiement est toutefois en repli. Face à cette situation et plus largement face au développement de la cyberdélinquance, qui affecte les entreprises et nos concitoyens dans leur vie quotidienne, plusieurs mesures ont été prises, tant sur le plan de la prévention que de la répression. La sécurisation des transactions par carte bancaire est une préoccupation constante des pouvoirs publics et de la Banque de France. Les chiffres précités font apparaître que le déploiement de dispositifs de prévention par l'ensemble des acteurs concernés, aussi bien les émetteurs de moyens de paiement que les commerçants et les entreprises, porte ses fruits. Comme 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. Au sein du ministère de l'intérieur, la lutte contre la cyberdélinquance incombe : - à la police nationale, à titre principal, à la sous-direction de la lutte contre la cybercriminalité (SDLC) 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 ; - à la gendarmerie nationale, sur un échelon spécialisé, le centre de lutte contre les criminalités numériques (C3N – 60 spécialistes), et sur le réseau « Cybergend », fort à ce

jour de 3 500 enquêteurs. La SDLC 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. Composé de policiers et de gendarmes, 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. S'agissant des fraudes à la carte bancaire, l'OCLCTIC dispose de deux brigades d'enquêtes chargées de lutter à la fois contre les escroqueries sur internet et contre tout type de fraudes aux moyens de paiement. En matière de prévention, l'OCLCTIC a renforcé son partenariat avec la fédération bancaire française (FBF), le GIE « cartes bancaires » et les professionnels chargés de la production d'automates de paiement. L'OCLCTIC siège également au sein de l'observatoire de la sécurité des moyens de paiement (OSMP), qui réunit les acteurs concernés (émetteurs, autorités publiques, entreprises, commerçants, etc.) et permet de coordonner en amont des actions de prévention et de lutte contre les escroqueries sur l'ensemble des moyens de paiement scripturaux. La gendarmerie a organisé une chaîne complète de police judiciaire, dédiée à la lutte contre la criminalité numérique, intégrée et n'excluant aucun échelon territorial ou spécialisé. Pour les cas les plus complexes, la gendarmerie dispose de sept groupes spécialisés dans la lutte contre la cybercriminalité, au sein des sections de recherches implantées au chef-lieu des juridictions interrégionales spécialisées ; et d'une unité spécialisée nationale (le centre de lutte contre les criminalités numériques). Ces échelons spécialisés appuient et agissent en coordination étroite avec le réseau d'enquêteurs « Cybergend », afin de répondre aux demandes des victimes et faciliter l'enregistrement des plaintes ou le recueil des signalements. Ce réseau s'appuie sur 130 enquêteurs sur internet affectés dans les unités de police judiciaire spécialisées (sections de recherches et organismes centraux), 260 enquêteurs spécialisés NTECH (titulaires d'une licence professionnelle), plus de 3 100 enquêteurs qualifiés C-NTECH (correspondants en technologie numérique) répartis sur l'ensemble du territoire national. Par ailleurs, dans une démarche de proximité numérique avec le citoyen, la gendarmerie a ouvert début 2018 une brigade numérique. Cette unité remplit (sur internet) toutes les fonctions d'une brigade territoriale classique, à savoir un accueil en ligne sous forme d'interaction dématérialisée (formulaire de contact, dialogue sur les réseaux sociaux) 24h/24h et 7 jours/7. Les gendarmes de la brigade numérique sont devenus des acteurs de prévention dans l'espace numérique. Ils interviennent de façon proactive sur certains espaces numériques (forums, réseaux sociaux) et vont à la rencontre de certains publics particulièrement ciblés. A ce titre, la brigade numérique se révèle particulièrement adaptée pour répondre aux besoins des victimes d'usages frauduleux de carte bancaire sur internet. La lutte contre la cybercriminalité, et les menaces qu'elle représente pour nos concitoyens, les entreprises et les collectivités, constitue une priorité du Gouvernement. Dans ce contexte, la mobilisation des services du ministère de l'intérieur – doté d'une délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC) - se poursuit et s'amplifie. Par circulaire du 9 avril 2018, le ministre de l'intérieur a rappelé aux forces de police et de gendarmerie qu'il s'agit d'un enjeu primordial de la protection de nos concitoyens. Il convient également de souligner que le ministre de l'intérieur a décidé que 800 des 10 000 postes de policiers et de gendarmes supplémentaires qui seront créés durant le quinquennat seront dédiés à la cybersécurité. A la demande du ministre de l'intérieur, la DMISC présentera en outre prochainement une « feuille de route » qui visera à renforcer encore les capacités d'action de l'État. Il convient également 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). Enfin, 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 (PSQ), le ministère de l'intérieur développe des télé-services innovants. Le télé-service PERCEVAL a ainsi été lancé en juin 2018. Il s'agit d'une plate-forme de recueil des signalements d'usages frauduleux de carte bancaire en ligne. Par ailleurs, l'OCLCTIC pilote un projet de plate-forme centralisée de prise de plainte en ligne, complémentaire de PERCEVAL, pour les faits d'escroquerie commis sur internet. Cette plate-forme, dénommée THESEE, devrait être opérationnelle en 2019.