ASSEMBLÉE NATIONALE

14ème legislature

Question N° : 70413	De **M. Georges Ginesta** (Union pour un Mouvement Populaire - Var)	**Question écrite**

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

Rubrique >moyens de paiement	**Tête d'analyse** >cartes bancaires	**Analyse** > paiement sans contact. données. sécurisation.

Question publiée au JO le : **02/12/2014**
Réponse publiée au JO le : **16/06/2015** page : **4582**

Texte de la question

M. Georges Ginesta attire l'attention de M. le ministre de l'intérieur sur les risques de piratage des cartes bancaires permettant le paiement sans contact. En effet, grâce à la technologie NFC (communication de proximité), les nouvelles cartes bancaires permettent de payer jusqu'à vingt euros en approchant seulement sa carte ou son smartphone à trois centimètres d'un terminal de paiement. Or, d'après certaines sources, un simple lecteur permettrait à une personne malintentionnée de récupérer les données stockées sur ce type de cartes bancaires pour en faire un usage prohibé. C'est pourquoi il lui demande de bien vouloir lui indiquer si ses services ont eu connaissance de telles pratiques et les mesures qu'il entend prendre afin de poursuivre les auteurs de tels agissements.

Texte de la réponse

La sécurisation des transactions par carte bancaire est une préoccupation constante des pouvoirs publics, notamment de la Banque de France qui est chargée « d'assurer la sécurité des moyens de paiement » en application de la loi du 15 novembre 2001 relative à la sécurité quotidienne. Les réseaux criminels tirent en effet profit du développement d'Internet et de la multiplication des échanges commerciaux en ligne pour mettre en place de nouveaux modes opératoires, par exemple pour commettre des escroqueries, s'approprier frauduleusement des données confidentielles de personnes effectuant des achats en ligne, etc. Selon le groupement d'intérêt économique des cartes bancaires, le montant des fraudes à la carte bancaire s'est élevé à 360 millions d'euros en 2013, soit + 8 % par rapport à 2012. Ces fraudes impactent essentiellement les ventes à distance et l'augmentation du phénomène doit à cet égard être mise en perspective avec l'essor du e-commerce (+ 11 % en 2013). Il y a lieu également de souligner que le taux de fraude est de 0,3 % dans le e-commerce et de 0,014 % dans le commerce de proximité. En matière de commerce de proximité, la France détient le taux de fraude le plus bas du monde. Plusieurs mesures ont été prises pour lutter contre les faits de cyber-délinquance, qui affectent nos concitoyens dans leur vie quotidienne, mais aussi les entreprises. Le code monétaire et financier comporte des dispositions pénales permettant de réprimer la contrefaçon ou la falsification d'une carte de paiement et l'usage d'une carte falsifiée ou contrefaite. La répression de l'infraction d'utilisation d'instruments de paiement falsifiés, si elle est commise en bande organisée, a été aggravée par la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, qui a par ailleurs créé une incrimination relative à l'utilisation frauduleuse de données à caractère personnel de tiers sur internet. Comme d'autres acteurs publics et privés, les forces de sécurité de l'Etat, qui disposent de structures dédiées, consacrent d'importants moyens à la lutte contre la cybercriminalité sous toutes ses formes. L'action de la police nationale et de la gendarmerie nationale s'appuie sur un réseau territorial d'environ 650 enquêteurs spécialisés (investigateurs en cybercriminalité de la police (ICC) et enquêteurs en technologies

numériques (NTECH) de la gendarmerie). Elle revêt également une forte dimension internationale, dans le cadre de diverses enceintes (Union européenne et notamment Europol, Conseil de l'Europe, Interpol, etc.) ou missions techniques bilatérales. Au sein du ministère de l'intérieur, la lutte contre la cyber-délinquance incombe pour la police nationale à la sous-direction de la lutte contre la cybercriminalité de la direction centrale de la police judiciaire (DCPJ), mais également aux services de la préfecture de police de Paris (brigade d'enquêtes sur les fraudes aux technologies de l'information, brigade des fraudes aux moyens de paiement, brigade de répression de la délinquance astucieuse...). Pour sa part, la gendarmerie nationale dispose également de structures dédiées pour lutter contre ce phénomène. Le centre de lutte contre les criminalités numériques (C3N) et la division criminalistique ingénierie et numérique de l'institut de recherche criminelle de la gendarmerie nationale sont actifs respectivement dans les investigations en ligne contre les fraudes à la carte bancaire sur Internet et dans les actes de police technique liés à ces phénomènes. Ils ont ainsi fait preuve d'une réelle réactivité en 2013-2014 face à un phénomène de terminaux de paiement électroniques piégés, permettant le recueil à distance de données des cartes bancaires (numéros et code PIN). La mise en place de dispositifs de détection des terminaux piégés ont permis à des services de police et de gendarmerie de procéder à des interpellations. La sous-direction de la lutte contre la cybercriminalité de la DCPJ, créée par arrêté du 29 avril 2014, est chargée du pilotage et de la coordination de la lutte contre la cybercriminalité sur le plan national pour les services de la police nationale. Elle s'attache à développer une réponse globale et transversale et à renforcer les partenariats avec les grandes sociétés de service de l'Internet, particulièrement avec le milieu 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 par décret du 15 mai 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 permettant aux internautes et professionnels de signaler tout contenu illicite sur internet. S'agissant plus particulièrement des fraudes à la carte bancaire, il doit être souligné que l'OCLCTIC dispose d'un groupe opérationnel d'enquête chargé de lutter contre les escroqueries sur Internet (fraude à la carte de paiement utilisée pour les ventes à distance par exemple). Par ailleurs, en matière de prévention, l'OCLCTIC a renforcé son partenariat avec la fédération bancaire française, le groupement d'intérêt économique des cartes bancaires et les professionnels chargés de la production d'automates de paiement. L'OCLCTIC et la gendarmerie siègent également à l'Observatoire de la sécurité des cartes de paiement, qui réunit les acteurs concernés (administrations publiques, secteur bancaire, représentants des consommateurs et des commerçants...) et permet de coordonner en amont des actions de prévention et de lutte contre les escroqueries en matière de cartes bancaires. La prévention est essentielle, notamment en matière de sécurisation des opérations de paiement par carte via Internet (dispositifs d'authentification « non rejouable » de technologie « 3D-Secure »...). Les axes d'amélioration reposent également sur une harmonisation des exigences sécuritaires par les autorités de régulation bancaire aux niveaux européen et international. En tout état de cause, une prévention efficace de la cyber-délinquance passe d'abord par une sensibilisation des internautes, qui doivent faire preuve au quotidien de vigilance. PHAROS 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. S'agissant de la sécurité des cartes de paiement sans contact, ce sujet est suivi par la gendarmerie nationale en liaison avec les acteurs du monde bancaire. Elle n'a pas détecté, à ce stade, de phénomène de fraude, liée à cette nouvelle modalité de paiement. La gendarmerie s'appuie également sur son réseau territorial. Sous la coordination de la direction générale, elle met en place, au besoin, des cellules d'enquête sur des fraudes aux cartes bancaires. S'agissant des escroqueries commises sur Internet, l'OCLCTIC, en association avec la gendarmerie nationale, est chargé de la mise en place d'une plate-forme centralisée de prise de plainte en ligne. Ce projet est conforme à la recommandation n° 50 du rapport récemment remis par un groupe de travail interministériel chargé d'élaborer une stratégie globale de lutte contre la cybercriminalité (voir ci-dessous). De manière plus générale, il doit être souligné que, 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 les cyber-menaces. A la suite du séminaire gouvernemental sur le numérique de février 2013, un groupe de travail interministériel (Justice/Economie/Intérieur/Economie numérique), présidé par un procureur général, a été institué 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. Ce rapport interministériel (Protéger les internautes) a été remis le 30 juin 2014 et comporte une cinquantaine de propositions, qui sont à l'étude dans les départements ministériels concernés. Par ailleurs, le ministre de l'intérieur a demandé début 2014 aux directeurs généraux de la police nationale et de la gendarmerie nationale et au préfet de police de Paris de définir un plan d'action spécifique. Le rapport sur la Lutte contre les cyber-menaces en matière de sécurité intérieure a été remis au ministre de l'intérieur le 31 mai 2014. Il recouvre les principaux enjeux suivants : adéquation du dispositif opérationnel à la menace en termes de moyens juridiques, organiques, humains et matériels ; prise en compte des contentieux de masse par une approche innovante et efficace ; développement de la coopération internationale ; développement des partenariats industriels et académiques. Dans ce cadre, le préfet Jean-Yves Latournerie a été nommé en novembre 2014 préfet en charge de la lutte contre les cyber-menaces auprès du ministre de l'intérieur. D'ores et déjà, la création, évoquée plus haut, d'une sous-direction spécifique au sein de la DCPJ répond à l'une de ses recommandations.