ASSEMBLÉE NATIONALE

14ème législature

cartes bancaires

Question écrite n° 55420

Texte de la question

M. Jean-Louis Christ appelle l'attention de M. le ministre de l'intérieur sur e développement des escroqueries à la carte bancaire. Selon une étude réalisée par l'Observatoire national de la délinquance et des réponses pénales, 700 000 ménages se sont déclarés victimes d'au moins un débit frauduleux en 2012, alors qu'on ne recensait que 500 000 déclarations similaires en 2010. Or, selon la même étude, seulement un tiers des victimes ont été averties par leur banque d'une ou de plusieurs opérations suspectes sur leurs comptes. L'absence d'avertissement systématique de la banque et le défaut de vigilance des clients favorisent la perpétuation des fraudes, dont on ne connaît pas l'origine dans 60 % des cas. Il lui demande quelles mesures il entend mettre en œuvre pour endiguer le développement des fraudes à la carte bancaire dans notre pays.

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. Plusieurs mesures ont été prises pour lutter contre ces phénomènes, qui affectent nos concitoyens dans leur vie quotidienne, mais aussi les entreprises et les administrations publiques. Le code monétaire et financier comporte des dispositions pénales permettant de réprimer la contrefaçon ou la falsification d'une carte de paiement, 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, est plus sévère (dix ans d'emprisonnement et un million d'euros d'amende) depuis 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. Aux côtés d'autres acteurs publics et privés, les forces de sécurité de l'Etat consacrent d'importants moyens à la lutte contre les cybermenaces. 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. Cet office central, composé de policiers et de gendarmes, 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). Une plate-forme téléphonique nationale d'information et de prévention sur les escroqueries est à la disposition du public pour répondre aux interrogations des victimes et les guider dans leurs démarches. Un site (www. internet-signalement. gouv. fr) est à la disposition des particuliers et des professionnels pour signaler en ligne tout contenu illicite de l'Internet. Ces signalements, qui peuvent être le point de départ d'enquêtes pénales, sont traités par la plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS), placée au sein de l'OCLCTIC. Au regard du caractère

transnational des affaires, le ministère de l'intérieur s'attache également à développer la coopération avec les pays concernés, européens ou autres. 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 siège 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 ce type d'escroqueries. La prévention, notamment technique, est essentielle et le dernier rapport de l'Observatoire de la sécurité des cartes de paiement fait état de réelles avancées en matière de sécurisation des opérations de paiement par carte bancaire via Internet. Toutefois, le déploiement de dispositifs d'authentification « non rejouable » et, partant, de la technologie « 3D-Secure », auprès des e-commerçants reste une priorité pour l'Observatoire de la sécurité des cartes de paiement. Une meilleure sécurisation exige aussi une poursuite des actions engagées en sensibilisant encore davantage le porteur de carte, les banques, les e-commerçants et commerçants afin d'accroître le niveau de coopération entre ces acteurs. 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 cyberdélinquance passe d'abord par une sensibilisation des internautes, qui doivent, au quotidien, faire preuve de vigilance. 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 cybermenaces. Il est en effet indispensable 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 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. Ses travaux sont achevés et son rapport devrait prochainement être remis. 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 franchir de nouvelles étapes en matière de capacités de réponse aux cybermenaces, tant préventives qu'administratives ou de police judiciaire. L'objectif est, notamment, d'optimiser les organisations internes au ministère et de développer une action tout à la fois transverse, globale et lisible, intégrant une politique de prévention, des dispositifs de répression et des capacités d'anticipation. Le rapport final devrait être prochainement remis au ministre. 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 la lutte contre cette délinquance.

Données clés

Auteur : M. Jean-Louis Christ
Circonscription : Haut-Rhin (2e circonscription) - Les Républicains
Type de question : Question écrite
Numéro de la question : 55420
Rubrique : Moyens de paiement
Ministère interrogé : Intérieur
Ministère attributaire : Intérieur

Date(s) clée(s)

Question publiée au JO le : 13 mai 2014, page 3793
Réponse publiée au JO le : 29 juillet 2014, page 6522