ASSEMBLÉE NATIONALE

14ème législature

cartes bancaires

Question écrite n° 87940

Texte de la question

M. Bernard Perrut attire l'attention de M. le ministre de l'intérieur sur les 800 000 ménages victimes d'une escroquerie bancaire, selon l'analyse de l'Observatoire national de la délinquance et des réponses pénales (ONDRP) sur les escroqueries bancaires constatées par les ménages français sur leurs comptes, selon ce qu'ils ont déclaré lors des enquêtes dites de victimation menées entre 2011 et 2014 par l'ONDRP et l'Insee. Elle révèle ainsi que le nombre de ménages victimes de débits frauduleux sur leurs comptes bancaires a augmenté « de façon régulière » depuis 2010 et que près des deux tiers des victimes avouent ne pas connaître le mode opératoire employé par l'auteur de l'infraction, et qu'un « tiers ont vu leurs informations bancaires dérobées tandis qu'elles avaient effectué un achat sur Internet ». Aussi, il lui demande les actions qu'il entend mettre en œuvre pour mettre fin à ces escroqueries.

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 profitent en effet du développement d'internet et 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 global de la fraude en matière de cartes bancaires était de 387 millions d'euros en 2014, chiffre à mettre en perspective avec le montant total des transactions, qui s'élève à 545 milliards d'euros. En 2015, le montant estimé global de la fraude a continué de progresser légèrement à 402 millions d'euros (pour un montant total de transactions de 565 milliards d'euros). La vente à distance (VAD) représente plus des deux tiers de la fraude. Pour la première fois depuis plus de 10 ans, le montant de la fraude « domestique » (porteurs de carte bancaire en France) a cependant diminué en 2015 par rapport à 2014 dans chacun des trois secteurs d'activité des cartes bancaires (paiements de proximité, retraits aux distributeurs automatiques et paiements à distance), tant en valeur qu'en taux (0,040 % en 2015 contre 0,043 % en 2014).Toutes opérations confondues, 868 400 cartes françaises ont fait l'objet d'au moins un piratage l'an dernier (soit - 4 % par rapport à 2014). Pour les paiements effectués à l'étranger avec des cartes françaises, le taux de fraude est globalement moins élevé quand ils sont effectués au sein de l'espace SEPA grâce aux efforts entrepris en Europe au cours des dernières années pour renforcer la sécurité des paiements (généralisation du standard EMV, recours à l'authentification forte notamment via la technologie 3D-Secure), alors que d'autres zones géographiques (notamment l'Asie et les États-Unis) sont encore en phase de migration vers le standard EMV. La progression de cette migration devrait, à terme, conduire à une meilleure maîtrise de la fraude aux points de vente et aux automates pour les porteurs de cartes françaises. 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. 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. La loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale a permis de poursuivre l'adaptation de notre arsenal législatif aux évolutions de cette délinquance, en fixant en particulier un nouveau critère de compétence territoriale qui permettra désormais à la justice française de connaître des faits commis en dehors du territoire national dès lors que la victime de cybermalveillance réside en France. 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 (N-TECH) de la gendarmerie). Elle revêt également une forte dimension internationale, dans le cadre de diverses enceintes (Union européenne, Conseil de l'Europe, Interpol, etc.) ou de missions techniques bilatérales. Au sein du ministère de l'intérieur, 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), qui s'appuie sur un réseau de policiers spécialisés au sein des services territoriaux de la police judiciaire. D'autres services de police concourent à la lutte contre la cybercriminalité, par exemple au sein 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). La gendarmerie nationale dispose aussi de structures spécifiques, notamment 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 (DCIN). Le C3N assure une triple mission d'enquête judiciaire (notamment sur des escroqueries sérielles touchant de multiples victimes sur l'ensemble du territoire national, ou sur des escroqueries de grande ampleur au préjudice de grands commerçants en ligne), d'appui opérationnel aux unités de terrain, et d'exploitation du renseignement criminel. A ce titre, le C3N recueille chaque mois une synthèse de l'ensemble des faits de cybercriminalité recensés par les unités de gendarmerie de terrain : sur les 5.000 faits mensuels (augmentation de +10 % sur les 12 derniers mois), 80 % portent sur des escroqueries en ligne (proportion constante). L'analyse de ces faits éparpillés permet d'effectuer des recoupements et de proposer des stratégies de centralisation à l'autorité judiciaire. A travers le département informatique-électronique de la DCIN, l'Institut de recherche criminelle de la gendarmerie nationale a développé depuis plusieurs années une très forte compétence dans l'expertise scientifique des dispositifs de piratage de cartes bancaires (skimmers). Ce département a également développé un outil préventif de détection de certains terminaux de paiement piratés. La sous-direction de la lutte contre la cybercriminalité de la direction centrale de la police judiciaire, 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. Elle s'attache à développer une réponse globale et transversale et à renforcer les partenariats avec les acteurs concernés : grandes sociétés de service de l'internet, secteur bancaire, etc. 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, dont les effectifs ont été significativement renforcés en 2015. 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. 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 plus particulièrement des fraudes à la carte bancaire, l'OCLCTIC dispose de deux groupes opérationnels d'enquêtes chargés 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 et la gendarmerie ont renforcé leur partenariat avec la Fédération bancaire française (FBF), le GIE « cartes bancaires » et les professionnels chargés de la production d'automates de paiement. L'OCLCTIC et la gendarmerie siègent également au sein de l'Observatoire de la sécurité des cartes de paiement, qui réunit les acteurs concernés (administrations publiques, secteur bancaire, représentants des consommateurs et des commerçants, etc.) et permet de coordonner en amont des actions de prévention et de lutte contre les escroqueries. La prévention, enjeu essentiel, passe surtout par une sensibilisation des particuliers, qui doivent faire preuve au quotidien de vigilance, et par la mise en œuvre des

protocoles sécurisés de paiement en ligne par les commerçants (ex. : Visa 3D-Secure). Un colloque organisé par la Banque de France en janvier 2016 sur les perspectives de développement de l'usage des cartes bancaires, au regard notamment des problèmes de fraude, a été l'occasion de renforcer encore le dialogue entre les pouvoirs publics, les acteurs du marché et les institutions européennes. S'agissant des escroqueries commises sur internet, l'OCLCTIC et la gendarmerie co-pilotent actuellement un projet de plate-forme centralisée de signalement et de prise de plainte en ligne, conformément à l'une des recommandations du rapport de février 2014 (Protéger les internautes) élaboré par le groupe de travail interministériel sur la lutte contre la cybercriminalité, institué à la suite du séminaire gouvernemental sur le numérique de février 2013. Plus généralement, il convient de souligner que le ministère de l'intérieur a fait de la cybersécurité une priorité et s'est doté d'un plan d'action ministériel spécifique qui vise, entre autres, à mieux accompagner les victimes de cybermalveillance. L'action du ministère de l'intérieur s'inscrit pleinement dans la Stratégie nationale pour la sécurité du numérique présentée le 16 octobre 2015 par le Premier ministre.

Données clés

Auteur : M. Bernard Perrut
Circonscription : Rhône (9e circonscription) - Les Républicains
Type de question : Question écrite
Numéro de la question : 87940
Rubrique : Moyens de paiement
Ministère interrogé : Intérieur
Ministère attributaire : Intérieur

Date(s) clée(s)

Question publiée au JO le : 8 septembre 2015, page 6782
Réponse publiée au JO le : 13 décembre 2016, page 10357