ASSEMBLÉE NATIONALE

14ème legislature

Question N° : 30470	De **M. Pascal Popelin** (Socialiste, républicain et citoyen - Seine-Saint-Denis)	**Question écrite**
Ministère interrogé > Économie sociale et solidaire et consommation	**Ministère attributaire** > Économie sociale et solidaire et consommation	
Rubrique >moyens de paiement	**Tête d'analyse** >cartes bancaires	**Analyse** > données. sécurisation.
Question publiée au JO le : **25/06/2013** Réponse publiée au JO le : **22/10/2013** page : **11086**		

Texte de la question

M. Pascal Popelin alerte M. le ministre délégué auprès du ministre de l'économie et des finances, chargé de l'économie sociale et solidaire et de la consommation, sur le manque de sécurisation des données bancaires des clients des hôtels. Il est fréquent de la part des établissements hôteliers de demander aux clients de présenter une carte bancaire pour effectuer une réservation ou garantir les éventuels « extras ». Il arrive alors que certains professionnels relèvent à la fois les 16 chiffres du recto de la carte et les 3 chiffres composant le cryptogramme nécessaire au paiement. Bien que des prélèvements indus sur un compte bancaire soient garantis par l'établissement teneur du compte, ils peuvent engendrer de forts désagréments en cas d'indélicatesse. Aussi, il lui demande de préciser quelles modalités le Gouvernement pouvait proposer pour sécuriser les données bancaires de ces clients.

Texte de la réponse

Les opérations frauduleuses sur les cartes bancaires font en effet l'objet d'un encadrement juridique très strict qui permet au porteur de la carte de bonne foi de ne pas voir sa responsabilité engagée. En tout état de cause, l'utilisation même de la carte ne suffit pas en tant que telle à prouver que l'opération a été autorisée par le payeur, ni même que celui-ci a fait preuve de négligence. Il appartient au prestataire de services de paiement de prouver que l'opération non autorisée par le client a été authentifiée et quand la fraude est constatée, il doit, le cas échéant, rétablir le compte dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu. Outre le régime juridique évoqué qui protège les utilisateurs de cartes, la sécurisation des transactions par carte bancaire est régie notamment par les articles 34 à 39 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, modifiant les dispositions des articles L. 132-2 à L. 132-6 et L. 141-4 du code monétaire et financier. Cette loi charge expressément la Banque de France « d'assurer la sécurité des moyens de paiement » et institue l'observatoire de la sécurité des cartes de paiement (OSCP). Cette instance de concertation qui rassemble toutes les parties concernées (consommateurs, commerçants, émetteurs et autorités publiques) adresse ainsi chaque année un bilan annuel sur les taux de fraude constatée sur les transactions par carte, tant à distance qu'en face à face, au plan national comme international. En ce qui concerne 2012, le rapport de l'OSCP du 1er juillet 2013 fait état cette année encore d'un montant de la fraude en augmentation affectant les paiements par carte bancaire en France. Il représente en effet un taux de 0,080 % contre 0,077 % en 2011 soit 450,7 millions d'euros. Cette augmentation de la fraude s'explique tout d'abord par une augmentation significative d'escroqueries sur les transactions internationales (+ 11,2 %) ou sur les paiements réalisés avec des cartes françaises auprès de commerçants étrangers (+ 37 %) ; elle apparaît plus maîtrisée sur les transactions nationales (+ 7,1 %) même si l'observatoire relève par ailleurs une hausse certaine des attaques de DAB (distributeurs automatiques de billets) ou de points de vente. En

revanche, l'observatoire constate pour la première fois depuis 2008 un léger infléchissement de la fraude sur les paiements par internet opérés auprès de sites français (0,290 % en 2012 contre 0,341 % en 2011). En prenant l'exemple de certains hôtels qui relèvent tous les chiffres portés sur la carte bancaire, les données sensibles qu'ils représentent, dès lors non protégées, sont susceptibles de faire l'objet d'utilisations frauduleuses, notamment pour des paiements à distance nécessitant la seule retranscription des éléments chiffrés. Cet excès de transparence expose ainsi fortement le détenteur de la carte. C'est pourquoi, pour réduire ce risque, les pouvoirs publics sont favorables à la diffusion des dispositifs d'authentification « non rejouable », comme le « 3D-Secure » mis en place depuis le 1er octobre 2008. En effet, avec ce type de dispositif, les informations contenues sur la carte bancaire ne peuvent à elles seules permettre une transaction puisqu'un code unique est délivré par SMS pour chaque opération. Cette sécurisation du paiement pour le titulaire de la carte garantit en outre la responsabilisation de la banque émettrice qui, si elle a admis l'authenticité du paiement, devient seule responsable en cas d'impayé. L'OSCP relève un accroissement des paiements sécurisés via ce type de dispositif qui représentent en 2012, 27,5 % des paiements en montant, contre 23 % en 2011 et appelle l'ensemble des acteurs à généraliser les dispositifs permettant l'authentification renforcée du porteur de la carte chaque fois que cela est possible et pertinent. Enfin, l'observatoire s'intéresse parallèlement à la sécurité des modes de paiement sans contact, suite à l'accroissement sensible du nombre de cartes et de terminaux de paiement de ce type. D'usage rapide et simple, ce mode de paiement n'est actuellement utilisé que pour des transactions de faibles montants. Il ne nécessite pas de la part du payeur d'avoir à insérer sa carte ni de composer son code confidentiel. Il suffit seulement de déposer la carte ou un téléphone mobile devant un terminal de paiement. L'observatoire, qui vise sa propagation pour satisfaire à l'évolution des moyens de paiement, a dû toutefois formuler des recommandations à l'adresse des banques notamment pour favoriser une meilleure confiance dans l'emploi de ce dispositif innovant afin de lui assurer dans l'avenir le maximum de sécurité pour des montants plus importants.