Commerce électronique et sécurité des paiements en ligne

Nadia ANTONIN, animatrice du groupe de travail Commerce électronique de l'Académie des Sciences commerciales est l'auteur de : **Commerce électronique et sécurité des paiements en ligne** rédigé en septembre 2016.

Le commerce électronique[1] connaît un essor rapide au niveau mondial. Son chiffre d'affaires s'est élevé à 1.671 milliards de dollars en 2015, soit une hausse de 25% par rapport à 2014. En France, 835 millions de transactions ont été effectuées en ligne en 2015 pour un montant total de 64,9 milliards d'euros (+14% par rapport à 2014). Selon la Fédération e-commerce et de la vente à distance (FEVAD), 78,3% des internautes français ont fait un achat en ligne en 2015 (35,5 millions d'acheteurs en ligne). Par ailleurs, 50% des acteurs de la vente en ligne implantés en France reçoivent des commandes de clients localisés à l'étranger. La France se place à la cinquième place du commerce en ligne dans le monde, derrière le Royaume Uni (3ème) et le Japon (4ème). Le marché du commerce électronique en France devrait progresser de 10% en 2016 et franchir la barre des 70 milliards d'euros.

Si les avantages du commerce électronique sont indéniables et notamment l'accès au marché mondial pour les entreprises, il apparaît que celui-ci se heurte à certains obstacles. Un de ses principaux freins est lié à la sécurité des transactions. Différentes études prouvent que les failles dans la sécurité des paiements sur internet freinent le développement du commerce électronique. Le rapport annuel de l'Observatoire de la sécurité des cartes de paiements publié par la Banque de France en juillet 2016 révèle que le nombre d'opérations frauduleuses a continué à fortement progresser pour les paiements transfrontaliers en 2015 et que les achats sur des sites de e-commerce étrangers restent problématiques. En outre, le rapport souligne que la sécurisation des transactions de proximité, qui ont enregistré une baisse continue de la fraude, a entraîné un report de cette dernière sur les paiements via internet, qui supportent désormais les 2/3 de la fraude globale. Dans ce contexte de fraude, certains consommateurs estiment que transmettre à un site de commerce électronique leurs coordonnées bancaires ou leur numéro de carte est risqué.

Après avoir dressé un état des lieux des principaux instruments de paiement en ligne, nous examinerons les solutions envisagées pour renforcer la confiance des acheteurs et des vendeurs dans les moyens de paiement en ligne et dans le commerce électronique en général.

1. Etat des lieux de la sécurité des paiements en ligne

Les Assises des moyens de paiement qui se sont tenues en mai 2015, ont souligné l'augmentation des problèmes de sécurité pour les paiements par internet.

Pour illustrer ces propos, nous allons faire un tour d'horizon des principaux instruments de paiement en ligne.

- ***Le paiement par carte bancaire***

Créée à l'origine pour les paiements de proximité, la carte bancaire s'est rapidement affirmée comme l'instrument le plus utilisé en France pour effectuer un règlement sur internet. Selon la

[1] "*Utilisation combinée et optimale des TIC qui permettent d'assurer et de développer les transactions d'affaires* ". (Source : Dictionnaire de l'EDI et du Commerce électronique/EDIFRANCE).

FEVAD, 80% des acheteurs français déclarent utiliser la carte bancaire pour leurs achats en ligne.

Cela étant, les statistiques révèlent que le paiement par carte bancaire est particulièrement touché par la fraude. Dès lors, pour redonner confiance aux achats et ventes en ligne et protéger les consommateurs ainsi que les commerçants contre toutes les fraudes au paiement à distance, les autorités françaises ont pris des dispositions en faveur de la sécurité des paiements. Ainsi par exemple, la sécurisation des paiements par carte sur internet est depuis plusieurs années la mission première de l'Observatoire de la sécurité des cartes de paiement de la Banque de France.

Les mesures adoptées visent notamment l'authentification renforcée du porteur de la carte bancaire. Ainsi, la Banque de France a imposé en juin 2010 à toutes les banques françaises le dispositif **3D-Secure** qui permet d'authentifier le porteur d'une carte de paiement de manière renforcée à l'occasion, par exemple, d'un achat sur internet. L'acheteur doit saisir un code d'authentification à usage unique, reçu le plus souvent par SMS, pour valider le règlement de ses achats.

Face à la réticence des acheteurs en ligne de communiquer leur numéro de carte en raison de la fraude, d'autres solutions de paiement sont apparues comme le paiement avec une e-carte bleue.

- ***Le paiement avec une e-carte bleue***

Certains organismes bancaires proposent la e-carte bleue qui permet d'effectuer des achats en ligne sur tous les sites marchands en France et à l'étranger, sans communiquer le numéro de la carte réelle. En fait, c'est une carte virtuelle rattachée à la carte réelle qui est générée par l'établissement bancaire pour une transaction précise. Cette carte virtuelle, à usage unique, ne peut être réutilisée pour une tout autre transaction et est valable pour un montant déterminé, un commerçant unique et une durée déterminée.

- ***Paiement par virement SEPA***

Le virement SEPA, mis en place progressivement depuis 2008, permet de payer en euros dans l'Union européenne ainsi qu'en Islande, en Norvège, au Liechtenstein, en Suisse, à Monaco et à Saint Marin. Dans le cadre des Assises des moyens de paiement de mai 2015, il a été rappelé que celui-ci, "*très utilisé dans les autres pays européens, a un potentiel de développement important en France, aux côtés de la carte bancaire, notamment pour les paiements par internet et par mobile*". Cependant, cet instrument de paiement est victime d'un taux de fraude qui progresse fortement malgré les mesures de sécurité mises en place.

- ***Paiement sur des sites sécurisés (PayPal, PayLib, etc.)***

Paypal est la première solution de paiement en ligne dans le monde qui permet d'effectuer des achats sans communiquer ses coordonnées bancaires, en s'identifiant uniquement avec son adresse électronique et un mot de passe. Malgré les dispositions prises en matière de sécurité des comptes PayPal, d'aucuns rapportent que ces derniers n'ont pas été exempts de piratage. D'où le lancement par trois banques (Banque Postale, BNP Paribas et Société Générale d'un nouveau système de paiement dénommé PayLib qui permet de faire ses achats en ligne sur son ordinateur, sa tablette ou son téléphone portable. A l'image de Paypal, ce nouveau système évite aux acheteurs de communiquer leurs coordonnées bancaires directement sur le site du commerçant. Au moment de payer, le client renseigne uniquement son identifiant PayLib et son mot de passe. Les atouts du système PayLib et notamment le fait d'intégrer une

approche des risques pour les paiements sur internet (mécanisme d'authentification non rejouable) sont certes indéniables mais ils restent à confirmer.

- ***Le portefeuille électronique ("wallet")***

Certains sites proposent d'utiliser un portefeuille électronique pour payer en ligne un achat effectué sur internet. Le rapport annuel 2011 de l'Observatoire sur la sécurité des cartes de paiement de la Banque de France définit le portefeuille électronique comme "*la solution permettant à un utilisateur de confier à un tiers, jugé de confiance, des données de paiement et des données personnelles, stockées en vue d'effectuer ultérieurement notamment des ordres de paiement*". Cette solution peut être proposée par des acteurs comme PayPal, le Crédit Mutuel avec l'offre Pay2You, des opérateurs téléphoniques avec l'offre Buyster et des systèmes de paiement par carte tels que Cartes Bancaires, Visa ou MasterCard.

Le portefeuille électronique est exposé, comme les autres instruments de paiement en ligne, à différents risques liés à la concentration des données sensibles et à la réutilisation de ces données à l'insu de leur titulaire légitime. D'où la nécessité, comme le préconise le rapport précité, de protéger les données sensibles et de vérifier l'identité du porteur, lors de l'enregistrement de sa carte ou de l'utilisation de son portefeuille électronique.

- ***Paiement par mobile ("m-payment")***

Le concept de paiement par mobile désigne généralement les différents usages d'un smartphone pour effectuer un paiement. L'usage le plus fréquent du paiement par mobile se réalise dans le domaine du commerce électronique et ressemble à un paiement effectué sur un ordinateur à l'aide d'une carte bancaire ou d'un compte PayPal.

La part des paiements par mobiles poursuit sa forte progression dans tous les pays du monde. Selon l'Index mondial des paiements mobiles, la part des paiements mobiles en France s'élève à 22,9% des paiements en ligne en mars 2015 contre 16,2% en mars 2014.

Les principaux risques liés au paiement par mobile sont bien évidemment le vol ou la perte du smartphone.

2. Comment renforcer la confiance des acteurs du commerce électronique ?

Un renforcement de la sécurité des paiements sur internet est indispensable pour réduire les risques de fraude et rétablir la confiance des acteurs du commerce électronique.

- **Un renforcement des systèmes de sécurité des paiements en ligne**
  - ***Une authentification forte :*** l'authentification consiste à vérifier que l'acteur du paiement est bien la personne morale ou physique qu'il prétend être. Il est important que ces acteurs – l'acheteur, le commerçant et la banque – puissent vérifier leur identité respective. A cet égard, l'Observatoire de la sécurité des cartes de paiement note que "*les évolutions des cadres règlementaires en Europe, dont la Directive européenne révisée sur les services de paiement (DSP2) visent systématiquement le recours à l'authentification forte du porteur de carte pour les transactions à distance*". En outre, pour renforcer toujours plus la sécurité des paiements en ligne, les banques s'équipent progressivement des dispositifs d'authentification forte à code non rejouable. Enfin, en décembre 2014, l'Autorité bancaire européenne a émis des orientations établissant un ensemble d'exigences minimales en ce qui concerne la sécurité des paiements sur internet. Ces orientations s'appliquent à la fourniture de

services de paiement proposés sur internet par les prestataires de services de paiement (PSP).

- ***L'intégrité des données*** : il ne faut pas que les informations de paiement échangées puissent être modifiées de manière frauduleuse.
- ***La confidentialité et la protection des données sensibles*** : certaines données n'ont pas à être connues des tiers comme le numéro de carte bancaire par exemple.

- **Un cadre de confiance pour le commerce électronique**

Le problème de la sécurité des paiements en ligne doit être posé dans un contexte plus large. En effet, la question de fond du commerce électronique est celle du développement de la confiance des consommateurs qui réclament au-delà de la sécurisation des paiements, une meilleure lisibilité de l'identité et de la notoriété des sites marchands, une offre de services de qualité et la mise en œuvre d'un mode de règlement des litiges, efficace, rapide et équitable.

3. Glossaire

Authentification : Procédure permettant au prestataire de services de paiement de vérifier l'utilisation d'un instrument de paiement donné, y compris ses dispositifs de sécurité personnalisés (Source : DSP2).

Autorité bancaire européenne (ABE) : Autorité européenne de surveillance mise en place le 1er janvier 2011 – avec siège à Londres – ayant reçu pour mission la surveillance des banques au sein de l'Union européenne.

Observatoire de la sécurité des cartes de paiement : Créé par la loi du 15 novembre 2001 relative à la sécurité quotidienne, l'Observatoire a pour mission de suivre les mesures adoptées par les émetteurs et les commerçants pour veiller à la sécurité des transactions par carte, d'établir des statistiques de fraude et d'assurer une veille technologique afin de proposer, le cas échéant, des moyens de lutter contre les atteintes d'ordre technologique à la sécurité des cartes de paiement.

Prestataires de services de paiement : Dans le cadre de la directive 2007/64/CE du 13 novembre 2007 concernant les services de paiement, personne morale dont l'activité principale consiste à fournir des services de paiement.

Système 3D Secure : Dispositif qui permet pour une banque d'authentifier de manière renforcée le porteur d'une carte de paiement lors d'un achat sur internet.
Différents modes d'authentification sont proposés par les banques et notamment celui de l'envoi par SMS d'un code à usage unique.

Virement SEPA : Transfert de fonds entre comptes bancaires sur ordre du débiteur à l'intérieur de l'Espace unique des paiements en euro.
Il s'appuie sur une méthodologie conforme aux normes internationales (ISO 20022) et utilise le BIC et l'IBAN comme identifiant des numéros de comptes.