Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

26-Jun-2012

Français - Or. Anglais

DIRECTION DE LA SCIENCE, DE LA TECHNOLOGIE ET DE L'INDUSTRIE
COMITE DE LA POLITIQUE A L'EGARD DES CONSOMMATEURS

RAPPORT SUR LA PROTECTION DES CONSOMMATEURS DANS LES PAIEMENTS EN LIGNE ET MOBILES

JT03324235

DSTI/CP(2010)22/FINAL
Non classifié

Français - Or. Anglais

AVANT-PROPOS

En 2009, le Comité de la politique à l'égard des consommateurs (CPC) a engagé une révision des principes contenus dans les *Lignes directrices de l'OCDE régissant la protection du consommateur dans le contexte du commerce électronique*. Pour ce faire, le comité a organisé une conférence intitulée : *Des consommateurs autonomes et mieux protégés dans l'économie Internet,* qui s'est tenue à Washington du 8 au 10 décembre 2009 au sein de la Federal Trade Commission (FTC) des États-Unis. L'émergence et le besoin de mécanismes de paiement sur Internet et sur mobile qui soient à la fois toujours plus sûrs et plus pratiques à utiliser ont été considérés, lors de cet évènement, comme des éléments essentiels à la promotion de l'innovation et de la croissance du commerce électronique. Suite à ces discussions, le comité a décidé d'entreprendre un travail de recherche et d'analyse dans ce domaine et de préparer un rapport mettant en évidence les problèmes de politiques publiques que les parties prenantes devraient prendre en considération.

Le présent rapport, qui a été déclassifié par le comité lors de sa 83e réunion le 23 avril 2012, a été préparé par Brigitte Acoca, du Secrétariat de l'OCDE. Il a bénéficié de contributions de représentants des gouvernements, de la société civile et des professionnels. Les problèmes abordés ont été débattus lors d'un *Atelier sur la protection des consommateurs dans les paiements en ligne et sur mobile* organisé à l'OCDE le 15 avril 2011[1]. Ils ont également été discutés par le Réseau international de contrôle et de protection des consommateurs (RICPC) qui, fin 2011, a mis sur pied un groupe de travail sur les paiements mobiles, ainsi que lors d'un atelier intitulé *Paper, Plastic,… or Mobile ?* organisé par la FTC le 26 avril 2012 à Washington (voir : www.ftc.gov/bcp/workshops/mobilepayments/). Ce rapport est publié sous la responsabilité du Secrétaire-Général de l'OCDE.

1 . Voir : *www.oecd.org/sti/consumer-policy/mobilepayments*.

SYNTHÈSE

Le présent examen de la problématique des paiements s'inscrit dans le cadre de la revue, par le CPC, des Lignes directrices de l'OCDE de 1999 sur le commerce électronique. Le rapport examine dans quelle mesure les principes relatifs aux paiements énoncés dans les Lignes directrices (OCDE, 1999, deuxième partie, section V) ainsi que ceux concernant l'information du consommateur, la loyauté des pratiques commerciales, le règlement des litiges et les recours, apportent une réponse adaptée aux problèmes liés aux mécanismes nouveaux et émergents des paiements en ligne et mobiles. Le rapport examine les éléments qu'il conviendrait de développer davantage, ou de modifier, pour améliorer la confiance des consommateurs dans ce domaine. Il intègre les contributions reçues des délégations nationales, du secteur privé et de la société civile ; il a été examiné lors d'un atelier organisé avec les parties prenantes en avril 2011.

Tendances

Le développement de systèmes de paiement innovants et d'une grande commodité d'usage par des établissements financiers et autres parties prenantes (opérateurs mobiles et sociétés Internet, notamment), a contribué à une expansion rapide du commerce électronique, offrant aux consommateurs, dans de nombreux cas, des moyens plus efficaces, plus pratiques et plus sûrs pour acheter des produits dont la gamme ne cesse de s'étendre, notamment des biens et services numériques. Ce développement a également apporté des réponses aux problèmes que peuvent rencontrer les consommateurs avec les commerçants lorsque, par exemple, les produits ne répondent pas à leurs attentes où n'arrivent pas à destination. Il ressort cependant de la présente analyse sur les systèmes de paiement en ligne et mobiles que le rôle que ces systèmes pourraient jouer pour faciliter les transactions et autonomiser les consommateurs dans le commerce électronique pourrait être renforcé pour répondre à un certain nombre de problèmes déjà présents ou émergents.

Enjeux pour les politiques publiques

Le rapport met en évidence une série de problèmes auxquels les responsables des politiques pourraient apporter des solutions pour renforcer la confiance des consommateurs dans les systèmes de paiement nouveaux ou émergents utilisés dans le commerce électronique. Ces problèmes portent sur cinq aspects principaux :

- La clarté, la transparence et l'exhaustivité de l'information fournie.
- La variabilité des régimes réglementaires et de protection.
- Les pratiques commerciales frauduleuses, trompeuses et mensongères.
- Le règlement des litiges et les voies de recours.
- La sécurité et l'interopérabilité.

TABLE DES MATIÈRES

INTRODUCTION

Le développement rapide de l'Internet, la croissance des services mobiles et d'autres innovations technologiques ont apporté des bienfaits considérables aux consommateurs tout en s'accompagnant également de risques nouveaux imposant aux responsables des politiques des consommateurs de non seulement rester au fait des évolutions mais aussi d'apporter des solutions aux problèmes existants et émergents. (OCDE, 2010*a*, Chapitre I). En 1999, pour soutenir le développement de l'Internet, l'OCDE a adopté des *Lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique* (« les Lignes directrices de 1999 » (OCDE, 1999). En 2008, suite à la *Réunion ministérielle de Séoul sur le futur de l'économie Internet,* le Comité de la politique à l'égard des consommateurs (CPC) a engagé un examen de ces lignes directrices. Un rapport de référence examinant les évolutions du marché et les problèmes qui se posent pour les consommateurs a été préparé pour soutenir la discussion à une conférence OCDE intitulée *Autonomiser les cyberconsommateurs : renforcer la protection des consommateurs dans l'économie Internet*, organisée à Washington du 8 au 10 décembre 2009 au sein de la Federal Trade Commission des États-Unis (OCDE, 2009*a*).

Suite à cette manifestation, le comité a fait le point et décidé d'entreprendre l'examen des Lignes directrices de 1999 en pour explorer les développements et difficultés rencontrées par les consommateurs dans le cadre des systèmes nouveaux et émergents de paiement en ligne et mobiles. Comme le montre l'encadré 1, quelques principes des Lignes directrices de 1999 répondent directement à certains de ces problèmes .

Encadré 1. Paiement (OCDE, 1999, Partie II, Section V)

Les consommateurs devraient pouvoir disposer de mécanismes de paiement faciles à utiliser, sécurisés ainsi que d'informations sur le niveau de sécurité assuré par ces mécanismes.

Les limitations de responsabilité en cas d'utilisation non autorisée ou frauduleuse des systèmes de paiement, et les mécanismes de remboursement sont des outils puissants pour renforcer la confiance des consommateurs, et il conviendrait d'encourager leur élaboration et leur utilisation dans le contexte du commerce électronique.

Les systèmes de paiement servent au transfert de sommes d'argent des consommateurs vers les commerçants en règlement des transactions de commerce électronique. Ils comprennent : *i)* les systèmes de paiement utilisant une carte de crédit/débit ou un compte bancaire pour réaliser les transactions de commerce électronique (par exemple les réseaux de cartes de paiement comme *Visa* ou *Mastercard,* ou les méthodes de paiement de type banque en ligne) ; *ii)* les systèmes alternatifs de paiement proposés par des établissements non bancaires opérant sur Internet et associés à une carte de paiement ou un compte bancaire directement (comme *Google Checkout* ou *Checkout by Amazon*) ou indirectement (comme *PayPal*) ; *iii*) les paiements mobiles, à savoir les paiements mobiles sans contact effectués dans les points de vente (comme *Google Wallet*) ainsi que les paiements à distance effectués au moyen d'appareils mobiles. (OCDE, 2011*b*, p. 172).

Dans son évaluation initiale des Lignes directrices de 1999, le comité a identifié un certain nombre de problèmes relatifs aux paiements nécessitant un examen plus approfondi. Il s'agit des points suivants :

- La variabilité des niveaux de protection des consommateurs (comme les limitations de responsabilité des consommateurs) dans les différents systèmes de paiement en ligne et mobiles.
- Le rôle que les prestataires de paiement peuvent jouer pour renforcer la protection des consommateurs, en fournissant, par exemple :

- Une information claire et transparente sur les mécanismes de résolution des différends existants.
- Des niveaux minimaux de protection des paiements qui s'appliqueraient à tous les mécanismes de paiement.
- Des outils d'authentification et des systèmes de vérification de l'âge pour garantir la sécurité des mécanismes de paiement.

On notera que les Lignes Directrices de 1999 ne font pas spécifiquement état des questions de vie privée, lesquelles font l'objet d'un instrument distinct de l'OCDE, à savoir les Lignes directrices de l'OCDE sur la vie privée, actuellement en cours d'examen. En conséquence, les questions de vie privée en relation avec les paiements en ligne et mobiles ne sont pas abordées directement dans ce rapport.

Le rapport présente des informations de référence sur les développements récents des paiements en ligne et mobiles, afin d'aider le comité à déterminer dans quelle mesure et de quelle manière les Lignes directrices de 1999 pourraient éventuellement être adaptées aux évolutions de l'économie Internet. Le rapport passe en revue les caractéristiques et la structure changeante du marché des paiements en ligne et mobiles (Section I). Il recense les difficultés existantes et émergentes qui se posent aux consommateurs (Section II). Ce travail s'appuie également sur des recherches réalisées par le CPC en 2001 sur les protections offertes aux titulaires de cartes de paiement (OCDE, 2002) pour les dispositifs de paiement traditionnels. Lors de la préparation de ce rapport, le comité a reconnu que les marchés des paiements connaissent des évolutions très rapides et que de nouvelles questions pourraient un jour se poser, qui n'ont pas été abordées ; il est important que les parties prenantes soient prêtes à répondre à tout nouveau défi dans les meilleurs délais.

ÉVOLUTION DES PAIEMENTS EN LIGNE ET MOBILES

Il y dix ans, les biens et services achetés sur Internet étaient principalement réglés par carte bancaire et par des mécanismes de paiement classiques (comme les chèques). Si les cartes de paiement demeurent le mode de règlement dominant sur Internet – utilisé en 2009 dans plus de 90 % des opérations de commerce électronique de détail en Europe, dans plus de 80 % aux États-Unis et dans plus de 74 % au Mexique (en 2008) –, l'industrie des paiements a développé, ces dernières années, tout un éventail de services en ligne et mobiles compétitifs, afin de répondre à la croissance des achats de biens physiques et numériques ainsi que de services en ligne (OCDE, 2011*b*, p. 172, para. 283).

La présente section est consacrée à la manière dont les mécanismes de paiement en ligne et mobiles se sont développés ces dernières années. Elle comprend *: i*) des définitions pour différents systèmes de paiement ; *ii*) des exemples de mécanismes actuels de paiement en ligne et mobiles ; *iii*) un tour d'horizon des prestataires de paiement traditionnels et nouveaux ; *iv*) un aperçu de l'évolution de ces marchés ; et *v*) une brève présentation des questions de comportement et préférences des consommateurs dans ce domaine.

I. Définitions

Dans le cadre de ce rapport, on entend par commerce électronique les commandes de biens ou de services effectuées et confirmées électroniquement *via* l'Internet (c'est-à-dire en ligne) ou *via* d'autres plateformes électroniques (comme celles exploitées par des opérateurs de réseaux mobiles) (voir OCDE, 2011*c*).

Les paiements pour ces biens et services peuvent être réalisés par divers moyens, notamment par voie électronique (voir ci-dessus), mais aussi par chèque, en liquide ou par téléphone (avec une carte de paiement ou d'autres moyens de paiement).

Les paiements mobiles sont des paiements pour lesquels les données et l'ordre de paiement sont transmis *via* un téléphone mobile ou tout autre équipement mobile. Entrent dans cette catégorie les paiements sur Internet réalisés au moyen d'un équipement mobile, de même que ceux effectués par des opérateurs de réseaux mobiles. On notera que la localisation du payeur et de l'infrastructure utilisée est sans importance : le payeur peut être aussi bien en déplacement que dans un point de vente (Innopay, 2011).

Ce rapport met l'accent sur les paiements électroniques destinés à conclure des transactions de commerce électronique.

II. Paiements en ligne et mobiles : options en présence

Les moyens de paiement en ligne

Dans un rapport de l'OCDE consacré aux *Systèmes de paiement en ligne du commerce électronique*, les systèmes de paiement en ligne suivants ont été recensés (OCDE, 2006, p. 38-53) :

Systèmes fondés sur un compte, dans lesquels le paiement est réalisé à travers un compte personnel existant (généralement un compte bancaire).

Cartes de crédit (comme *Visa*, *MasterCard* et *American Express*).

Cartes de débit (comme *Visa*, *MasterCard* ainsi que des fournisseurs nationaux de cartes de débit comme *EFTPOS* en Australie).

Services d'intermédiation (comme *PayPal* et, aux États-Unis, le système ACH [Automated Clearing House, chambre de compensation automatisée][2]).

Mécanismes automatisés de paiement de factures.

Portefeuilles en ligne : pour créer un compte d'un portefeuille en ligne, l'utilisateur doit s'inscrire auprès d'un prestataire de paiement. Le compte est généralement associé à l'adresse de messagerie de l'utilisateur. Celui-ci peut ensuite l'alimenter, généralement au moyen d'une carte de débit ou de crédit. Les paiements peuvent être effectués après la saisie d'un identifiant et mot de passe. Le paiement peut être effectué et débité du compte dès que l'identité de l'utilisateur a été confirmée.

Systèmes de monnaie électronique (ou services de paiement prépayés), dans le cadre desquels un 'utilisateur approvisionne à l'avance un compte personnel créé chez un prestataire de services de paiement au moyen d'un portefeuille en ligne ou bien encore un appareil comme une carte à puce.

Il existe également d'autres mécanismes de paiement comprenant :

Les paiements Internet transitant par un site de banque en ligne. Le consommateur utilisant cette plateforme est redirigé, directement à partir de la page web d'un commerçant, vers le site de banque en ligne de l'établissement qui tient son compte. Un formulaire de virement pré-rempli peut s'afficher, donnant le détail de la transaction. Le consommateur approuve alors le paiement. Ce mode de règlement est de plus en plus prisé dans certains pays européens dont l'Autriche (*EPS*), les Pays-Bas (*iDEAL*), la Belgique (*Bancontact/Mister Cash*) et l'Allemagne (*Giropay*). La méthode commence également à apparaître aux États-Unis (*Secure Vault Payments*) et au Canada (*Interac en Ligne*).

Le paiement à la livraison, qui consiste à régler un article commandé en ligne au moment où on le reçoit physiquement.

Les services de dépôt sur un compte séquestre, lesquels sont souvent utilisés pour les achats réalisés dans le cadre d'enchères en ligne. Un tiers intermédiaire est chargé de conserver le paiement de l'acheteur tant que celui-ci n'a pas reçu et approuvé la marchandise. En Corée, à compter d'août 2011, le seuil de valeur des articles couverts par le dispositif national de dépôt en compte séquestre sera abaissé de 91 USD à 45 USD. Aux Pays-Bas, l'entreprise postale *TNT* met actuellement au point un nouveau service de paiement en ligne qui permettra aux consommateurs de payer en amont grâce à un dispositif de banque en ligne ; ces règlements anticipés seront conservés par *TNT* sur un compte séquestre. Le paiement en faveur du commerçant sera débloqué

2. Aux États-Unis, les prestataires ACH permettent aux titulaires de comptes de chèques ou d'épargne d'accepter et d'émettre des paiements de manière électronique. Ce système offre à de nombreux clients la possibilité d'accéder aux produits et services d'entreprises présentes en ligne. Dernièrement, les Banques de réserve fédérale ont commencé à proposer des services FedACH internationaux pour la transmission de fonds entre les États-Unis et d'autres pays par l'entremise de la National Automated Clearing House Association (NACHA, association des chambres nationales de compensation automatisée), une organisation qui conçoit des dispositifs électroniques améliorant le système de paiement ACH.

uniquement lorsque le consommateur aura confirmé, au moyen d'un code spécial, la réception des produits achetés.

Les moyens de paiement mobiles

Les consommateurs équipés d'un appareil portable peuvent acheter des produits en faisant appel à deux principaux modes de paiement (EPC, 2010*a*, p. 58) :

Les paiements mobiles sans contact au point de vente : ces paiements concernent les achats pour lesquels l'acheteur et le vendeur sont tous les deux présents ; le règlement est effectué au moyen de technologies radio sans contact, telles que la NFC qui est une technologie à radiofréquence de courte portée permettant à des appareils électroniques de communiquer entre eux –, Bluetooth ou encore les technologies infrarouge pour le transfert de données.

Le paiement mobile à distance : le règlement est effectué au moyen d'appareils portables ; les transactions sont exécutées par l'entremise de réseaux de télécommunications tels que le système global pour les communications mobiles (GSM) ou Internet. Ces paiements, qui sont indépendants des points de vente, reposent sur deux systèmes :

- SMS : le consommateur ouvre un compte auprès d'un prestataire de service de paiement mobile (PSPM) ; ce compte peut être associé à un compte bancaire, à une carte de crédit, de débit ou bien à une carte prépayée. Le consommateur envoie un SMS au PSPM en indiquant le montant à régler et le numéro de téléphone du bénéficiaire ; le PSPM renvoie ensuite un message de confirmation de la transaction au consommateur et lui demande de saisir un numéro d'identification personnel (code PIN) afin d'authentifier le paiement. Enfin, le PSPM vire le montant de la transaction sur le compte du bénéficiaire. Ce système de paiement est souvent utilisé pour payer dans les parkings et les stations-service et pour effectuer des règlements entre particuliers. Il est très répandu en Asie et en Afrique.
- Protocole d'application sans fil (Wireless Application Protocol, WAP) : selon ce système, les consommateurs accèdent à un site web marchand au moyen du navigateur de leur appareil portable et procèdent à des achats de la même manière que dans le cadre d'un achat en ligne habituel.

Les paiements mobiles peuvent être traités de diverses façons :

Ils peuvent être inscrits sur la facture du téléphone portable du consommateur. C'est généralement le cas pour les services achetés auprès d'opérateurs de télécommunications, comme les sonneries ou les thèmes/fonds d'écran pour terminaux portables. La technique, qui a été lancée pour la première fois en Corée en 2000 par le prestataire de paiements mobiles *Danal*, rencontre un vif succès chez les jeunes. En 2007, environ 70 % des achats de contenus numériques dans le pays étaient portés sur les factures de téléphonie mobile (KPMG, 2007). En outre, l'utilisation des appareils portables s'est étendue ; ainsi, dans certains pays, ces appareils permettent d'effectuer des achats auprès de distributeurs automatiques (Banque de Finlande, 2003).

Ils peuvent se faire à l'aide d'une carte de débit ou de crédit. Toutefois, nombre de parties prenantes jugent ce moyen de paiement peu adapté aux appareils portables, la saisie d'un numéro de carte à 16 chiffres sur un combiné n'étant pas toujours facile. En outre, des travaux de recherche font état de problèmes liés au traitement des paiements effectués à l'aide de cartes de crédit *via* les appareils portables dans la mesure où un grand nombre de combinés ne peuvent gérer les connexions logicielles sécurisées utilisées dans le traitement des données de carte de crédit (Consumer Focus, 2009, p. 44). Pour y remédier, des opérateurs de téléphonie mobile français travaillent actuellement à un nouveau système (*Buyster*) grâce auquel les consommateurs

pourront acheter des produits sur Internet avec leurs téléphones portables sans avoir à saisir leur numéro de carte de crédit. Lorsque le client s'inscrit sur le site web de *Buyster* (en fournissant les coordonnées bancaires qu'il devrait autrement communiquer au cybermarchand), celui-ci reçoit un code personnel. C'est ce code que le consommateur devra ensuite communiquer à chaque achat, son compte bancaire étant alors débité automatiquement.

Ils peuvent être effectués au moyen d'une carte à puce intégrée, avec ou sans fil (paiements prépayés).

III. Les prestataires de services de paiement

Parmi les prestataires traditionnels de services de paiement figurent les banques (notamment, dans le cas des paiements par carte, la banque « émettrice », qui fournit la carte au détenteur ou consommateur, et la « banque acquéreur », qui est utilisée par le commerçant ou le vendeur), les réseaux de cartes bancaires et les opérateurs de paiement (c'est-à-dire les intermédiaires chargés de traiter les paiements entre les commerçants et les banques acquéreurs).

Ces dernières années, de nouveaux acteurs du paiement, souvent appelés opérateurs de paiement alternatifs ou autres prestataires de paiement, ont accru leurs parts de marché et gagné la confiance des consommateurs à travers le monde. Parmi ces organisations non bancaires qui, d'après les travaux de recherche, ont exécuté 156 millions de transactions en 2009 (soit quelque 5 % de l'ensemble des m-paiements) (Capgemini, 2010), on trouve des prestataires de services de paiement en ligne et des opérateurs de réseau mobile.

Les prestataires de paiement en ligne comprennent *Amazon Payments*, *Google Checkout*, *PayPal* et *Bill Me Later* (acquis par *PayPal* en 2008). Il convient de noter que, dans certains pays, ces prestataires sont considérés comme des banques par les autorités de réglementation. En Asie, *Facebook* a noué récemment un partenariat avec un prestataire de services de paiement malaisien pour permettre à ses utilisateurs d'Asie et d'Océanie (notamment en Australie, en Nouvelle-Zélande et en Inde) d'acheter des biens et des jeux virtuels à partir de sa plateforme. Le monde du paiement a reçu un nouveau coup de fouet lorsque *PayPal*, à la fin de 2009, a ouvert sa plateforme (*PayPal X*) aux développeurs de logiciels pour stimuler la création de nouveaux services de paiement.

Dans un certain nombre de pays, les opérateurs de réseau mobile jouent également un rôle de plus en plus important en matière de paiement. Ils s'appuient sur divers modèles économiques qui peuvent être classifiés comme suit:

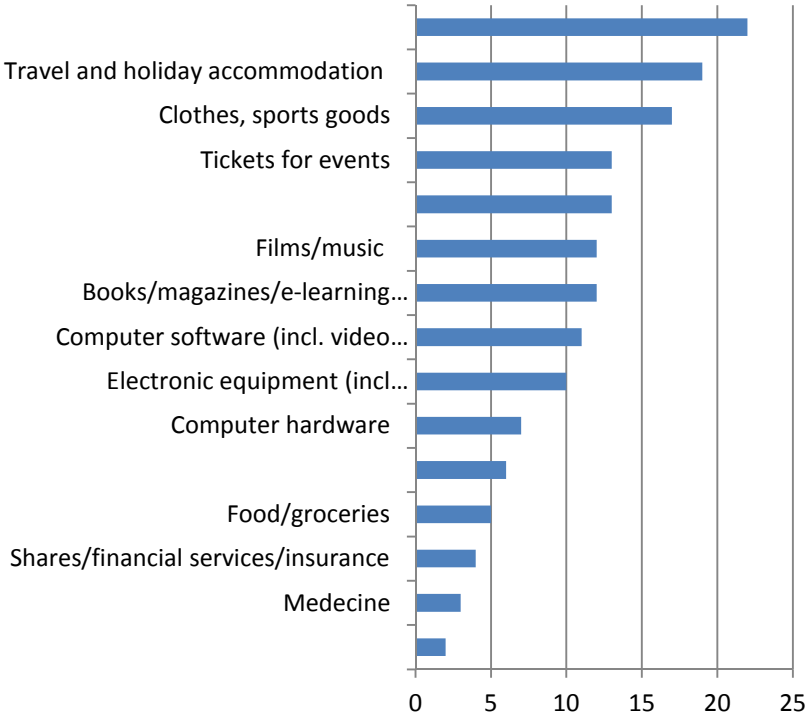
- *Modèle centré sur les opérateurs de téléphonie mobile :* les opérateurs agissent de façon indépendante pour déployer des applications de paiement sur des appareils portables compatibles avec la technologie NFC. Ces applications peuvent gérer le dépôt de sommes prépayées ou bien encore le montant des achats est ajouté à la facture de téléphonie mobile des clients (comme *NTT DoCoMo* au Japon).
- *Modèle centré sur les banques :* selon ce modèle, les banques mettent au point, de manière indépendante, des mécanismes de paiement destinés au grand public, sans faire appel aux opérateurs de téléphonie mobile ni aux fabricants de téléphones portables. En France, par exemple, la *Caisse d'épargne* a conçu le service *Movo* qui offre la possibilité de régler des achats par SMS.
- *Modèle d'intégration partiel :* il implique qu'un opérateur de téléphonie mobile crée une succursale bancaire pour gérer les paiements mobiles, comme *Mobikom* en Autriche, qui propose un mécanisme de paiement des achats effectués aux distributeurs automatiques.

– *Modèle de collaboration totale :* selon ce modèle, une co-entreprise est constituée entre des opérateurs de téléphonie mobile, des banques et d'autres prestataires de paiement. Entre autres exemples, on citera celles mises sur pied par *AT&T Mobility*, *Verizon Wireless* et *T-Mobile* aux États-Unis, ou bien encore l'expérience pilote CITYZI de paiements NFC menée à Nice en 2010 par de grandes banques françaises, des opérateurs de téléphonie mobile, des sociétés de transport et les autorités locales. En 2011, *Google* a adopté ce modèle aux États-Unis en lançant *Google Wallet*, un système NFC qui a donné lieu à la création d'un partenariat avec *Citi* (la banque émettrice), *MasterCard* (le réseau de paiement), *First Data* (l'opérateur de paiement) et *Sprint* (l'opérateur de télécommunications initial). Malgré son coût de départ élevé, ce modèle économique peut être attractif tant pour les consommateurs que pour les entités commerciales concernées, car il exploite le savoir-faire de chacune des parties (du secteur financier et du secteur des télécommunications) et permet d'établir une norme technologique unique pour les paiements mobiles.

IV. Développement des mécanismes de paiement en ligne et mobiles

L'expansion du commerce électronique, y compris du commerce mobile, s'est accompagnée du développement de dispositifs de paiement innovants, faciles à utiliser et plus sûrs. Cette évolution a permis à son tour de renforcer la confiance du consommateur et de stimuler les achats en ligne. Comme l'illustre la Figure 1, la palette des biens et services que les consommateurs achètent sur Internet est large, particulièrement en ce qui concerne les films, la musique, les livres, ainsi que les voyages et les services de vacances.

Figure 1. Biens et services commandés par des particuliers sur Internet au cours des 12 derniers mois UE-27, en pourcentage de l'ensemble des personnes concernées (2009)



Source : Eurostat, 2009.

Parallèlement au développement du commerce électronique, on a assisté à une croissance des paiements en ligne et mobiles. En 2009, les paiements en ligne s'élevaient à environ 790.1 milliards EUR dans le monde ; ils devraient atteindre, selon des estimations, 1 382.3 milliards EUR en 2012 (Capgemini, 2010). Les m-paiements, quant à eux, étaient évalués à 41.5 milliards EUR dans le monde en 2009, et devraient atteindre 140 milliards EUR d'ici à 2012, selon des prévisions ; cette hausse serait due, en grande partie, aux évolutions dans les économies en développement (Capgemini, 2010).

Utilisation des paiements en ligne et perspectives d'évolution

Les cartes de crédit demeurent la forme prépondérante de paiement en ligne. Cette préférence de paiement peut s'expliquer par l'usage répandu de ces cartes aujourd'hui, mais elle pourrait également découler du fait que, dans certains pays, ces cartes offrent les meilleurs mécanismes de remboursement et de protection en cas de perte ou de fraude. Les commissions acquittées sur les paiements par carte de crédit figurant généralement parmi les plus élevées, certains commerçants se sont efforcés d'encourager les consommateurs à utiliser d'autres moyens de paiement, moins onéreux à traiter. Certains commerçants, par exemple, souhaiteraient proposer aux consommateurs des remises pour l'utilisation d'une carte de débit à la place d'une carte de crédit, ou pour l'emploi d'une carte de crédit n'offrant pas d'avantages (Internet Retailer, 2010*b*). Selon un rapport de Javelin Research, le recours à la carte de crédit pour payer en ligne recule, quoique lentement, aux États-Unis. Il représentait 43.5 % du volume total des paiements en ligne en 2009, et devrait, selon les estimations, tomber à 39.4 % en 2014 (Javelin Research, 2010). Au Royaume-Uni, les cartes de débit gagnent des parts de marché. Pour la première fois, en 2009, elles ont eu plus d'utilisateurs que les cartes de crédit pour des achats en ligne (Payments Council du Royaume-Uni, 2010, p. 20). Comme nous le verrons plus loin (voir la section consacrée à l'espace unique de paiement en euros [SEPA, Single Euro Payments Area]), les cartes de débit sont de plus en plus souvent perçues, notamment dans la période actuelle de ralentissement économique, comme un moyen commode et peu onéreux pour les consommateurs d'effectuer facilement des micro-paiements.

Les consommateurs semblent accorder une confiance croissante aux prestataires alternatifs de paiement. D'après des travaux de recherche menés par le secteur privé, la confiance des consommateurs dans les banques qui offrent des mécanismes de paiement est à peu près équivalente à celle relative aux prestataires alternatifs (67 % pour les premières contre 64 % pour les seconds). Les consommateurs âgés de 45 à 64 ans ont même davantage confiance dans ces derniers que dans les banques (CISCO, 2008).

Le développement des prestataires de paiement alternatifs est lié à cinq facteurs principaux :

Coûts inférieurs pour les commerçants. Les commissions facturées par les prestataires de paiement alternatifs aux commerçants sont souvent bien inférieures à celles des sociétés de carte de crédit (Roth, 2010).

Sécurité des données et conservation des données d'identification. Les prestataires de paiement alternatifs permettent aux consommateurs d'acheter des produits au moyen d'une combinaison unique d'un nom d'utilisateur et d'un mot de passe, sans avoir à communiquer les références de leur carte de crédit au commerçant. Ainsi, *Obopay*, une société spécialisée dans les systèmes de paiement mobile aux États-Unis, donne aux consommateurs la possibilité de faire leurs achats avec une carte de crédit ou de débit associée à leur numéro de téléphone portable, sans qu'ils aient à divulguer d'informations personnelles, comme une adresse de facturation ou un numéro de carte de crédit. Avec *PayPal*, une fois inscrit au service, il suffit au consommateur de cliquer sur l'icône représentant ce service pour payer ses achats chez tout commerçant affilié sans avoir à ressaisir de données personnelles. Le prestataire paie le commerçant en débitant la carte de crédit ou le compte bancaire du consommateur. Avec le service *Bill Me Later*, les paiements peuvent être traités sans passer par une carte de crédit : les consommateurs règlent en ligne à partir d'un compte chèques ou d'épargne.

Nouvelles procédures d'encaissement. Alors que les sociétés de carte de crédit facturent une commission par transaction aux commerçants, de nouveaux dispositifs ont été mis en place pour réduire les coûts de transaction. Ainsi, les programmes de paiement d'*Apple* (*iTunes*) et de *Research in Motion* diminuent les commissions de transactions en regroupant les achats d'un même client avant de les envoyer à une société de carte de crédit pour traitement.

Croissance des réseaux sociaux et des jeux en ligne. Aujourd'hui, divers produits sont achetés sur les plateformes des réseaux sociaux, en particulier des contenus numériques et des produits virtuels. Le jeu en ligne, en pleine expansion, bénéficient du développement et de la disponibilité d'un certain nombre de moyens de paiement, dont la monnaie virtuelle, qui est utilisée dans le système *Facebook Credits*.

Essor des transactions de consommateur à consommateur (C2C). La multiplication des transactions C2C a eu une incidence considérable sur la croissance de certains des prestataires de paiement alternatifs. Aux États-Unis, elles ont également joué un rôle important dans l'expansion des systèmes de paiement ACH.

Certains s'attendent à ce que les prestataires de paiement alternatifs continuent leur progression, en partie parce que les consommateurs s'estiment mieux protégés de la fraude par les modes de paiement de ces prestataires qu'ils ne le sont lorsqu'ils paient avec une carte de débit (Javelin Research, 2010).

Les solutions de paiement sont de plus en plus souvent assorties de services complémentaires proposés pour accroître la satisfaction des consommateurs en ligne. Ainsi, certains prestataires de paiement alternatifs donnent aux consommateurs la possibilité de convertir en espèces l'argent gagné sur Internet (dans le cadre de jeux en ligne, par exemple). La carte de débit de *PayPal* permet notamment à ses clients aux États-Unis de retirer de l'argent aux guichets automatiques de banque. Même chose pour la société britannique *Ukash*, qui autorise les joueurs en ligne à retirer de l'argent hors connexion. En mars 2010, *Visa* a lancé un nouveau portefeuille en ligne (*Rightcliq by Visa*), dans lequel les consommateurs peuvent conserver leurs numéros de carte de paiement de façon à ne communiquer qu'un minimum d'informations personnelles (adresse de messagerie et mot de passe *Rightcliq*) pour régler leurs achats auprès des commerçants affiliés. Avec *Rightcliq*, les consommateurs peuvent également obtenir des réductions de prix de la part des commerçants affiliés et gérer leurs activités de commerce électronique (en stockant par exemple des informations relatives à certains sites marchands ou produits). Une fonction d'« achat social » permet aux consommateurs de solliciter l'avis de leurs amis sur des produits. Le service est accessible à partir de la plateforme *Rightcliq* et des sites web des commerçants affiliés.

Certaines économies en développement montrent également un intérêt croissant pour les paiements électroniques. En Chine, le marché des paiements en ligne a progressé rapidement pour atteindre 555 milliards CNY (81.4 milliards USD) en 2009, soit une hausse de 135.6 % depuis 2008. Plus d'une centaine de sociétés de paiement en ligne sont présentes dans le pays, au premier rang desquelles on trouve *Alipay* (le service de paiement de *Taboao/Alibaba*), avec 52 % de parts de marché, suivie de *Tenpay* (une unité de paiement en ligne de *Tencent*), avec 24.7 %. Par ailleurs, *Alipay* envisagerait de développer ses services de paiement à l'étranger (The Paypers, 2010*c*). Face aux problèmes posés par ce type de règlements, la Banque populaire de Chine a annoncé en juin 2010 l'application de nouvelles règles aux sociétés souhaitant proposer des services de paiement en ligne dans le pays. Ainsi, les établissements non bancaires devront acquérir une licence pour offrir ces services de manière autonome (China Daily, 2010).

Utilisation des paiements mobiles et perspectives d'évolution

Les achats réalisés au moyen d'appareils portables équipés du haut débit devraient aussi s'accélérer. Le nombre de possesseurs d'un téléphone portable de troisième génération (3G) dans le monde dépasse d'ores et déjà largement celui de titulaires de cartes de paiement. En outre, le taux de pénétration

des appareils portables numériques à l'échelle mondiale est aujourd'hui supérieur à celui des ordinateurs personnels.

À la fin de 2008, la barre des 4 milliards d'abonnements mobiles était atteinte, les économies émergentes étant les plus dynamiques dans ce domaine (CNUCED, 2009). En juin 2010, la barre des 5 milliards était franchie. Les appareils portables sont devenus un mécanisme de paiement courant dans certains pays en développement, surtout dans ceux où les cartes de crédit ne sont pas très répandues et où quantité de personnes ne possèdent pas de compte bancaire. La croissance des abonnements et des applications de téléphonie mobile, conjuguée à l'essor des réseaux sociaux et des jeux en ligne, a augmenté l'attrait des paiements mobiles pour les consommateurs.

Néanmoins, bien que ce mode de paiement ait suscité une attention considérable depuis dix ans, il n'a pas progressé aussi vite que beaucoup le prévoyaient. La Corée, le Japon et Singapour, où le commerce mobile a fait un bond en avant, font figure d'exceptions.

En Australie, selon des recherches menées par *eBay*, environ un quart des Australiens détenteurs d'un téléphone portable s'en servent pour acheter en ligne, dont plus de 80 000 sur le seul site d'*eBay* en juin 2010 (Noone, 2011). Au Mexique, les premiers systèmes de paiement mobile ont été mis en place en 2011. Au vu de ce marché naissant mais prometteur (en 2010, on comptait approximativement 87 millions d'abonnements mobiles pour une population de 110 millions d'habitants), un nouveau cadre réglementaire est en cours d'élaboration par la Banque centrale du Mexique et le ministère des Finances, avec le concours de la commission nationale de réglementation des opérations bancaires et des marchés financiers.

Dans l'Union européenne (UE), malgré quelques tentatives de commercialisation dans certains pays, le m-paiement sans contact reste à l'état embryonnaire. Il en va de même pour l'Amérique du Nord. Une étude menée en 2010 par Forrester Research aux États-Unis fait apparaître que la croissance des paiements mobiles est relativement modeste malgré la forte pénétration des abonnements. Bien que 18 % des internautes adultes se disent intéressés par ce mode de paiement, moins de 6 % y ont eu recours au moins une fois. En 2009, alors que la population comptait 89.5 % d'utilisateurs de téléphone portable, seuls 3 % environ avaient effectué des m-paiements, 1.1% au moyen de dispositifs sans contact et 2 % par SMS (FRBB, 2010*b*). Toujours selon Forrester, du fait de l'absence d'un modèle économique répondant aux besoins de tous les acteurs du paiement aux États-Unis, il est difficile de convaincre les consommateurs de l'utilité des différents systèmes et services disponibles, et ce malgré l'intérêt croissant qu'ils y accordent depuis trois ans (Forrester Research, 2010). De nouvelles initiatives comme *Google Wallet*, qui au final sera intégré à *Google Offers*, ainsi que le nouveau programme d'« offres promotionnelles du jour » prépayées de la société, pourraient changer la donne. Le rapport note que les pays où une grande part des transactions était réalisée en espèces ont développé leur marché des paiements mobiles plus rapidement que ceux où les transactions par carte étaient déjà fortement implantées. Au Japon et en Corée, le paiement en numéraire représentait respectivement 50 % et 34 % du total des transactions en 2006, contre 14 % aux États-Unis (FRBB, 2010*a*). Ce constat ne peut toutefois être étendu à l'ensemble des pays. En Italie et en Grèce, où la part des transactions en espèces est très élevée, le marché des paiements mobiles n'a pas encore décollé.

Les paiements mobiles progressent néanmoins dans la plupart des régions. En 2009, le nombre d'utilisateurs de ce mode de règlement dans le monde était estimé à 108 millions, en hausse de 25.6 % par rapport à 2008, et on s'attendait à ce qu'il atteigne 147 millions en 2010 (Report Linker, 2010). ABI Research prévoit que les m-paiements aux États-Unis pourraient atteindre 2.4 milliards USD en 2010, soit le double de l'année précédente (tout en ne représentant, d'après les prévisions, que 8 % du marché total du commerce électronique) (Internet Retailer, 2010*c*). Dans certains pays, le nombre de commerçants qui lancent des sites de vente en ligne augmente, tout comme le nombre de mécanismes de paiement mobile. Ces dispositifs, qui sont de plus en plus souvent perçus par les commerçants et les

consommateurs comme une bonne solution pour l'achat de produits peu coûteux (25 USD au maximum), comprennent :

Les voyages, stationnement, billets de concert.

Les contenus et services mobiles tels que les jeux, la musique, les sonneries, les vidéos, les images, les actualités, la consultation d'annuaire et les itinéraires de déplacement en transport en commun.

Les achats aux distributeurs automatiques et aux diverses autres formes d'automates en libre-service.

L'essor rapide des paiements mobiles est dû, en partie, à la commodité d'emploi de ces dispositifs, y compris aux points de vente, où ils sont considérés comme remplaçant avantageusement les espèces. Le fait qu'ils permettent de payer ou de prépayer des achats facilement et sans le moindre compte bancaire peut également jouer en leur faveur. Les jeunes consommateurs, qui utilisent de plus en plus souvent des appareils portables au détriment des ordinateurs fixes, pour l'accès à Internet par exemple, montrent peut-être plus d'empressement à adopter les paiements mobiles. Selon une étude réalisée par Juniper Research, la disponibilité d'applications de paiement sûres et simples d'emploi, et la prise de conscience croissante chez les utilisateurs qu'ils peuvent effectuer des achats en ligne au moyen de leurs portables devraient stimuler le marché des articles numériques, comme les produits de loisirs et la billetterie, ainsi que des biens matériels, dont l'alimentation, l'habillement, les cadeaux et les livres. Juniper Research prévoit que la valeur des produits physiques et numériques achetés par des particuliers au moyen de leurs appareils portables, qui se chiffrait à 100 milliards USD dans le monde en 2010, pourrait doubler d'ici à 2012 (Juniper, 2010). En outre, d'aucuns anticipent que la mise en place et l'adoption de solutions de paiement mobile NFC donnera un nouveau coup de fouet à la croissance de ce secteur (Gigaom, 2011).

En 2009, le Conseil européen des paiements (EPC, European Payments Council) a confirmé cette tendance dans sa feuille de route pour les paiements mobiles (*Roadmap for Mobile Payments*) qui explore les moyens de faciliter les paiements NFC. Comme cela a été indiqué à l'occasion de l'atelier de travail sur les paiements, depuis 2007, la GSM Association (GSMA) travaille aux côtés de plus de 60 opérateurs majeurs de réseau mobile à son projet *Pay-Buy-Mobile*, afin de parvenir à une vision commune des paiements mobiles compatibles NFC au niveau national et international. Des initiatives de ce type commencent à être commercialisées dans certains pays, dont la France (depuis mai 2010) et le Royaume-Uni (depuis mai 2011). Dans de nombreux pays, toutefois, il reste encore beaucoup à faire pour stimuler l'adoption des paiements NFC : dans ces pays, les lecteurs NFC sont relativement peu nombreux et la volonté des grands acteurs du paiement d'investir dans cette technologie et de l'intégrer dans leur activité demeure limitée. En outre, la valeur ajoutée que ces moyens de paiement peuvent apporter aux consommateurs par rapport aux cartes de crédit et de débit reste à démontrer.

Dans quelques pays, en revanche, l'utilisation des téléphones portables pour les paiements NFC aux les points de vente a bien progressé, et les opérateurs de réseaux mobiles eux-mêmes travaillent depuis plusieurs années à offrir des solutions spécifiques de m-paiement. En Corée, en 2003, *LG Telecom* a noué un partenariat avec la *Kookmin Bank* pour mettre en place un système NFC. *SK Telecom* a, pour sa part, lancé *MONETA*, un service financier intégré avec et sans fil destiné aux téléphones portables. Les utilisateurs doivent s'inscrire pour obtenir une authentification auprès de *SK Telecom*. Les paiements sont ensuite effectués en insérant une puce *MONETA* dans le combiné. Au Japon, les ventes de combinés portables NFC ont franchi la barre des 64 millions à la fin de 2009 (FeliCa, 2010).

Le recours au paiement mobile varie selon les pays. En règle générale, les m-paiements sont utilisés pour traiter des transactions de faible montant. Au Canada et aux États-Unis, les paiements mobiles servent essentiellement à acheter des produits numériques et virtuels (comme la musique, les sonneries et

articles utilisés dans les jeux). Dans certains pays d'Asie et d'Europe, ils sont employés pour acheter une gamme plus large de produits, dont des billets de transport, des films en téléchargement et des biens physiques (Mopay, 2010).

En mars 2009, au Japon, la monnaie électronique sur téléphone portable totalisait 12.1 millions JPY, soit 11.5 % du total de la monnaie électronique comprenant les cartes prépayées, les cartes de crédit ainsi que les cartes-portemonnaies électroniques émises par les banques (Banque du Japon, 2009). En mars 2010, *NTT DoCoMo* comptait 14.2 millions d'abonnés pour son produit de paiement *iD*, dont 11.3 millions étaient des clients de *DCMX*. D'après des représentants de *NTT DoCoMo*, toutefois, la plupart des achats effectués à travers son service de paiement sont de faible montant et le marché du paiement mobile sans contact n'a pas encore atteint son plein potentiel. Les transactions de montant supérieur tarderaient à s'imposer. Certains services de paiement électronique (NFC ou non) sont également proposés, par exemple sous la forme de sommes prépayées ou de crédits. Une étude fait ressortir qu'au cours de l'exercice 2009, *Nanaco*, un service de paiement assuré par *Seven & I Holdings Co.*, la plus grande entreprise de distribution et de vente au détail du Japon, a été le service de paiement électronique prépayé le plus employé, tant pour les paiements mobiles que non mobiles, représentant 25.9 % de l'ensemble des transactions de paiement électronique (M's Communicate, 2010). Arrivait ensuite le service *Suica*, proposé par la compagnie ferroviaire *JR East*, avec 22.2% de parts de marché. Le succès de ces prestataires découle, en partie, de l'avantage que leur procure l'intégration de services de paiement dans leur activité. Ainsi, *Nanaco* est largement utilisé comme mode de paiement dans l'ensemble des points de vente du groupe *Seven & I Holdings Co*. *Suica* est surtout utilisé dans les transports publics, mais il est aussi communément accepté pour des achats en magasin ou en kiosque. Certaines entreprises comme *NTT DoCoMo* proposent en outre à leurs abonnés des services de paiement mobile à crédit.

En Amérique du Nord, il a été constaté en 2009 que 44 % des propriétaires d'*iPhone* achetaient des produits numériques (notamment des applications et des jeux), alors qu'ils n'étaient que 28 % en 2008. Parmi les options de paiement, les cartes de crédit et *PayPal* arrivaient en tête, 51 % des acheteurs ayant indiqué avoir recouru à l'une de ces deux méthodes, tandis que 16 % des consommateurs de produits numériques utilisaient le service *Facebook Credits* pour régler leurs achats (The Paypers, 2010*b*). Aux États-Unis, le prestataire de services de paiement mobile *Boku* a lancé en 2009 un service de paiement mobile permettant d'acheter des biens virtuels au moyen d'un téléphone portable sur des sites de réseaux sociaux et des portails de jeux. Depuis, la société gère le traitement des paiements mobiles pour le compte d'un grand nombre de développeurs de jeux et d'applications. Son service est assuré à travers 190 opérateurs de télécommunications répartis dans 58 pays, (soit un potentiel de 1.8 milliard de clients) (Virtual Goods News, 2010).

En Chine, selon des données fournies par iResearch, le secteur du paiement mobile a enregistré un total de 286 millions EUR de transactions en 2009, soit une augmentation de 202 % par rapport à l'année précédente. La croissance devrait se poursuivre aussi bien en 2011 (5 milliards EUR) qu'en 2012 (13.8 milliards EUR) The Paypers, 2010*d*). En mai 2010, 18 banques chinoises, associations de paiement par carte, opérateurs de réseau mobile, fabricants de téléphones et fournisseurs du secteur ont constitué une alliance. Leur but était de définir des normes et un modèle économique, afin de mettre en place une plateforme ouverte unique que les entreprises pourraient utiliser dans toute la Chine pour proposer des services de paiement NFC et mobile. Dans d'autres économies en développement, comme le Kenya, les Philippines et l'Inde, où la proportion de personnes possédant un compte bancaire est assez faible, le marché du paiement mobile semble également prometteur. En 2008, la majorité des 361 millions d'abonnés à la téléphonie mobile 3G dans le monde vivaient dans des économies émergentes et en transition (CNUCED, 2009). Toutefois, il convient de noter que, dans ces pays, les m-paiements sont principalement des paiements entre personnes et des transferts de fonds.

PROBLÈMES RENCONTRÉS PAR LES CONSOMMATEURS DANS LE CADRE DES PAIEMENTS EN LIGNE ET MOBILES

Les responsables des politiques et autres parties prenantes doivent faire face à trois sortes de problèmes rencontrés par les consommateurs dans les marchés du paiement en ligne et mobiles.

Le premier type d'enjeux concerne les cadres réglementaires, qui englobent à la fois les règles de droit et des mesures relevant du secteur privé. Comme on l'a vu dans le cadre de la section I de ce rapport, un certain nombre d'acteurs, et particulièrement des établissements financiers et non financiers, interviennent dans les transactions de paiement en ligne aux côtés des consommateurs. Leurs activités peuvent être soumises à des règlementations divergentes en matière de télécommunications, de concurrence, de services financiers ainsi qu'en matière de protection des consommateurs (propre au commerce électronique et/ou aux paiements, ou bien encore d'ordre général). Parfois, les consommateurs, les commerçants et d'autres parties intervenant dans la transaction n'ont qu'une connaissance imparfaite des normes légales ou d'autorégulation qui régissent la transaction en question et ne comprennent pas bien comment les responsabilités se répartissent – en cas de fraude ou de problèmes liés à la sécurité par exemple – ni quels sont les mécanismes de règlement des différends ou les droits à réparation dont peuvent bénéficier les consommateurs lorsqu'un problème survient. Ces parties prenantes elles-mêmes peuvent avoir une perception différente de leurs responsabilités respectives, ce qui complique encore la situation (FRBB, 2010). La question revêt une acuité particulière dans le cas des paiements mobiles qui font intervenir un certain nombre d'acteurs, tous susceptibles d'être responsables, au moins partiellement, en cas de problème : opérateurs de réseau mobile, organismes de paiement, réseaux de cartes de débit ou de crédit, chambres de compensation et de règlement, fournisseurs de solutions logicielles, commerçants et développeurs d'applications. Dans beaucoup de pays de l'OCDE, le commerce électronique et les paiements mobiles ne sont régis par aucune loi particulière et leur degré de prise en charge par les règles générales de protection des consommateurs reste souvent à vérifier.

Le second type d'enjeux comprend des questions générales qui intéressent les consommateurs, à savoir : les débits non autorisés ; la non-livraison, le retard de livraison, la non-conformité des produits ; ainsi que le règlement des litiges et la réparation. À ces questions sont étroitement liées celles de l'information, de l'autonomisation et de l'éducation des consommateurs.

Le troisième type d'enjeux concerne les aspects techniques ayant attrait aux paiements et relatifs aux transactions. Il s'agit notamment ici des questions de sécurité, comme la gestion des identités numériques. Les questions concernant l'interopérabilité, les options de paiement dont dispose le consommateur ainsi que le commerce électronique transfrontières sont également importantes.

I. Enjeux d'ordre réglementaire

Le niveau de protection dont bénéficient les consommateurs lors de paiements en ligne et mobiles varie considérablement d'un pays à l'autre et à l'intérieur même de chaque pays (OCDE, 2005, p. 14). Plusieurs facteurs interviennent ici :

- L'instrument utilisé pour traiter le paiement (comme les cartes de débit/crédit, les SMS, les cartes prépayées, *etc*.).
- Le véhicule employé pour effectuer le paiement (Internet ou appareils portables entraînant, par exemple, l'ajout du paiement à la facture de téléphonie mobile).
- L'organisme de paiement concerné (banque ou organisation non bancaire).

La nature du problème (non-livraison, retard de livraison, non-conformité, erreurs de traitement ou de facturation, mais aussi pratiques trompeuses telles que l'usage de faux ou les débits non autorisés).

La nature du bien acheté (corporel ou incorporel). Que ce soit lors de la table ronde organisée par l'OCDE sur les contenus numériques ou lors de l'atelier sur les paiements, les parties prenantes ont relevé l'absence de lois de protection des consommateurs régissant spécifiquement l'achat de produits incorporels (comme les livres électroniques et les jeux).

La nature de la transaction (paiements entre personnes ou paiements entre entreprises et consommateurs en ligne [B2C]).

À la lumière de ce qui a été dit plus haut, on peut se demander si les nouveaux dispositifs de paiement, comme les cartes prépayées et les systèmes de paiement mobile (dans lesquels le paiement est traité par un opérateur de réseau mobile), sont couverts par les régimes juridiques et réglementaires applicables aux cartes de crédit et de débit classiques (voir TACD, 2009). La Federal Trade Commission des États-Unis met en évidence des différences sur ces aspects dans son guide intitulé *Consumer Guide to E-Payments* (FTC, 2003). Elle note que les utilisateurs de cartes prépayées ne bénéficient pas du même type de protection que, par exemple, les titulaires d'un compte *PayPal* associé à un compte bancaire ou à une carte de crédit. Les études font apparaître en outre que les pays n'octroient aux consommateurs que peu de droits au dédommagement ou à la réparation qui soient exécutoires en cas de défaut ou de non-livraison d'un produit numérique mobile (Consumer Focus, 2009). Au Royaume-Uni, on s'interroge sur la question de savoir si le paiement mobile, qui permet au consommateur de dépenser à hauteur d'une certaine somme et de payer ultérieurement, ne devrait pas être considéré comme un accord de crédit plutôt que comme un service de paiement. Si la première interprétation l'emportait, les consommateurs pourraient bénéficier des possibilités de remboursement que prévoit la loi britannique de 1974 sur le crédit à la consommation, intitulée *Consumer Credit Act* (Consumer Credit Act, 1974), ainsi que des protections anti-fraude.

Il est difficile de dire à quel point les consommateurs sont informés du niveau de protection associé aux différents mécanismes de paiement. Il serait utile à cet égard de rechercher les facteurs qui guident leur choix d'un mode de paiement.

Cadres réglementaires en place

L'environnement réglementaire qui régit les paiements en ligne et mobiles est en constante évolution. Certains pays ont une législation propre à ces modes de paiement, tandis que d'autres appliquent les réglementations générales relatives à la protection des consommateurs, aux télécommunications ou au secteur financier.

La Corée applique une réglementation spécifique. En vertu de la *Loi sur les transactions financières électroniques* adoptée en 2007 et de la *Loi sur la protection des consommateurs dans le domaine du e-commerce*, les prestataires de services de paiement intervenant dans le commerce électronique doivent :

Utiliser des formulaires de commande qui permettent aux consommateurs de modifier ou de confirmer leur commande avant la validation définitive.

Fournir au consommateur des informations sur le vendeur (qui doivent aussi figurer sur le site web de celui-ci) et sur les mécanismes disponibles en vue du règlement des litiges.

Protéger les informations personnelles que les consommateurs communiquent durant le traitement du paiement.

De nouvelles réglementations sont en cours d'élaboration et de mise en œuvre dans d'autres pays. Au Canada, l'ensemble du cadre des paiements fait actuellement l'objet d'une remise à plat, l'objectif étant de déterminer comment les règles en place devraient être adaptées ou s'il conviendrait d'en élaborer de nouvelles pour apporter une réponse efficace aux problèmes qui commencent à se poser. Des recommandations doivent être transmises au ministre des Finances d'ici à fin 2011. L'Encadré 2 présente un résumé des évolutions survenues dans d'autres pays.

Encadré 2. Évolution de la réglementation

Fédération de Russie : En 2010, le gouvernement a approuvé le projet de loi sur le Système national de paiement. Destiné à réglementer les paiements électroniques, ce système exige des opérateurs de monnaie électronique qu'ils acquièrent une licence auprès de la Banque Centrale (The Paypers, 2010*e*).

États-Unis : En juillet 2010, le Congrès a adopté la loi intitulée *Wall Street Reform and Consumer Protection Act* (réforme de Wall Street et protection des consommateurs), dite loi Dodd-Frank (Dodd-Frank Act, 2010). En vertu de cette loi, la Réserve Fédérale doit établir des normes applicables aux commissions perçues sur les paiements par carte de débit (appelées « commissions d'interchange »), pour faire en sorte que celles-ci soient raisonnables et proportionnées au coût du traitement de ces transactions, que la carte de débit soit une carte classique ou une carte prépayée rechargeable. La loi permet aussi aux commerçants de fixer un montant minimal pour l'utilisation de la carte de crédit, à condition que ce minimum ne dépasse pas 10 USD, ou encore d'offrir un escompte si les consommateurs règlent en espèces, par exemple, plutôt que par carte de crédit, étant entendu que ces réductions ne doivent pas être liées à un émetteur ou un réseau de cartes particulier. Le Conseil de la Réserve fédérale a publié en juin 2011 une mesure finale d'application, qui définit les normes à appliquer pour évaluer si les commissions d'interchange des cartes de débit perçues par les émetteurs sont raisonnables et proportionnées aux coûts supportés. Aux termes de cette mesure d'application, la commission d'interchange maximale qu'un émetteur est autorisé à percevoir pour une transaction de débit électronique est fixée à 0.21 USD par transaction plus 5 points de base multipliés par la valeur de la transaction. En outre, la loi Dodd Frank donne au Consumer Financial Protection Bureau des États-Unis, récemment créé, des pouvoirs de réglementation, de supervision et d'exécution sur un large éventail d'entités fournissant des produits et services financiers utilisés par les consommateurs. Cela comprend notamment les entités fournissant des mécanismes de paiement par tout moyen technologique, comme les systèmes de banque en ligne ou les réseaux de téléphonie mobile. La nouvelle agence, qui est devenue opérationnelle le 21 juillet 2011, disposera également de vastes pouvoirs en matière de pratiques et d'agissements déloyaux, trompeurs ou illicites dans le domaine des services financiers aux consommateurs.

UE : Ces dernières années, divers instruments réglementaires ont été élaborés pour harmoniser et sécuriser les systèmes de paiement en ligne et renforcer la confiance des consommateurs dans ces dispositifs, dans la perspective de créer un marché unique sans frontières. Exemples :

Directive 2007/64/CE concernant les services de paiement (PSD) dans le marché intérieur (Directive PSD, 2007) : Cette directive a été adoptée pour créer, à l'échelle de l'UE, un marché unique des règlements scripturaux transfrontières traités dans l'espace économique européen (l'EEE, qui comprend également la Norvège, l'Islande et le Liechtenstein). Ce texte couvre le paiement hors ligne, en ligne et mobile. Il contient des règles sur la transparence, les modalités de paiement et les informations à communiquer aux consommateurs, en particulier les conditions générales des services proposés, les mesures de sécurité et de prévention de la fraude, ainsi que les droits et obligations des utilisateurs et des prestataires des services de paiement, notamment les règles de responsabilité en cas de défaut ou de non-exécution d'une transaction de paiement ou d'utilisation frauduleuse d'un instrument de paiement. La directive offre un cadre destiné à protéger les consommateurs contre les transactions récurrentes non souhaitées, qui leur permet de contacter leur banque afin d'arrêter le traitement des paiements restants. Il convient de noter, toutefois, qu'en ce qui concerne les paiements déjà effectués, les banques demandent généralement de commencer par s'adresser au commerçant. Enfin, la directive met en place un régime d'octroi des agréments, qui a pour objet d'encourager les organismes non bancaires à entrer sur le marché des services de paiement.

Directive 2009/110/CE concernant la monnaie électronique (Directive sur la monnaie électronique, 2009) : cet instrument, qui doit être interprété en conjonction avec la directive précédente, a pour but de réglementer les conditions dans lesquelles les organismes non bancaires pouvaient émettre de la monnaie électronique parallèlement aux établissements de crédit. La monnaie électronique se définit comme la valeur monétaire émise à la réception de fonds. Elle est stockée sur un support de paiement électronique ou à distance sur un serveur, et gérée par celui qui en est détenteur, au moyen d'un compte prévu à cet effet (ce qui comprend les autres prestataires de paiement). Ce concept a été élaboré en réponse à l'émergence et à l'utilisation croissante de produits prépayés de paiement électronique, qui sont utilisés en particulier pour traiter des micro-paiements au moyen de téléphones portables.

Directive 2000/31/CE sur le commerce électronique (Directive sur le commerce électronique, 2000) **:** un examen de l'efficacité de cette directive a été lancé par la Commission européenne en 2010.

Directive relative aux droits des consommateurs (Directive sur les droits des consommateurs, 2011) : à la suite de l'examen de l'*acquis communautaire en matière de protection des consommateurs* entrepris par la Commission européenne en 2004, une Directive relative aux droits des consommateurs a été adoptée en juillet 2011, pour renforcer et pleinement harmoniser la législation applicable aux ventes à distance dans l'ensemble des pays membres de l'UE. Cet instrument vise à protéger efficacement les consommateurs, en particulier lors de l'achat de contenus numériques et dans le cas de transactions transfrontières. Son article 9 prévoit la communication aux consommateurs d'informations obligatoires avant la conclusion de toute transaction distante (ce qui comprend la plupart des transactions en ligne et mobiles), notamment les modalités de paiement, de livraison et d'exécution, et la procédure à suivre pour adresser une réclamation. Les États membres de l'UE devront avoir transposé la Directive dans leur droit national d'ici le 13 décembre 2013.

Dans le prolongement de son *Livre vert* sur un marché communautaire intégré pour les paiements par carte, par Internet et sur mobiles (CE, 2012*a*), la CE va élaborer, courant 2012, une stratégie visant notamment à évaluer les obstacles à l'accès et à la concurrence sur ces marchés et à faire en sorte que les services de paiement soient transparents pour les consommateurs et les vendeurs (CE, 2012*c*).

Initiatives sectorielles générales

Parallèlement aux initiatives de réglementation, plusieurs mesures sectorielles ont été prises sur les marchés des paiements en ligne et mobile.

SEPA, e-SEPA, SEPA mobile

Pour mettre en œuvre les instruments juridiques de l'UE évoqués précédemment, des règles et normes visant à créer un espace unique de paiements en euros (SEPA) sont en cours d'élaboration par le secteur bancaire, avec le soutien énergique des institutions européennes. Dans le cadre du SEPA, les consommateurs des pays appartenant à cet espace pourront effectuer des paiements en utilisant un ensemble commun d'instruments de paiement libellés en euros, sans souci des frontières internes, avec les mêmes droits et obligations et où qu'ils se trouvent. Afin de superviser l'initiative, le secteur bancaire a créé un consortium, le Conseil européen des paiements (CEP), dont le rôle est d'examiner le fonctionnement pratique de SEPA pour les entreprises souhaitant y participer (voir CEP, 2010*b*). Dernièrement, la Commission européenne a proposé de fixer les dates pour la migration vers les virements et prélèvements paneuropéens.

Des travaux sont en cours pour faire en sorte que ce nouveau marché sans frontières couvre aussi les paiements en ligne et mobiles. S'agissant de ces derniers, le CEP collabore avec les banques, les établissements de paiement et les opérateurs de réseau mobile à l'harmonisation des normes relatives aux m-paiements, de manière à soutenir leur développement au sein des banques (CEP, 2010*a*). En 2011, le CEP, qui voit dans ces paiements un bon moyen d'exploiter et de promouvoir l'utilisation des instruments de paiement SEPA, a publié un guide de mise en œuvre consacré à la question (CEP, 2011).

Systèmes de marques de confiance

Un certain nombre de systèmes de marques de confiance ont été instaurés pour rassurer les consommateurs à propos du commerce électronique. Ces dispositifs ont pour but de garantir aux consommateurs, d'une part, que les commerçants se conforment à certaines règles visant à renforcer la sécurité et la confidentialité des informations et à lutter contre les pratiques commerciales déloyales, et, d'autre part, que les paiements répondent à des normes bien précises. Ces marques de confiance nationales s'appuient souvent sur des mécanismes d'application des normes (EMOTA, 2010).

Entre autres exemples, on citera la marque suédoise *Trygg E-Handel*, lancée en 2007 dans le cadre d'un consortium entre organisations privées et publiques. Son rôle est d'appuyer l'élaboration de lignes directrices unifiées à l'intention des consommateurs et des entreprises du commerce électronique (Figure 2). Dans ce système, un administrateur réalise des vérifications aléatoires. Les membres du consortium de la marque de confiance se voient également attribuer une note financière. Un prestataire externe effectue un audit des pages d'accueil des membres, en examinant les points suivants :

- les informations relatives à la société et aux produits ;
- les informations sur le coût total d'un produit ;
- les délais de livraison ;
- les informations sur la garantie ;
- les conditions d'annulation des contrats ;
- le traitement des réclamations ;
- la prise en compte de l'âge des consommateurs ;
- les dispositifs de sécurité financière et de sécurisation des paiements

Figure 2. Exemple de marque de confiance : Svensk Distanshandel, en Suède

II. Questions générales relatives à la protection des consommateurs

La protection des consommateurs en matière de paiements pose un certain nombre de problèmes ou questions d'ordre général : *i*) débits non autorisés ; *ii)* pratiques commerciales mensongères et frauduleuses ; *iii*) non-livraison, retard de livraison et non-conformité des produits ; *iv*) règlement des litiges et réparation ; *v*) information, autonomisation et éducation des consommateurs.

Débits non autorisés

Les débits non autorisés associés aux paiements en ligne et mobiles comprennent : *i*) les montants prélevés sur le compte d'un consommateur suite à l'utilisation illicite d'informations financières ou personnelles (mot de passe donnant accès à un compte en ligne, ou numéro de carte de crédit ou de débit traité en ligne) ; *ii*) les montants débités sur un compte en ligne sans le consentement du consommateur. Ils résultent parfois de pratiques frauduleuses, mais pas toujours. Il peut s'agir par exemple d'un paiement effectué par un enfant sans l'accord de ses parents.

Il y a débit non autorisé quand un tiers se sert des coordonnées d'un consommateur pour acheter un article en ligne à l'insu de ce dernier ou sans son accord. Des parties prenantes indiquent que ce type de fraude demeure un problème majeur des paiements en ligne et mobiles. Dans de nombreux cas, la fraude intervient lorsqu'un escroc récupère et utilise les données personnelles précédemment communiquées en ligne par le consommateur. C'est ce que l'on appelle le vol d'identité en ligne (Voir OCDE, 2008*a* et *b*).

En dépit de toutes les initiatives d'amélioration de la sécurité, la plupart des systèmes de paiement en ligne demeurent exposés au problème des débits non autorisés. Le type de risques varie selon les moyens de paiement. Les cartes de crédit et de débit, par exemple, n'ont pas été conçues initialement pour être utilisées sur Internet ; toute personne qui vole les coordonnées d'une carte peut s'en servir pour acheter un article, sans même avoir la carte entre les mains.

Protections juridiques

Les autorités de réglementation ont déployé des efforts considérables pour répondre aux inquiétudes des consommateurs, notamment par l'instauration de mécanismes de remboursement. Ces mécanismes sont fournis par les émetteurs des cartes de paiement pour apporter des solutions aux consommateurs lorsque des achats se terminent mal. Ainsi, aux États-Unis, la responsabilité du consommateur en cas de perte ou de vol de sa carte de crédit est plafonnée à 50 USD en vertu de la loi intitulée *Fair Credit Billing Act* (loi sur la transparence de la facturation des crédits renouvelables). Lorsque seul le numéro de carte de crédit du consommateur a été utilisé sans autorisation, la responsabilité est nulle. Conformément à la loi intitulée *Electronic Fund Transfer Act* (loi sur les transferts électroniques de fonds), l'emploi non autorisé d'une carte de débit peut engager la responsabilité du consommateur à hauteur de 50 à 500 USD, au minimum, voire davantage, selon le délai écoulé avant déclaration de la perte ou du vol de la carte. Dans l'Union européenne (ainsi qu'en Islande, au Liechtenstein et en Norvège), les consommateurs ont droit, conformément à la *Directive concernant les services de paiement*, au remboursement immédiat des débits non autorisés ou des sommes débitées par erreur (CE, 2007). Il convient de noter, toutefois, que cette directive instaure un équilibre entre la responsabilité du consommateur et celle du commerçant. La responsabilité du consommateur est dégagée uniquement s'il a informé le commerçant dès que possible, ou dans les 13 mois suivant la transaction frauduleuse. En Finlande, la *loi sur les services de paiement* limite la responsabilité des consommateurs en cas d'utilisation non autorisée de cartes de crédit, de cartes de débit et de certains paiements mobiles. En France, le *Code monétaire et financier* prévoit que le titulaire d'une carte ne peut pas être tenu responsable d'un paiement effectué sans son autorisation, à distance et sans utilisation physique de la carte. Au Mexique, en application du *règlement 34/2010*, un utilisateur qui informe la banque émettrice du vol ou de la perte de sa carte de crédit n'est pas responsable des paiements effectués avec celle-ci après le signalement. Le titulaire d'une carte peut déposer une réclamation auprès de la banque émettrice dans les 90 jours qui suivent le paiement. Au Canada, la responsabilité maximale du consommateur est de 50 CAD. Des recherches récentes menées au Royaume-Uni révèlent que sur les 6 % d'internautes à avoir perdu de l'argent en raison d'un vol d'identité en ligne, les victimes avaient réussi à obtenir un remboursement de la part de leur prestataire de paiement dans trois quarts des cas (OFT, 2010*a*, p. 16 ; OFT, 2010*b*, p. 69).

Protections émanant des organisations sectorielles

Le secteur du paiement également a pris des mesures pour assurer aux consommateurs une protection au moyen de mécanismes de remboursement. Au Royaume-Uni, en vertu du *Banking Code* (Code bancaire), un titulaire de carte n'aura généralement rien à payer si quelqu'un d'autre a utilisé les coordonnées de sa carte sans autorisation (BBA, 2008, paragraphe 12.12). Aux termes des *Conditions d'utilisation du service PayPal*, le consommateur peut être remboursé intégralement en cas de débits non autorisés ou d'erreurs de traitement, à condition qu'il signale les éventuelles transactions illicites à la société dans les 60 jours suivant la première apparition du problème sur son compte. Faute de quoi, le consommateur pourra être tenu responsable des pertes occasionnées après cette période de 60 jours si *PayPal* peut prouver que, informée à temps, elle aurait eu les moyens de les empêcher. Ce délai pourra être étendu au-delà de 60 jours si le signalement n'a pas pu être effectué pour une « raison valable, hospitalisation par exemple » (PayPal, 2010). En outre, *Visa*, *MasterCard* et *American Express* ont mis en place des systèmes volontaires, généralement dits de « responsabilité zéro », dans lesquels la responsabilité du client n'est pas engagée en cas d'utilisation non autorisée de sa carte de crédit. Pour les achats payés

avec une carte de débit, le *Code de pratique canadien des services de cartes de débit* énonce les pratiques sectorielles ainsi que les responsabilités liées à ce type de carte qui incombent aux consommateurs et aux prestataires de services. Ce code volontaire, entériné par les banques, les caisses de crédit et les caisses populaires, stipule expressément que le consommateur n'est pas responsable des pertes résultant de circonstances indépendantes de sa volonté.

Responsabilités relatives aux paiements mobiles

S'agissant des paiements mobiles, d'aucuns ont demandé le renforcement de la protection des consommateurs contre les débits non autorisés. Alors que les cas de vol et de débits non autorisés sont fréquents, dans un certain nombre de pays, c'est le consommateur qui, la plupart du temps, supporte la responsabilité des éventuelles pertes financières (Consumer Focus, 2009). En vertu des cadres mis en place dans la grande majorité des pays, si un consommateur effectue un paiement mobile à distance avec une carte de crédit ou de débit, il a droit aux protections associées à celle-ci. En revanche, si le service de paiement est assuré directement par un opérateur de téléphonie mobile et que l'achat est porté sur la facture d'abonnement du consommateur, il peut ne pas y avoir de protection juridique (MacCarthy & Hillebrand, 2010). De même, lorsque l'opérateur de téléphonie mobile a demandé au consommateur d'effectuer un dépôt pour couvrir ses achats ultérieurs, le consommateur risque de ne bénéficier d'aucune protection. Avec l'application de paiement de Facebook *Spare Change*, qui peut être téléchargée sur des téléphones portables pour faire des achats de faible montant, aucun remboursement n'est prévu (Facebook, 2009).

Quelques pays ont instauré des mesures de protection spécifiques pour les paiements mobiles. Au Danemark, la carte SIM (Subscriber Identification Module, module d'identification de l'abonné) incluse dans les téléphones portables est explicitement considérée comme un moyen de paiement comme un autre. Résultat, il incombe à l'organisme d'émission d'indemniser le détenteur du téléphone portable pour toute perte due à une utilisation non autorisée (OCDE, 2007*c*, p. 31). En Norvège, si le vol d'un téléphone portable est signalé à l'opérateur, le consommateur n'est pas responsable des sommes débitées par la suite. De même en Finlande, la *loi relative au marché des communications* prévoit de limiter la responsabilité des consommateurs en cas d'utilisation non autorisée des appareils portables. Au Canada, en Suède et aux États-Unis, la législation couvre parfois certains cas d'emploi illicite des téléphones portables. Aux États-Unis, le Procureur général de Californie a conclu un accord de règlement avec l'opérateur de téléphonie mobile *AT&T Mobility*, en vertu duquel ce dernier ne facturera pas à ses clients des services non autorisés. L'accord impose à l'opérateur de créditer le compte du consommateur ou d'ouvrir une enquête sans délai lorsqu'un consommateur signale que des appels ont été réalisés après la perte ou le vol de son combiné. L'opérateur ne peut facturer le consommateur que si l'enquête détermine que celui-ci avait bel et bien autorisé l'opération. D'autres opérateurs de télécommunications du pays ont adopté des politiques similaires. En Finlande, l'association des consommateurs a déposé une proposition de loi (en cours d'examen), aux termes de laquelle les opérateurs de réseau mobile qui traitent des paiements pour l'achat de produits seraient tenus responsables en cas de problèmes liés à la transaction. La directive de la Commission européenne concernant les droits des consommateurs, qui contient des dispositions relatives aux mécanismes de remboursement, ne se limite pas à une technologie en particulier et couvre les problèmes liés aux paiements mobiles (Directive sur les droits des consommateurs, 2011).

Pratiques commerciales trompeuses et frauduleuses

Les pratiques commerciales trompeuses ou frauduleuses sont souvent liées à une information inadéquate ou mensongère. Avec les appareils portables, les questions d'information prennent une acuité particulière en raison de la petite taille de l'écran et des difficultés qui en découlent pour naviguer d'un lien ou d'une page à l'autre afin de prendre connaissance des conditions d'achat. Il faut toutefois noter qu'avec la prévalence croissante des terminaux dotés d'écrans de plus grande taille et de plus de mémoire , comme les *smartphones* et les tablettes informatiques, certains de ces problèmes pourraient s'atténuer. Parfois, il

est même impossible de consulter les conditions générales sur les plateformes de m-commerce du fait de limitations techniques.

Certaines informations clés, comme le coût réel total de la transaction, peuvent être dissimulées dans les conditions générales de vente, ce qui accroît le risque que les consommateurs n'aient pas conscience de ces coûts ou qu'ils ne les comprennent pas. En outre, dans les cas où les achats sont ajoutés à l'abonnement de téléphonie mobile, et non facturés à la société émettrice de la carte de crédit, le consommateur risque de s'apercevoir qu'il ne bénéficie, dans le meilleur des cas, que d'une faible partie des protections que ces sociétés peuvent offrir. Cette situation peut devenir très problématique pour les consommateurs qui s'attendent à voir leurs litiges réglés comme ils le sont habituellement en cas de paiement par carte de crédit : la présentation claire et lisible des conditions générales revêt alors une importance accrue dans le cas des transactions mobiles.

Les conséquences des pratiques commerciales trompeuses peuvent être considérables. Ainsi, l'Office of Fair Trading (OFT, Bureau de la concurrence) au Royaume-Uni estimait en 2007 que les débits supplémentaires non prévus coûtaient entre 76 et 126 millions EUR par an aux seuls consommateurs britanniques (CE, 2008*c*). Les répercussions sont particulièrement nettes dans le cas des enfants, qui ne s'aperçoivent pas toujours qu'ils s'exposent à des coûts supplémentaires ou qu'ils ont souscrit un service assorti d'un prélèvement régulier sur une carte téléphonique prépayée. En 2008, quelque 23.7 % des adolescents belges ont indiqué qu'ils avaient payé une sonnerie plus chère que prévu et 7.5 % qu'ils s'étaient abonnés à un service du type de celui mentionné précédemment sans s'en rendre compte (OCDE, 2011*a*).

Face à ces problèmes, certains pays appliquent au commerce mobile les dispositions générales de protection des consommateurs interdisant toute action ou pratique trompeuse ou déloyale. Au Canada, par exemple, la *Loi sur la concurrence* contient une disposition prohibant les indications et les pratiques commerciales trompeuses, et ce indépendamment de la technologie utilisée (OCDE, 2007*c*, p. 27). Le texte a été amendé en décembre 2010, pour y ajouter des dispositions et des outils spécifiquement destinés à lutter contre de telles indications ou pratiques sur le cybermarché, notamment celles consistant à falsifier l'objet, l'expéditeur ou l'URL (localisateur) d'un message électronique. Ces amendements devraient entrer en vigueur au début de 2012.

Aux États-Unis, en octobre 2010, *Verizon Wireless* a accepté de payer une amende de 25 millions USD pour régler un différend qui l'opposait à la Federal Communications Commission, laquelle l'accusait de prélever des sommes sans autorisation à ses clients depuis plusieurs années. Suite à l'accord de règlement, *Verizon Wireless* a remboursé environ 15 millions de clients pour un montant total supérieur à 50 millions USD. En Finlande, en février 2011, la *loi relative au marché des communications* a été amendée, afin de doter l'organisme de protection des consommateurs de nouveaux pouvoirs d'application qui lui permettent d'ordonner à un opérateur de télécommunications de désactiver un numéro de téléphone portable utilisé pour offrir des services de contenus frauduleux ou trompeurs.

La transmission de données dans un but marketing

La transmission de données dans un but marketing est une pratique par laquelle des plateformes de commerce électronique nouent des partenariats financiers avec des parties prenantes tierces pour inciter les consommateurs à acheter des biens ou services à ces parties tierces (programmes d'abonnement, par exemple) sans que l'acheteur réalise nécessairement qu'il effectue une transaction avec ces dernières. En vertu de ces partenariats, les coordonnées de la carte de crédit ou de débit du client peuvent être transmises automatiquement par le site marchand « connu » à la société tierce, à l'insu et sans le consentement du consommateur. Souvent, l'offre intervient dans la phase qui suit la transaction, entre l'acte d'achat et la validation du processus de confirmation de la vente par le consommateur (Sénat [États-Unis], 2009). Les

options présentées au consommateur sont trompeuses et celui-ci peut raisonnablement croire qu'il termine la transaction originale et non qu'il s'engage dans une nouvelle opération.

En 2010, *Visa* a lancé une initiative destinée à empêcher la transmission de données dans un but marketing sur son réseau. *Visa* exige désormais des consommateurs qu'ils ressaisissent les coordonnées de leur carte de crédit s'ils souhaitent acheter un produit ou un service auprès d'une partie tierce (Credit Union Times, 2010). En décembre 2010, le Président des États-Unis a promulgué la loi intitulée *Restore Online Shoppers' Confidence Act* (ROSCA, loi sur le rétablissement de la confiance des acheteurs en ligne), laquelle interdit tout particulièrement les pratiques de transmission de données dans un but marketing en ligne. La loi ROSCA oblige les vendeurs tiers à fournir au consommateur des informations précontractuelles claires avant toute vente, notamment sur le fait qu'ils ne sont pas affiliés au commerçant initial. Elle stipule en outre que les vendeurs doivent obtenir le consentement éclairé du consommateur directement auprès de celui-ci, ce qui implique de lui indiquer le montant total à payer, de lui demander de saisir ses coordonnées et de l'inviter à confirmer la nouvelle transaction séparément de la transaction initiale.

Ventes par défaut

Les ventes par défaut représentent également un problème croissant pour les consommateurs internautes. Cette pratique consiste pour une entreprise à considérer le silence ou l'absence d'annulation par un consommateur comme valant acceptation d'une offre et autorisation d'être facturé. Ainsi le consommateur peut recevoir un exemplaire gratuit d'un quotidien en ligne, qui débouche automatiquement sur un abonnement à moins d'un annulation dans un délai prescrit. Si le procédé peut sembler commode au consommateur, l'absence d'autorisation expresse de celui-ci ou le fait qu'il ne soit pas bien informé du contenu de l'offre et des conséquences financières à long terme qui en découlent peuvent poser problème.

Le 1er juillet 2009, la Communications and Media Authority d'Australie (ACMA, autorité de régulation des communications et des médias en Australie) a donné force de loi au code sectoriel intitulé *Mobile Premium Services Code* (MPSC, code des services annexes de la téléphonie mobile), qui institue notamment une obligation de double validation : le client potentiel devra confirmer son choix à deux reprises avant de pouvoir souscrire un abonnement SMS « premium ». En outre, depuis novembre 2010, l'ACMA peut rendre une ordonnance temporaire d'interdiction de facturation (*Do Not Bill*), afin d'empêcher les fournisseurs de contenus suspects de facturer les clients pendant qu'elle enquête sur un service. À la suite de la révision du MPSC, l'ACMA a examiné en 2010, en coordination avec les acteurs du secteur et des groupes de consommateurs, le code sectoriel de protection des consommateurs de télécommunications (*Telecom Consumer Protections Code*, TPSC). À l'issue de cet examen, le MPSC devrait être intégré dans le TPSC.

Des évolutions similaires ont été observées à Singapour où, à compter de janvier 2011, en vertu du *Telecom Competition Code* (code de concurrence applicable aux télécommunications) révisé, les opérateurs de téléphonie mobile ne seront plus autorisés à facturer automatiquement un service initialement proposé à titre gratuit, une fois la période d'essai terminée ; ils devront obtenir l'autorisation préalable expresse du consommateur (IDA, 2010). Aux États-Unis, en application de la section IV de la loi ROSCA, les commerçants en ligne ont interdiction de pratiquer la vente par défaut de biens ou services, s'ils n'ont pas *i*) informé le consommateur de manière claire et lisible des conditions matérielles de l'opération ; *ii*) obtenu le consentement du consommateur avant le début des prélèvements ; *iii*) donné au consommateur un moyen simple de mettre fin aux prélèvements. La FTC a ouvert plusieurs dossiers de poursuites portant sur des affaires de vente par défaut.

Bourrage de facture

Autre pratique préoccupante évoquée, le bourrage de facture *(ou « cramming »)*, qui consiste à facturer des commissions ou des frais pour des services que les consommateurs n'ont ni achetés ni autorisés, généralement après qu'ils ont répondu à un courriel ou téléchargé un article qu'ils pensaient gratuit ou de très faible montant. Les lignes directrices édictées par la Mobile Marketing Association (MMA, association pour le marketing mobile) en vue de l'adoption de meilleures pratiques de consommation aux États-Unis (*United States Consumer Best Practices Guidelines*), ci-après dénommées « les lignes directrices de la MMA », imposent aux commerçants du marché national américain d'obtenir des consommateurs une double validation de leurs achats ; en d'autres termes, l'opérateur est tenu de demander au consommateur de confirmer à deux reprises sa décision d'acquérir un service annexe (pour un coût supplémentaire) avant de lui facturer ledit service. Destinées au marché des États-Unis, les lignes directrices de la MMA contiennent aussi des indications précieuses pour les distributeurs de produits et services mobiles, dont certaines techniques peuvent contrevenir aux lois contre les pratiques commerciales trompeuses et déloyales. Elles abordent notamment les questions suivantes : *i*) les jeux de hasard et les concours – rappelant l'obligation de proposer une autre méthode gratuite de participation et soulignant la nécessité de solliciter un avis juridique lors de l'élaboration des règles ; *ii*) l'emploi des termes « gratuit » et « bonus » – rappelant le bon usage de ces termes ; *iii*) le marketing d'affiliation – définissant cette notion et prodiguant des recommandations à l'intention des fournisseurs de contenus qui font appel à des distributeurs affiliés ; *iv*) les conditions générales de vente – donnant des conseils sur les meilleures pratiques à appliquer pour faire en sorte que ces dispositions soient communiquées de façon claire et lisible aux consommateurs.

En juillet 2011, la Federal Communications Commission des États-Unis (FCC, Commission des communications fédérales des États-Unis) a proposé des règles relatives au bourrage des factures. Bien que cette pratique s'observe surtout à ce jour sur les factures de téléphonie fixe, ces règles prévoient de faire obligation aux entreprises de télécommunications, y compris aux opérateurs de réseau sans fil, d'indiquer sur les factures téléphoniques et sur leurs sites web les conditions dans lesquelles les consommateurs peuvent déposer une réclamation auprès de la FCC (FCC [États-Unis], 2011). La FCC s'efforce également de recueillir des avis sur la question de savoir s'il faut exiger des opérateurs de télécommunications avec ou sans fil qu'ils fournissent les coordonnées précises des fournisseurs tiers sur les factures téléphoniques de leurs clients ou qu'ils recherchent d'éventuels antécédents de non-respect des règles en vigueur chez ces fournisseurs avant d'accepter toute imputation d'achats effectués auprès de ces derniers sur la facture téléphonique d'un client.

Applications

Les problèmes de paiement liés aux applications utilisées sur les appareils portables sont une autre source de préoccupation évoquée par les participants à la table ronde de l'OCDE sur les contenus numériques et à l'atelier sur les paiements. L'exemple a été donné d'une affaire survenue aux États-Unis dans laquelle des jeux gratuits destinés aux enfants avaient permis l'achat de modules complémentaires, des « in-apps », à l'insu des parents en l'absence de mention claire des frais encourus pour ces compléments ; ces achats avaient conduit à une facturation de sommes importantes à l'égard des parents.

Blanchiment de capitaux et financement d'activités terroristes

En 2006, le Groupe d'action financière sur le blanchiment de capitaux (GAFI) s'est dit préoccupé par les risques de blanchiment d'argent et de financement d'activités terroristes associés aux nouvelles méthodes de règlement, dont les paiements en ligne et mobiles (GAFI, 2006). Le GAFI a formulé un certain nombre de recommandations pour prévenir ou réduire le plus possible les risques, appelant à un renforcement de la réglementation des systèmes de paiement sur Internet (GAFI, 2008). Selon lui, les systèmes de paiement en ligne, qui n'exigent aucune authentification physique, sont traités rapidement et

n'impliquent pratiquement pas d'intervention humaine, peuvent être facilement utilisés pour vendre ou acheter des produits illicites, comme de la drogue ou des contrefaçons. Le même problème a été soulevé au sujet des services mobiles prépayés qui ne demandent pas aux utilisateurs de s'enregistrer auprès d'un point de vente. Si l'on ajoute à cela que le rechargement des services prépayés se fait souvent à l'aide d'espèces ou de bons d'achat, il peut être difficile, voire impossible, de pister un paiement et donc d'identifier l'utilisateur d'un téléphone muni d'une carte prépayée. D'après une étude menée en 2005, neuf pays de l'OCDE sur les 24 considérés exigent des opérateurs de téléphonie mobile qu'ils enregistrent l'identité des clients de leurs services mobiles prépayés pour éviter l'anonymat. Ces pays sont l'Afrique du Sud, l'Allemagne, l'Australie, la France, la Hongrie, le Japon, la Norvège, la Slovaquie et la Suisse (Université Simon Fraser, 2006).

Agents de paiement extraterritoriaux

Au Japon, ces dernières années, les consommateurs ont déposé un nombre croissant de réclamations liées à l'intervention d'intermédiaires de paiement (parfois appelés « agents de paiement ») dans les transactions de paiement en ligne. Ces acteurs, qui peuvent agir au nom du commerçant dans la conclusion d'une opération de paiement avec une entité japonaise de carte de crédit, opèrent souvent de l'étranger. Les commerçants bénéficient du faible coût des services de ces agents et du fait qu'ils prennent en charge la gestion des informations clients. Toutefois, il arrive que des opérations de paiement en ligne soient conclues au nom de commerçants peu scrupuleux qui autrement n'auraient pas eu accès directement aux réseaux de cartes bancaires. Devant les difficultés rencontrées par les consommateurs pour contacter les agents de paiement basés à l'étranger et obtenir de leur part un remboursement en cas de problème lié au paiement, l'Agence des affaires de consommation envisage de créer un registre en ligne publiquement accessible contenant des informations sur les agents et sur les moyens pour les consommateurs de les contacter, de même que les autres parties à la transaction, en cas de problème.

Non-livraison, retard de livraison, non-conformité et défaut des produits

Aux yeux de la réglementation officielle comme à ceux des prestataires de paiement, les problèmes de non-livraison, de retard de livraison, de non-conformité ou de défaut des produits sont étroitement liés aux problèmes de paiement, en particulier pour ce qui est du règlement des litiges. Quand, par exemple, un commerçant et un acheteur ne réussissent pas à s'entendre sur un point particulier, l'organisme de paiement propose souvent un moyen de parvenir à un accord. À cet égard, les mécanismes de remboursement mentionnés plus haut jouent un rôle important dans la protection des consommateurs. Ainsi, en cas de problème de livraison, de non-conformité ou de défaut des produits, la procédure de remboursement mise au point par *Visa* offre un dispositif de règlement des litiges en vertu duquel l'émetteur d'une carte *Visa* (un établissement financier) peut transférer la responsabilité à l'acquéreur *Visa* (le commerçant). Lorsque le commerçant conteste la validité d'une demande de remboursement adressée par un consommateur, si la banque et le commerçant n'ont pas pu s'entendre, *Visa* peut être amené à statuer en dernier ressort sur le litige. En tant que tel, toutefois, le mécanisme de remboursement élaboré par *Visa* n'octroie aucun droit direct au titulaire de la carte ou au consommateur.

Les protections actuelles varient néanmoins fortement d'un pays à l'autre. Seuls quelques pays de l'OCDE (Corée, États-Unis, Finlande, Grèce, Japon, Norvège et Royaume-Uni), par exemple, ont adopté des dispositions juridiques ou réglementaires particulières protégeant les titulaires de cartes en cas de non-livraison des biens ou de non-exécution des services. Aux États-Unis, le titulaire de la carte de crédit peut différer le versement des montants contestés ou se voir provisoirement restituer les fonds prélevés tant que la procédure de règlement du litige n'a pas abouti (OCDE, 2005). Cette protection juridique est toutefois limitée aux cartes de crédit et ne s'applique pas aux cartes de débit en cas de non-livraison ou de non-conformité.

En Corée, les détenteurs de cartes de débit ou de crédit peuvent refuser le paiement si les marchandises ne sont pas livrées. Au Royaume-Uni, si la valeur de l'article est comprise entre 100 GBP et 30 000 GBP, le créancier et le fournisseur sont tous les deux tenus responsables en cas de rupture du contrat ou d'inexactitudes dans les informations fournies. Dans l'Union européenne, en vertu de la directive de la CE relative aux droits des consommateurs, lorsqu'un commerçant manque à ses obligations en matière de livraison, le consommateur est en droit de demander le remboursement des sommes déjà versées dans un délai de sept jours à compter de la date de livraison prévue.

Dans la plupart des pays, aucune mesure de protection spéciale n'est prévue en cas de non-livraison de contenus mobiles. Seuls quelques pays disposent d'une législation propre au commerce électronique couvrant le commerce mobile ; la *loi coréenne sur la protection du consommateur à l'égard du commerce électronique*, qui réglemente les cas de non-livraison ou de téléchargement incomplet des contenus mobiles, en est un exemple typique. Elle fait obligation à l'entreprise de livrer les produits dans un délai de trois jours ouvrables après réception du règlement, ou de rembourser le client dans le même délai (Consumer Focus, 2009).

S'agissant des produits non conformes, là encore, seul un petit nombre de pays (Corée, États-Unis, Finlande, Grèce, Japon, Norvège et Royaume-Uni) ont mis en place une législation particulière, afin de fournir aux consommateurs des mécanismes de réparation. De l'avis de certaines parties prenantes, les mécanismes existants de protection des consommateurs en cas de produits non conformes ne sont pas aussi développés et efficaces que ceux prévus pour les débits non autorisés.

À cet égard, des initiatives sectorielles ont contribué à résoudre les problèmes dans un certain nombre de pays. Au Japon, par exemple, la première plateforme de commerce en ligne, *Rakuten*, a instauré des services de paiement avec dépôt obligatoire sur un compte séquestre (*Rakuten Anshin Kessai Service*, service payant) pour toutes les transactions CCL, afin de résoudre les problèmes de non-livraison des marchandises. Le paiement n'est débloqué en faveur du vendeur qu'une fois que l'acheteur a effectivement reçu l'article commandé. *Yahoo! Japan* offre aussi ce type de service, sans aucun frais. En Chine, *Alipay* (le prestataire de services de paiement d'*Alibaba*) fonctionne de façon similaire grâce à un partenariat noué avec des banques. *PayPal* a mis en œuvre diverses solutions pour assurer une protection aux consommateurs en cas de non-livraison. La société peut geler le compte d'un vendeur qui n'a pas livré les articles achetés. Sa *Politique de protection des acheteurs* prévoit également que, si un client n'a pas reçu un article ou si l'article acheté diffère sensiblement de celui décrit, le client peut déposer une réclamation auprès de l'acheteur dans un délai de 45 jours à compter de la date de paiement, afin d'obtenir réparation. Des questions ont été soulevées, toutefois, quant à l'adéquation des périodes de notification et de traitement des réclamations.

En l'état actuel des réglementations, si la réclamation vise à obtenir le remboursement d'un bien ou d'un service incorporel défectueux (comme une sonnerie ou une application), les droits de recours et les droits à réparation octroyés aux consommateurs sont limités.

Règlement des litiges et réparation

Le problème ici a trait aux litiges qui naissent entre commerçants et clients au sujet de la réception, de la nature ou de la qualité du bien ou du service acheté lorsque les intermédiaires de paiement interviennent uniquement de manière indirecte. Dans cette situation, certains prestataires de paiement ont adopté des mesures visant à régler en ligne les litiges portant sur ces différents aspects. Certains pays imposent ce type de mesures à travers leur régime juridique, tandis que, dans d'autres, ces initiatives relèvent du secteur privé.

Comme nous l'avons vu précédemment, des dispositifs particuliers, fondés sur l'annulation du paiement et le remboursement du vendeur, peuvent offrir aux consommateurs une protection efficace en cas de problèmes liés à une opération de paiement. La protection peut prendre la forme de limitations de l'obligation de paiement, et permettre notamment aux consommateurs de faire corriger les erreurs de facturation ou d'obtenir réparation en cas de problème sur la livraison ou le produit acheté (OCDE, 2007*b*, annexe, section IV.2*c*). Cette protection peut être très étendue. À titre d'exemple, au Canada, certaines provinces ont introduit dans leurs lois de protection des consommateurs des dispositions qui imposent aux émetteurs de cartes de crédit de rembourser le montant objet du litige lorsqu'un contrat a été annulé en application d'une loi provinciale et que l'acheteur n'a pas été remboursé par le commerçant.

Hormis ces mécanismes d'annulation de paiement et de remboursement, d'autres systèmes ont été mis en place pour régler les litiges entre vendeurs et consommateurs. Un certain nombre d'options faisant intervenir des tierces parties sont possibles, que ce soit par les pouvoirs publics ou par le secteur privé. Elles font souvent appel à des organismes de paiement. Ces options revêtent une importance particulière dans le cas des paiements mobiles et en ligne, car le consommateur peut avoir des difficultés à contacter le vendeur directement, et la discussion en tête-à-tête est généralement impossible. Lorsque les consommateurs rencontrent des problèmes en rapport avec l'achat ou le paiement de biens ou de services, ils ont besoin de savoir à qui s'adresser pour trouver une solution au moindre coût. L'un des défis qui se posent est de concevoir des procédures viables pour les produits de faible valeur. Il faut également disposer de mécanismes permettant de traiter efficacement les opérations commerciales transnationales.

En 2001, la Commission européenne a mis en place FIN-NET, un réseau pour la résolution des litiges financiers composé des organismes de traitement extrajudiciaire des réclamations qui sont établis dans les pays de l'Espace économique européen (à savoir les États membres de l'Union européenne plus l'Islande, le Liechtenstein et la Norvège) et qui sont chargés de régler les litiges entre les consommateurs et les prestataires de services financiers, tels que les banques, les compagnies d'assurance, les sociétés d'investissement et autres. Les organismes coopèrent afin de faciliter l'accès des consommateurs aux procédures extrajudiciaires de réclamation dans les affaires transnationales. Si un consommateur a un litige avec un prestataire de services financiers d'un autre pays, les membres du réseau FIN-NET le mettront en contact avec l'organisme extrajudiciaire compétent et lui communiqueront les informations nécessaires sur celui-ci.

Les travaux de recherche montrent que les consommateurs sont mal informés sur les dispositifs en place pour le règlement des litiges, ainsi que sur le rôle potentiel des prestataires de paiement, en particulier dans le domaine des paiements mobiles. Selon une enquête menée en 2009, en cas de litiges portant sur une transaction mobile et notamment sur le paiement, 46 % des fournisseurs ne communiquaient pas au consommateur de renseignements adéquats sur la partie chargée de traiter les éventuelles réclamations, tandis que 71 % n'informaient pas le consommateur sur les procédures applicables de règlement des litiges (Consumer Focus, 2009, p. 8).

Le développement constant de l'utilisation d'Internet suscite un intérêt croissant pour la conception de mécanismes efficaces de résolution des litiges afférents aux achats en ligne. Les plus classiques, comme l'action en justice, peuvent prendre du temps et se révéler coûteux pour le consommateur, aussi les acteurs concernés s'intéressent-ils de plus en plus aux dispositifs en ligne. Définie comme « un moyen de règlement des différends par la conciliation ou l'arbitrage qui implique l'utilisation de technologies en ligne pour faciliter la résolution des litiges entre les parties », la médiation en ligne peut permettre des économies substantielles en regard de la procédure judiciaire classique.

Comme il a été conclu lors d'une conférence internationale organisée par la Commission des Nations Unies pour le droit commercial international (CNUDCI) les 29 et 30 mars 2010, dans un contexte transnational, la médiation en ligne adaptée aux transactions de faible montant peut se révéler la seule

option abordable pour les consommateurs (CNUDCI, 2010*a*). Tout en reconnaissant ses avantages, les associations de consommateurs relèvent certains problèmes posés par ces procédures : *i*) l'absence de contact personnel direct, qui risque de limiter la possibilité pour le consommateur d'expliquer son problème au commerçant ; *ii*) l'obligation pour le consommateur d'être suffisamment familiarisé avec des techniques web sophistiquées, ce qui peut constituer un obstacle pour certaines personnes. Les acteurs concernés estiment qu'il est indispensable de disposer de mécanismes de règlement des litiges et de réparation qui soient à la fois plus efficaces, moins onéreux, justes et pratiques, et susceptibles d'être mis en place à l'échelle mondiale. Partant de ces conclusions, en décembre 2010, la CNUDCI a entamé des travaux sur l'élaboration de normes juridiques sur le règlement des litiges en ligne dans les opérations internationales de commerce électronique (CNUDCI, 2010*b*). Un projet de règlement de procédure a été examiné lors des réunions du Groupe de travail III, qui se sont tenues en mai et novembre 2011 (CNUDCI, 2011).

Un certain nombre d'entreprises privées et de gouvernements ont mis au point des systèmes en ligne de réparation qui se sont montrés efficaces. Ainsi, PROFECO, au Mexique, exploite *ConciliaNet*, un dispositif de résolution en ligne des litiges. Selon PROFECO, le recours à ce dispositif a permis de réduire considérablement le temps nécessaire pour résoudre les litiges (de près de 50 %) et d'augmenter le nombre d'accords de règlement (jusqu'à 96 % des réclamations). Quelque 97 % des consommateurs interrogés par PROFECO ont déclaré qu'ils réutiliseraient ce mécanisme.

En 2009, *eBay* a annoncé la modification des mécanismes de résolution des litiges proposés aux consommateurs achetant des produits sur sa plateforme et se servant de *PayPal* pour payer. Alors qu'*eBay* dirigeait auparavant ses clients vers le centre de règlement des litiges de *PayPal*, les consommateurs peuvent dorénavant tenter de trouver une solution avec *eBay* directement, quelle que soit l'instrument employé pour payer la transaction contestée.

Information, autonomisation et éducation des consommateurs

D'autres mesures pourraient être nécessaires pour faire en sorte que les consommateurs reçoivent l'éducation qu'il leur faut sur les droits et obligations des consommateurs dans les paiements en ligne et mobiles, que celle-ci soit utile et bien comprise, et qu'elle soit suivie d'effets. Ce besoin a été noté dans les lignes directrices de 1999 (section VIII, partie II), dans un rapport de 2002 du CPC consacré à la protection des titulaires de cartes de crédit (OCDE, 2002), dans les orientations de l'OCDE sur le commerce mobile (OCDE, 2008*c*), dans les recommandations, toujours de l'OCDE, sur l'éducation des consommateurs (OCDE, 2009*b*, annexe II), et, plus récemment, à l'occasion de l'atelier sur les paiements (OCDE, 2011*c*).

Un rapport récent de l'Office of Fair Trading du Royaume-Uni soutient l'idée qu'il est essentiel d'informer les consommateurs sur les conditions dans lesquelles les transactions en ligne et mobiles peuvent être traitées, afin de leur permettre de choisir en toute connaissance de cause (voir OCDE, 1999, section III, C) (OFT, 2010*b*). Ce rapport souligne qu'il convient d'améliorer l'éducation dispensée aux consommateurs pour les aider à comprendre leurs droits en ligne. L'étude indique que 80 % des internautes savent qu'ils peuvent demander un remboursement à l'émetteur de leur carte de crédit si les biens ou services ne sont pas livrés ; trois quarts sont conscients qu'ils seraient en droit de retourner les marchandises dans un délai de sept jours contre un remboursement intégral, et deux tiers, qu'ils peuvent réclamer un remboursement au vendeur si les produits ne sont pas livrés à la date prévue ou dans un délai de 30 jours à compter de la date de la commande (OFT, 2010*b*, p. 11).

Lors de l'atelier sur les paiements, les participants ont également souligné la nécessité de renforcer l'information des consommateurs sur les éventuels fournisseurs douteux. Au Mexique, PROFECO a créé une base de données en ligne (disponible à l'adresse : http://burocomercial.profeco.gob.mx/BC/faces/inicio.jsp), qui contient des renseignements sur plus de

450 commerçants vendant des produits dans tout le pays et notamment sur les réclamations dont ils ont fait l'objet et les contrats léonins qu'ils ont pu offrir. Ces renseignements sont à la disposition des consommateurs et leur permettent de s'informer avant leurs achats.

En outre, les consommateurs ont souvent du mal à déterminer les protections dont ils bénéficient lorsqu'ils achètent des produits auprès de sociétés installées à l'étranger. Certains gouvernements ont alerté les consommateurs sur les différences dans les protections dont peuvent faire l'objet des achats en ligne, selon qu'ils sont effectués dans le pays ou à l'étranger. La Competition and Consumer Commission en Australie (ACCC) a par exemple averti les consommateurs australiens qu'en cas d'achat réalisé auprès d'un vendeur implanté à l'étranger, ceux-ci risquent de ne pas bénéficier des mêmes droits fondamentaux que ceux dont ils disposent lorsqu'ils achètent dans leur pays. Compte tenu des éventuelles difficultés pratiques pour obtenir réparation de la part d'un vendeur basé hors du pays, l'organisme conseille aux consommateurs de vérifier les conditions générales du contrat proposé avant d'effectuer un achat en ligne (ACCC, 2010).

Lorsque des problèmes surviennent, il est possible de faire part de son expérience en déposant une réclamation sur *econsumer.gov*, un site web public multilingue créé à l'initiative du Réseau International de Contrôle et de Protection des Consommateurs (RICPC).

III. Problèmes techniques liés aux paiements

Sécurité

On observe que le manque de confiance des consommateurs à l'égard de la sécurité des paiements en ligne et mobiles reste l'un des facteurs les plus importants affectant le développement du commerce électronique. La plupart des études montrent que ce manque de confiance est lié à des inquiétudes sur la sécurité des données de paiement ou sur une éventuelle utilisation illicite de ces dernières. Une enquête réalisée aux États-Unis, au Japon et au Royaume-Uni montre que 86 % des détenteurs de téléphones portables sont préoccupés par les risques pour la sécurité liés à leurs appareils, tandis que 55 % des personnes interrogées disent avoir des inquiétudes sur la sécurité des paiements mobiles (McAfee, 2008). Toutefois, certaines parties prenantes estiment que cette méfiance excessive pourrait être due davantage à une surestimation des risques de sécurité des paiements en ligne et mobiles. Dans l'Union européenne, on considère que cette méfiance des consommateurs est liée à leur perception erronée de l'ampleur du risque associé au vol d'informations de paiement, alors que l'incidence réelle de ce problème est assez faible ; en 2010, seuls 1 % des consommateurs de l'UE qui ont effectué des achats en ligne ont été victimes de tels agissements (CE, 2011).

En outre, on constate que les consommateurs ne savent pas bien qui est tenu d'assurer la sécurité des systèmes de paiement. En Australie, selon l'ACMA, les consommateurs s'attendent à ce que ce soient les prestataires des nouveaux services de paiement mobiles qui soient chargés de les protéger des menaces liées à la sécurité (Noone, 2011). Par ailleurs, les consommateurs ne sont pas conscients qu'une participation active de leur part à la sécurisation des paiements mobiles est également nécessaire (en adoptant, par exemple, un comportement responsable).

Les parties prenantes reconnaissent généralement que les menaces liées à la sécurité sont plus délicates à contrer sur les appareils mobiles, plus facilement perdus ou volés, que sur les ordinateurs personnels. Les pirates informatiques peuvent également mettre la main sur des données par divers moyens, tels que le Bluetooth ou la RFID, ou en infectant les appareils lors du téléchargement d'applications. Les orientations élaborées par l'OCDE en 2008 abordent cette question, en encourageant les intervenants du commerce mobile à (OCDE, 2008*c*) :

faire en sorte que les consommateurs soient informés des problèmes possibles d'atteinte à la sécurité et à la vie privée auxquels les expose le commerce mobile, et des mesures à leur disposition pour limiter les risques ;

encourager l'élaboration de mesures de sécurité et de fonctions de sécurité intégrées ;

encourager les opérateurs de téléphonie mobile à mettre en place des politiques et mesures de sécurisation afin de prévenir les transactions non autorisées et les atteintes à la sécurité des données.

De nombreuses parties prenantes estiment qu'on peut adopter plusieurs approches pour améliorer la sécurité des consommateurs en matière de paiements en ligne et mobiles. Comme les experts l'ont indiqué lors de l'atelier OCDE intitulé *Le rôle des intermédiaires Internet face aux objectifs de l'action publique*, organisé le 16 juin 2010 (OCDE, 2011*b*), ces approches comprennent des mécanismes législatifs et non législatifs. Ainsi, un certain nombre de normes techniques, de codes de bonne conduite et de règles de bonne pratique ont été mises en place par le secteur. Plusieurs réseaux de cartes de paiement (dont *Visa*, *MasterCard* et *American Express*) ont élaboré un ensemble harmonisé de normes de sécurité (intitulé PCI DSS, pour « Payment Card Industry Data Security Standards ») ; ces normes énoncent douze conditions requises pour assurer une sécurité adéquate. Dans les deux contextes, il est essentiel que toutes les parties en jeu (notamment les commerçants et les organismes de paiement) s'engagent à atteindre l'objectif (CE, 2008b, p. 5). La mise en application du cadre de sécurité évoqué ci-dessus a toutefois été délicate. Les résultats d'une enquête font apparaître que seulement un tiers environ (39 %) des détaillants en ligne comprennent réellement ce que recouvre la conformité aux normes PCI DSS, alors que 65 % considèrent que les fraudes dans les paiements liées à leur site ne sont pas de leur ressort.

L'une des principales approches élaborées ces dernières années en faveur de la sécurité concerne la gestion de l'identité numérique (GIN), laquelle se définit comme un ensemble de règles, procédures et éléments techniques requis pour mettre en œuvre la politique d'une organisation en ce qui concerne la création, l'utilisation et l'échange d'informations d'identité numérique (OCDE, 2008*d*). Dans le secteur commercial, elle a été reconnue comme étant peut-être l'outil le plus efficace pour renforcer la sécurité dans le domaine des paiements électroniques, où un certain nombre d'acteurs interviennent et s'échangent les données financières des consommateurs (OCDE, 2008*d*, p. 10). Parmi les différents processus de GIN, l'authentification et la vérification de l'âge (voir ci-dessous) sont considérées comme des outils complémentaires pour lutter contre les menaces liées à la sécurité et instaurer la confiance dans l'économie Internet. En 1998, à l'occasion de la conférence ministérielle d'Ottawa sur le thème *Un monde sans frontières : concrétiser le potentiel du commerce électronique mondial*, les ministres ont reconnu l'importance de l'authentification comme outil contribuant de manière précieuse au développement du commerce électronique (OCDE, 1998). L'OCDE, par l'entremise de son Groupe de travail sur la sécurité de l'information et la vie privée (GTSIP), a mis sur pied un certain nombre de projets visant à renforcer la sécurité dans l'économie Internet, au nombre desquels figurent les travaux suivants :

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : cadre favorisant des approches nationales cohérentes en matière de gestion des risques liés à la sécurité (OCDE, 2002).

Recommandation de l'OCDE sur l'authentification électronique et Orientations pour l'authentification électronique : *i*) les orientations définissent des principes destinés à aider les pays de l'OCDE à établir ou à moderniser leurs approches de l'authentification électronique ; *ii*) la recommandation encourage les pays Membres à poursuivre leurs efforts pour établir des approches qui soient compatibles et technologiquement neutres pour une authentification électronique efficace des personnes et des entités au niveau national et transfrontalier (OCDE, 2007*a*).

Gestion de l'identité numérique : en s'appuyant sur les travaux réalisés dans le domaine de l'authentification électronique et sur la déclaration ministérielle de Séoul de 2008, le GTSIP a établi un rapport qui explique la raison pour laquelle la gestion de l'identité numérique est fondamentale pour la poursuite du développement de l'économie Internet et qui souligne la nécessité de prendre en compte les limitations que présentent les approches actuelles du fait de la complexité de la gestion des éléments d'identité et de la robustesse requise pour des services à forte valeur. Le rapport propose à l'intention des responsables gouvernementaux des orientations pour la mise en place de conditions cadres efficaces en faveur de l'innovation dans l'ensemble des secteurs public et privé, tout en renforçant la sécurité, la vie privée et la confiance dans l'économie Internet (OCDE, 2011*d*).

Protection des enfants en ligne : en 2011, le GTSIP a publié un rapport sur les diverses menaces auxquelles sont exposés les enfants dans l'environnement numérique, y compris en matière de sécurité (OCDE, 2011*a*). Les conclusions de ce rapport servent de base à une recommandation du Conseil en cours d'élaboration dans ce domaine.

Authentification et outils de détection des fraudes

L'authentification est un processus permettant à un prestataire de services de paiement ou un détaillant, ou les deux, de vérifier l'identité d'un acheteur potentiel avant de traiter un règlement. Cette vérification peut augmenter la confiance des consommateurs à l'égard de l'opération de paiement et réduire les cas de fraude.

Plusieurs initiatives ont été prises par les autorités de réglementation et par le secteur pour améliorer le processus d'authentification dans les paiements, parfois en partenariat avec les pouvoirs publics. Au Mexique, la Commission nationale des banques et des valeurs mobilières a créé une unité spéciale qui supervise et contrôle le niveau de sécurité des systèmes de paiement électronique, y compris pour les règlements effectués sur le point de vente. Les banques ont par exemple mis en place le protocole sécurisé de paiement sur Internet « 3-D Secure », dont l'objet est d'authentifier les acheteurs en temps réel pour faire en sorte que les cartes de paiement ne puissent être utilisées que par les personnes autorisées. Selon ce protocole, la responsabilité de l'authentification de l'acheteur et du traitement de toute réclamation pour un achat non autorisé par ce dernier est assumée par l'institution financière qui a émis la carte, et non par le commerçant (ce qui était généralement le cas auparavant).

Par ailleurs, des cartes EMV, dotées à la fois d'une puce et d'un code confidentiel, ont été introduites dans la plupart des pays. La norme EMV Contactless Communication Protocol Specification a été élaborée par *EMVCo*, une co-entreprise créée par les grands réseaux de paiement, *American Express*, *JCB*, *MasterCard* et *Visa*. Elle définit des spécifications pour la fabrication d'instruments de paiement sans contact destinés à remplacer les pistes magnétiques sur les cartes de crédit et de débit, ainsi que les téléphones portables. Paradoxalement, on s'attend à ce que ces cartes plus sécurisées incitent les fraudeurs à reporter leur attention sur les transactions de type « carte non présente », ce qui pourrait se traduire par une augmentation de la fraude en ligne (voir CE, 2008*b* et Innopay, 2010).

En novembre 2010, *American Express* a lancé *SafeKey*, un outil de prévention des fraudes qui fait appel au protocole 3-D Secure de *Visa*. Dans certains pays, comme le Royaume-Uni et la France, des banques proposent aux consommateurs des contrôles renforcés pour les transactions d'un montant élevé. À cet effet, elles fournissent à leurs clients un numéro fictif de carte de crédit, à usage unique, garantissant ainsi que le commerçant n'a pas accès au numéro « permanent » de la carte de crédit du consommateur (voir Encadré 3). Dans l'Union européenne, en 2009, quelque 300 000 détaillants représentant près de 37 % du volume des transactions de commerce électronique ont fourni ce service à plus de 50 millions de titulaires de carte (Visa Europe, 2009, p. 30).

Encadré 3. Exemple d'authentification électronique : l'e-Carte Bleue française

***e-Carte Bleue Visa* française** (lancée en 2002) : au moyen d'une application téléchargeable, l'*e-Carte Bleue* permet à un consommateur, chaque fois qu'il souhaite effectuer un achat en ligne, de générer un numéro fictif de carte de crédit, à usage unique, associé au numéro réel de sa carte de crédit. Le numéro virtuel constitue la seule et unique information financière communiquée au commerçant. En juillet 2010, *Visa* a lancé une nouvelle carte nommée *Visa CodeSure* : d'un format identique aux cartes de crédit classiques, elle comprend un écran à cristaux liquides et un petit pavé numérique alimentés par une pile. Lors d'un achat en ligne ou d'une connexion à un service bancaire en ligne, le titulaire de la carte doit : *i*) appuyer sur le bouton *Verified by Visa* du clavier de la carte ; *ii*) saisir un code confidentiel à l'aide de ce même clavier. Un code à usage unique permettant au titulaire de la carte de s'authentifier en ligne apparaît alors sur l'écran de cette dernière.

En outre, afin de prévenir et de limiter les atteintes à la sécurité et les pertes, le secteur a mis en place plusieurs mesures techniques destinées à renforcer la confiance, parmi lesquelles des puces inviolables sur les cartes de paiement et l'utilisation de techniques de cryptage perfectionnées ; le plafonnement des montants stockables sur les appareils électroniques des consommateurs ; la limitation de la valeur des transactions et l'utilisation d'un code confidentiel pour autoriser les paiements.

En outre, dans le cadre du processus d'authentification, les détaillants et les banques utilisent de plus en plus souvent des outils améliorés de détection des fraudes, qui renforcent la sécurité des cartes lors des achats en ligne. Il peut s'agir d'outils manuels ou automatiques. En 2009, quelque 97 % des commerçants en ligne aux États-Unis et au Canada utilisaient au moins un outil de vérification automatique (généralement mis à disposition par les réseaux de cartes de paiement) permettant d'authentifier les cartes et leurs titulaires. En outre, des systèmes automatiques de filtrage sont couramment utilisés pour analyser en temps réel les commandes entrantes. Si une commande dépasse un certain montant, par exemple, ou si les adresses d'expédition et de facturation ne correspondent pas, la commande est signalée comme potentiellement frauduleuse et placée dans une file d'attente du système de gestion du commerçant en vue d'un examen complémentaire. En outre, à l'issue de la phase de contrôle automatique, la plupart des commerçants effectuent des vérifications manuelles de certaines commandes. Un quart environ des commandes passées en ligne aux États-Unis et au Canada ayant fait l'objet d'un examen manuel dans le cadre de la prévention de la fraude, ces procédures peuvent coûter relativement cher aux commerçants (OCDE, 2011*b*).

S'agissant de l'authentification lors des paiements mobiles, la question de savoir si un numéro de téléphone portable devrait être utilisé pour identifier payeur et bénéficiaire ne fait pas l'unanimité. Un grand volume de transactions repose sur des SMS, qui nécessitent uniquement un accès par code PIN.

Vérification de l'âge

Les enfants achètent beaucoup de produits en ligne et au moyen de leurs appareils mobiles, sans toujours être conscients des risques qu'ils courent. Ces achats ont lieu en dépit du fait que, dans la plupart des pays, les mineurs ne sont pas autorisés légalement à conclure des transactions commerciales. L'un des moyens de les protéger est de veiller à ce que leur âge et leur identité soient vérifiés en ligne avant tout achat. Les travaux de recherche montrent que les contrôles sont rares, et l'un des rapports souligne que 76 % des achats réalisés à l'aide d'appareils mobiles ne passent pas par une étape obligatoire de vérification de l'âge (Consumer Focus, 2009, p. 47). Même lorsqu'une procédure de ce type est prévue, il est relativement facile pour les enfants de se présenter comme des adultes lorsqu'ils sont en ligne, contrairement à ce qui se passe dans le cas d'une transaction en personne dans un magasin. Les orientations pour les politiques publiées en 2008 par l'OCDE mettent en évidence la nécessité d'instaurer des systèmes efficaces de vérification de l'âge (OCDE, 2008*c*). Toutefois, il convient de noter que de tels outils ne peuvent pas être utilisés comme seul et unique moyen de protection des enfants dans le contexte des paiements en ligne et mobiles. Lors de la conférence sur le commerce électronique organisée en 2009 par l'OCDE, les participants ont reconnu que les parents, les commerçants en ligne, les prestataires de

services mobiles et les organismes de paiement se partageaient la responsabilité de sensibiliser les enfants aux risques que présentent les achats en ligne et mobiles, et aux moyens de se protéger contre ces menaces.

Connaissances et compétences des consommateurs

Du fait de l'évolution rapide des technologies, les consommateurs peuvent ne pas être en mesure d'évaluer les risques et ne pas savoir comment se prémunir contre les fraudes ni comment préserver leur sécurité en ligne. L'éducation et la sensibilisation peuvent contribuer à y remédier. Ces besoins ont été rappelés à plusieurs reprises, dans les lignes directrices de 1999 (section VIII, partie II), dans les orientations de l'OCDE sur le vol d'identité en ligne (OCDE, 2008*b*) et le commerce mobile (OCDE, 2008*c*), ainsi que dans les recommandations, toujours de l'OCDE, sur l'éducation des consommateurs (OCDE, 2009*b*, annexe II).

Dans son rapport de 2002, le CPC a souligné la nécessité de mieux éduquer les consommateurs sur les questions, en particulier, de l'utilisation et de la sécurité des cartes de crédit et de débit en ligne (OCDE, 2002). Selon un rapport de la Commission européenne (CE, 2008*b*, p. 27), il ne faut pas surestimer la capacité des consommateurs à se préserver contre la fraude liée aux paiements et contre les problèmes de sécurité qui y sont associés. Souvent, surtout s'il s'agit d'enfants et autres personnes vulnérables ou désavantagées, ils ne savent pas comment se protéger en ligne, en dépit des nombreuses campagnes d'éducation et de sensibilisation menées à leur intention. L'effort de pédagogie doit être accentué : il faut s'assurer que le message passe véritablement auprès des consommateurs et qu'il est suivi d'effets. Le Plan d'action de l'UE (2004-2007) pour la prévention de la fraude sur les moyens de paiement autres que les espèces recommande à cet égard que les citoyens disposent d'une information plus abondante et plus claire sur la sécurité des paiements et que les commerçants puissent bénéficier d'un meilleur matériel pédagogique et d'outils adéquats pour se protéger du piratage de données (CE, 2007*b*). Les travaux de recherche laissent penser qu'il faudrait que les consommateurs soient beaucoup mieux informés des risques de sécurité associés aux paiements mobiles (Consumer Focus, 2009, p. 9). Il existe toutefois des limites à l'efficacité des initiatives de sensibilisation et d'éducation. Les consommateurs ignorent souvent comment se protéger en ligne, malgré les multiples campagnes d'éducation et de sensibilisation (OCDE, 2010*a*, p.24).

Interopérabilité, choix du mode de paiement et commerce électronique transnational

L'utilisation par les consommateurs des systèmes de paiement en ligne varie selon les pays et les régions. En Europe occidentale, une grande majorité de consommateurs règlent leurs achats en ligne par carte de crédit ou de débit. En Allemagne, le prélèvement est le principal moyen de paiement. Selon un rapport établi en 2010, tandis qu'aux Pays-Bas, le système *iDEAL*, qui permet de payer par l'entremise d'une banque en ligne, est prédominant, les Danois règlent plutôt par carte de débit et les Français par carte de crédit ; quant aux Européens de l'Est ils ont principalement recours à la livraison contre remboursement (Innopay, 2010). Les différences de modes de paiement entre les pays ont été mises en évidence comme l'un des facteurs ralentissant le développement du commerce électronique transnational. S'agissant des paiements mobiles en Europe, le Conseil européen des paiements (EPC) a présenté le manque de normes ouvertes d'interopérabilité entre les émetteurs de cartes et les opérateurs de réseau mobile comme un obstacle majeur au succès des déploiements commerciaux (EPC, 2010*a*, p. 52). Pour remédier à ce problème, l'EPC travaille en collaboration avec la GSMA à l'harmonisation des normes de paiement dans la région.

Une interopérabilité renforcée des mécanismes, technologies et systèmes de paiement est considérée comme essentielle pour faciliter le commerce électronique transnational. Selon une enquête réalisée en 2010, des commerçants en ligne britanniques souhaitant vendre des produits à l'étranger n'y parvenaient pas en raison de la multitude de systèmes de paiement utilisés dans les différents pays de l'UE.

Il leur aurait en effet fallu accepter un grand nombre de modes de paiement : ceux de *Visa Inc*. et de *MasterCard Worldwide*, la carte de débit *Maestro* de *MasterCard*, la carte *American Express Co*., le système de prélèvement et les systèmes *ELV* en Allemagne et *iDeal* aux Pays-Bas (The Internet Retailer, 2010*d*). En conséquence, les choix des consommateurs en ligne sont continuellement entravés par la limitation des moyens de paiements acceptés par les commerçants. La plupart des commerçants qui vendent dans d'autres pays exigent que le paiement soit effectué au moyen de cartes de crédit et de débit internationalement acceptées.

Le secteur a lancé une autre initiative pour favoriser l'interopérabilité des systèmes de paiement bancaire en ligne des différents pays : *OBeP* (Online Banking Enabled e-Payments, paiements électroniques par l'entremise d'une banque en ligne). Avec ce système, le consommateur souhaitant acheter un bien ou un service n'a pas à fournir d'informations financières au commerçant en ligne. Au moment du paiement, il est redirigé vers le site de sa banque, où les détails de la transaction lui sont présentés. Il peut alors confirmer à sa banque l'instruction de paiement du commerçant en question. Des travaux sont en cours pour élargir le champ d'application du système OBeP par l'élaboration de normes mondiales. Un conseil international des opérateurs de réseau de paiement, l'ICPNO (International Council of Payment Network Operators), a été créé dans le but d'élaborer le cadre et d'établir les règles et normes à respecter pour rejoindre les réseaux OBeP mondiaux. Des questions clés doivent y être examinées, comme les technologies, les systèmes de règlement internationaux, la conformité juridique, la sécurité, les communications, les structures tarifaires et les mécanismes de taux de change.

En outre, des partenariats ont été noués entre entreprises de différents pays afin de stimuler le développement du commerce électronique transnational. Une alliance a ainsi été conclue le 1er juin 2010 entre *Taobao* et *Yahoo! Japan* pour faciliter les achats transfrontaliers des consommateurs japonais et chinois (voir encadré 4).

Encadré 4. Alliance entre *Yahoo! Japan Corp.* et *Taobao* (Chine) dans le domaine du commerce électronique transfrontalier

Le 1er juin 2010, *Yahoo! Japan Corp*. et *Taobao* en Chine ont lancé des services d'achat en ligne complémentaires, qui permettent aux consommateurs japonais d'acquérir des produits auprès de commerçants chinois, et vice-versa. Dans ce système commun, qui vise à éliminer les obstacles au commerce électronique transfrontières, comme la langue, la complexité de la réglementation, les services logistiques de livraison et les questions liées au paiement :

- les consommateurs japonais peuvent acheter des produits auprès de commerçants *Taobao* en Chine par l'entremise du nouveau site *Yahoo! Japan China Mall* (http://chinamall.yahoo.co.jp) créé par Yahoo! Japan, et
- les consommateurs chinois peuvent effectuer des achats à partir de *Yahoo! Japan* sur le nouveau site web *TaoJapan* (http://taojapan.com) créé par *Taobao*.

Un partenariat similaire a été lancé en 2008 entre *Alipay* (prestataire de services de paiement détenu par la plus importante plateforme de commerce électronique chinoise, *Alibaba*) et *Paymate* (prestataire de services de paiement australien). Par ailleurs, en juillet 2010, un protocole d'accord a été signé entre plusieurs sociétés coréennes et japonaises afin de permettre aux consommateurs d'acheter des produits auprès de commerçants des deux pays. Ce protocole prévoit que les consommateurs pourront télécharger une application de paiement mobile sur leur téléphone intelligent, laquelle sera dotée de la technologie NFC.

IMPLICATIONS POUR LA POLITIQUE À L'ÉGARD DES CONSOMMATEURS

Les problèmes rencontrés par les consommateurs et traités ici ont des implications dans un certain nombre de domaines de l'action gouvernementale. Celles-ci ont été débattues pare le Comité avec le secteur privé et la société civile au fur et à mesure de l'avancement des travaux, notamment lors d'un atelier tenu en avril 2011. Ces questions sont exposées ci-après. L'analyse servira de base à l'élaboration d'orientations à l'intention des pouvoirs publics dans le domaine des paiements en ligne et paiements mobiles.

Clarté, transparence et exhaustivité des informations communiquées

Il peut ne pas toujours être aisé pour les consommateurs de consulter, lire, mémoriser et préserver les modalités et conditions des transactions et les détails correspondants des paiements et procédures.

Les transactions en ligne et sur mobile distant se font souvent en situation de mobilité, laquelle peut influer sur la prise de décision du consommateur. De ce fait, celui-ci peut ne pas toujours aisément consulter, lire, revoir ou conserver les détails de la transaction avant d'effectuer le paiement. De plus, les modalités et conditions des contrats en ligne sont souvent affichées en petits caractères ou dans une fenêtre défilante. Des informations clés sur le paiement sont parfois enfouies dans des notes de base de page ou nécessitent d'ouvrir des fenêtres supplémentaires. Les problèmes d'information peuvent être exacerbés dans l'environnement des paiements mobiles par la petite taille des écrans des terminaux mobiles, leur faible puissance de traitement et leur autonomie limitée. On notera toutefois que la situation pourrait évoluer avec l'usage croissant parmi les consommateurs de terminaux mobiles comme les *smartphones* et les tablettes informatiques, qui ont de plus grands écrans, davantage de mémoire et des fonctions plus performantes.

Les informations essentielles sur les droits et les éventuelles responsabilités des consommateurs dans le cadre des paiements en ligne et sur mobile ne leur sont pas toujours communiquées au moment voulu et de manière claire et transparente.

La section III des lignes directrices de 1999, qui concerne l'information donnée dans le commerce en ligne, énumère les éléments d'information clés qui devraient être communiqués aux consommateurs lors de la vente. Beaucoup de ces informations se rapportent de près ou de loin au paiement. En pratique, les informations sont souvent présentées dans un langage technique et verbeux qui les rend difficiles à utiliser ou à comprendre pour les consommateurs. Il arrive aussi que l'information ne soit communiquée que dans les dernières étapes du paiement. Par ailleurs, il n'est pas toujours évident de déterminer laquelle des parties à la transaction de paiement est tenue de fournir des informations aux consommateurs, quels éléments doivent figurer, et à quel moment du processus de paiement ces informations doivent être fournies.

Lors de l'atelier sur le paiement, les parties prenantes ont évoqué différentes solutions susceptibles d'améliorer l'information et d'autres aspects des systèmes de paiement. Un certain nombre de participants ont préconisé une meilleure information du consommateur sur les clauses de retrait ou d'annulation des achats. D'autres ont indiqué que le consommateur devrait être informé avant qu'il n'effectue le paiement des délais de livraison, de leurs éventuels droits en matière de retrait ainsi que des mécanismes de règlement des litiges et des voies de recours dont il dispose (notamment les programmes en ligne et alternatifs de règlement des litiges). En cas d'incident lié à une transaction, le consommateur devrait aussi disposer d'informations claires sur les personnes à contacter et de moyens pour les joindre, par exemple un numéro d'appel gratuit ou un lien vers un site web accessible depuis la plate-forme de commerce électronique du site marchand. Il a également été noté qu'il faudrait mieux informer les

souscripteurs d'abonnements en ligne, pas toujours suffisamment conscients de ce que les tarifs avantageux pratiqués au début ne sont parfois valables que pendant une durée limitée. Par ailleurs il serait utile de mieux renseigner le consommateur sur les « add-ons », ces extensions proposées avec certains produits, qu'ils peuvent parfois acheter sans le savoir, et de faire figurer plus clairement le prix de ces extensions.

Variabilité des régimes réglementaires er de protection

Les consommateurs qui achètent en ligne ou sur mobile ne comprennent pas toujours parfaitement quelles réglementations s'appliquent à une opération de paiement et la façon dont celles-ci peuvent différer selon la méthode de paiement et la plate-forme utilisées, les parties intervenant dans la transaction de paiement et la nature du produit acheté.

Cette méconnaissance s'explique par le fait qu'une transaction de paiement donnée peut associer une multitude d'intervenants financiers et non financiers, comme les banques et les réseaux de cartes bancaires, les systèmes de paiement « alternatifs » proposés par exemple par les opérateurs de réseaux mobiles et d'autres acteurs de paiement non bancaires qui opèrent sur l'Internet. Les opérations sont souvent encadrées par plusieurs organes de régulation, eux-mêmes soumis à des réglementations différentes. Il peut donc être difficile pour le consommateur de déterminer : *i)* quelles sont les voies de recours à sa disposition (pour la rectification de la commande, le retour, l'échange ou le remboursement de produits) ; *ii)* à quelle entité s'adresser en cas de problème lié au paiement ; *iii)* vers quel organisme de régulation se tourner si son problème ne peut être résolu directement avec le site marchand. La situation devient encore plus complexe avec les transactions transnationales.

Les participants semblent s'accorder à penser que cette situation pourrait être améliorée par un effort d'information et de pédagogie en direction des consommateurs sur leurs droits et leurs responsabilités et sur les règles applicables. Certains intervenants, toutefois, jugeraient souhaitable de prendre des mesures supplémentaires pour rationnaliser et simplifier l'environnement réglementaire. Cela a d'ailleurs été réalisé dans certains pays, où les règles génériques de protection des consommateurs sont appliquées parallèlement à des initiatives d'autorégulation et de co-régulation.

Aux yeux de certains, des problèmes spécifiques se posent pour le commerce mobile. Ce type de transaction n'en est qu'à ses balbutiements dans de nombreux pays et les prestataires de services de paiement mettent en garde contre une adoption prématurée de nouvelles réglementations qui pourraient avoir des effets secondaires négatifs sur le développement du mobile. Les responsables des politiques publiques doivent se garder de toute initiative qui pourrait risquer de ralentir l'innovation ou d'entraver la concurrence. Ils doivent aussi veiller à ce que les conditions de concurrence soient équitables pour tous les prestataires de services de paiement.

Le commerce en ligne et mobile n'offre pas aux consommateurs le même niveau de protection selon le mécanisme de paiement utilisé au sein d'un même pays, ce qui peut compliquer les recours en cas de problème. De plus, les régimes de protection varient d'un pays à l'autre, ce qui risque de détourner les consommateurs des transactions transnationales.

Le régime de protection des paiements diffère entre pays et au sein des pays, selon : *i)* la méthode de paiement utilisée (carte de crédit ou de paiement, carte prépayée, paiement via la facture de l'opérateur mobile) ; *ii)* la nature du problème (prélèvement non autorisé, fraude, non-livraison ou non-conformité des produits) ; *iii)* la nature du produit acheté (le traitement peut différer selon qu'il s'agisse de biens ou de services, de biens matériels ou incorporels) ; *iv)* le prestataire de service de paiement (les prestataires « alternatifs » tels que les opérateurs de réseaux mobiles et les autres établissements non financiers

échappent parfois à l'application de certains régimes réglementaires du fait de leur statut non bancaire dans certains territoires de compétence).

Il ressort des échanges entre les parties prenantes qu'il faudrait au minimum faire en sorte que les consommateurs soient mieux informés du niveau de protection dont ils bénéficient en fonction du moyen de paiement qu'ils utilisent. A cet égard, il serait utile d'accentuer les efforts de pédagogie et de sensibilisation. Au-delà, certaines parties prenantes sont favorables à ce que soit fixé un niveau minimum de protection du consommateur qui s'appliquerait quel que soit le mécanisme de paiement utilisé au sein d'un même territoire de compétence. Ce niveau minimum de protection pourrait être garanti par la loi ou par la réglementation, ou par un moyen moins formel. L'établissement d'un niveau minimum de protection ne saurait toutefois empêcher les prestataires de services de paiement d'offrir des protections plus importantes ; cette marge de manœuvre est, aux yeux de certains, essentielle pour préserver la concurrence et offrir un choix aux consommateurs. Pour ce qui est des opérations transnationales, améliorer la situation semble une ambition plus complexe ; une convergence des systèmes serait souhaitable, mais difficile à obtenir concrètement.

Pratiques commerciales frauduleuses, trompeuses ou mensongères

Les pratiques commerciales frauduleuses, trompeuses ou mensongères associées aux paiements en ligne et mobiles sont un problème qui perdure et qui peut porter préjudice aux consommateurs et de façon plus générale saper leur confiance, au sein d'un pays ou à l'international

Les transactions en ligne et mobiles diffèrent parfois des achats pratiqués auprès des magasins traditionnels, et ce pour différentes raisons : *i)* les consommateurs ne peuvent souvent pas vérifier l'identité et l'intégrité des commerçants ; *ii)* les consommateurs ne peuvent généralement pas examiner le produit avant l'acte d'achat ; *iii)* une transaction en ligne ou mobile peut se conclure en quelques secondes, et le consommateur n'est pas toujours en mesure de comprendre les conditions générales de vente ou de bien réfléchir avant de consentir à l'achat. Parfois, la possibilité et la probabilité de pratiques frauduleuses, trompeuses et mensongères semblent, a priori, beaucoup plus élevées dans le commerce en ligne et mobile, en particulier lorsque le commerçant est éloigné et n'a pas d'antécédents connus. On notera toutefois que ces problèmes ne se posent pas forcément pour tous les paiements mobiles, dans la mesure ou des terminaux équipés d'une technologie de paiement sans contact (NFC) sont également utilisés pour régler des achats effectués auprès de commerçants traditionnels.

Quel que soit le contexte dans lequel s'effectue le paiement, les participants s'accordent généralement à considérer que la responsabilité de la protection contre la fraude doit être partagée entre les prestataires de services de paiement et les sites marchands. Ces derniers doivent en particulier s'assurer que leur système de commerce électronique est approprié, transparent et sûr. Certaines parties prenantes ont suggéré la mise en place d'outils destinés à renforcer les protections offertes, comme l'utilisation de comptes séquestre permettant de ne procéder au paiement que si le consommateur reçoit les biens commandés. De plus, l'existence de moyens effectifs de règlement des litiges et une lutte déterminée et énergique contre les commerçants indélicats contribueraient à raffermir sensiblement la confiance des consommateurs. Certains pays ont déjà pris des mesures en ce sens, avec par exemple des réglementations qui limitent la responsabilité du consommateur en cas de fraude.

Règlement des litiges et voies de recours

Du fait de la multiplicité des parties pouvant intervenir dans une transaction de paiement, le consommateur peut avoir des difficultés à comprendre vers qui se tourner en cas de problèmes.

Des participants ont fait valoir que les prestataires de services de paiement, les commerçants et les autres parties intervenant dans une transaction pourraient avoir avantage à œuvrer ensemble pour faire en sorte que les consommateurs disposent d'une information claire et complète sur l'entité à contacter en cas de problème avec une transaction de paiement et sur celle à contacter en cas de problème avec un produit ou service acheté ou utilisé en ligne.

Les discussions entre parties prenantes donnent à penser que les prestataires de services de paiement pourraient œuvrer avec les commerçants et autres intervenants pour mettre en place des mécanismes efficaces de règlement des litiges et de recours.

Autres questions

De nombreux consommateurs hésitent à pratiquer le commerce électronique en recourant aux dispositifs de paiement en ligne et mobiles car ils doutent de la sécurité qu'offrent ces systèmes.

Qu'elles soient ou non justifiées, les réticences du public quant à la sécurité des paiements ont toutes les chances de limiter l'activité des consommateurs en ligne et sur mobile. Une meilleure connaissance des mesures prises par les professionnels pour assurer la sécurité permettrait de dissiper certaines idées fausses chez les consommateurs ; un effort de pédagogie serait également bienvenu pour apprendre aux consommateurs les précautions à prendre pour éviter de compromettre leurs informations financières et personnelles. Certaines parties prenantes notent que des initiatives de formation seraient aussi utiles en direction des commerçants, pour qu'ils soient mieux armés face aux menaces émergentes contre la sécurité. L'effort de lutte par des moyens technologiques se poursuit résolument. Il y a par exemple les clés de sécurité qui génèrent un code numérique aléatoire qui est envoyé à l'utilisateur par SMS, ou les jetons permettant de se connecter à l'aide d'un identifiant et d'un mot de passe, ou encore les applications d'identification et d'authentification à télécharger qui permettent de vérifier l'authenticité d'un courriel reçu d'un prestataire de services de paiement.

Les parties prenantes s'inquiètent des risques que peuvent représenter les systèmes de paiement Internet et mobiles pour les consommateurs vulnérables et défavorisés (en particulier les enfants).

Un problème majeur est que les parents sont inquiets de ce que font leurs enfants dans l'univers numérique. Dans certains pays, on observe une progression sensible de l'utilisation par les enfants d'appareils mobiles intelligents, qu'ils préfèrent de plus en plus à l'ordinateur. Cette appétence les expose à un certain nombre de problèmes de paiement qu'ils ne sont pas toujours en mesure de comprendre. Comme on a pu le constater à travers plusieurs affaires récentes dont la presse s'est largement fait écho, les enfants peuvent facilement engager au moyen d'appareils mobiles des dépenses importantes à l'insu et sans le consentement de leurs parents. Avec la sophistication, la puissance et la complexité accrues des appareils mobiles, beaucoup de parents ne se doutent pas ou ne réalisent pas ce que peuvent faire leurs enfants à l'aide de ces objets (notamment effectuer des achats de biens virtuels ou de services sans posséder de carte de débit). Les solutions existantes, comme les technologies de détermination de l'âge et le plafonnement des dépenses, peuvent s'avérer insuffisantes face au dynamisme des technologies et à la rapidité de l'évolution des marchés.

Plus généralement, on s'accorde à considérer qu'il existe aussi un besoin de protection et d'éducation pour d'autres publics vulnérables ou défavorisés, notamment les personnes âgées et des

groupes sociaux spécifiques, qui peuvent être particulièrement vulnérables aux pratiques commerciales mensongères ou avoir des difficultés à comprendre les mécanismes de paiement.

Dans différents pays, ou même au sein de certains pays, on trouve des moyens et des plateformes de paiement qui ne sont pas toujours interopérables, ce qui peut empêcher les consommateurs de procéder à certains achats en ligne ou sur mobile.

Un certain nombre de moyens de paiement utilisés dans certains pays, pour des raisons techniques ou commerciales, ne sont pas acceptés par tous les commerçants. Le problème est encore exacerbé lorsque l'on passe à la dimension internationale : il arrive ainsi que des consommateurs situés dans un pays ne puissent pas effectuer avec leur carte de paiement des achats auprès d'un commerçant basé dans un autre pays.

RÉFÉRENCES

ACCC (Australian Competition and Consumer Commission) (2010), *Online shopping - When Things Go Wrong*, www.accc.gov.au/content/index.phtml/itemId/268478, consulté le 6 janvier 2011.

Banque de Finlande (2003), *Card, Internet and mobile payments in Finland*, Financial Markets Department, mars 2003, http://129.3.20.41/eps/dev/papers/0405/0405004.pdf.

Banque du Japon (2009), *Developments in Electronic Money in Japan during Fiscal 2008*, Payments and Settlement Systems Department, 24 août 2009, www.boj.or.jp/en/research/brp/ron_2009/data/ron0908b.pdf.

BBA (British Bankers' Association) (2008), *UK Banking Code*, March 2008, www.bba.org.uk/content/1/c6/01/30/85/Banking_Code_2008.pdf.

BILETA (2002), « Enhancing Consumer Confidence in Electronic Commerce: Consumer Protection in Electronic Payments », 17e conférence annuelle BILETA, www.bileta.ac.uk/Document%20Library/1/Enhancing%20Consumer%20Confidence%20in%20Electronic%20Commerce%20-%20Consumer%20Protection%20in%20Electronic%20Payments.pdf.

Bin Tang - YeePay CEO (2009), *Innovations in China's e-Payment Market*, novembre 2009, http://iis-db.stanford.edu/docs/189/epayment_bin_tang.pdf.

Capgemini (2010), *World Payment Report 2010*, 19 octobre 2010, www.fr.capgemini.com/ressources/publications/le-world-payment-report-2010/.

China Daily (2010), *Third party payments regulated*, 22 juin 2010, www.chinadaily.com.cn/bizchina/2010-06/22/content_10001206.htm.

CISCO (2008), *Consumer Online Shopping and Payment Experience Shape In-store Expectations*, Cisco Internet Business Solutions (IBSG) Primary Research, septembre 2008, www.aboutcisco.biz/web/strategy/docs/finance/ConnectedPaymentsExecSummary_092208.pdf.

Credit Union Times (2010), *Additional Consumer Protection Strategy is Launched by Visa*, 12 mai 2010, www.cutimes.com/Issues/2010/May-12-2010/Pages/Additional--Consumer-Protection-Strategy-Is-Launched-by-Visa.aspx.

Consumer Focus (2009), *Pocket Shopping*, décembre 2009, www.consumerfocus.org.uk/assets/1/files/2009/06/Pocketshopping.pdf.

Cour de justice de l'Union européenne (CJUE) (2010), *Verbraucherzentrale Nordrhein-Westfalen eV v. Handelsgesellschaft Heinrich Heine GmbH*, Affaire C-511/08, au Journal officiel de l'Union européenne C 148, 5 juin 2010, p. 6, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:148:0006:0007:FR:PDF.

CSN (Consumer Sentinel Network) (2010), *Data Book for January-December 2009*, US Federal Trade Commission, février 2010, www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf.

CyberSource (2010), *Online Fraud Report*, 11e édition annuelle, 2010, http://forms.cybersource.com/forms/FraudReport2010NACYBSwwwQ109.

Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (Directive sur le commerce électronique), 8 juin 2000, Bruxelles (Belgique), Journal officiel, n° L 178, p. 1-16, 17 juillet 2000, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT.

Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 *concernant les services de paiement dans le marché intérieur*, 13 novembre 2007, Bruxelles (Belgique), Journal officiel, n° L 319, p. 1-36, 5 décembre 2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:01:FR:HTML.

Directive 2009/110/CE of the European Parliament and of the Council of 16 September 2009 du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissement Directive sur la monaie électronique), Bruxelles (Belgique), OJ L 267, 10 octobre 2009, p. 7-17, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:FR:PDF.

Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs (Directive sur les droits des consommateurs), Bruxelles (Belgique), Journal officiel de l'Union européenne L. 304/64, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:304:0064:0088:FR:PDF

Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), Public Law 111-203, H. R. 4173, Washington, D.C., États-Unis d'Amérique, 21 juillet 2010, www.gpo.gov/fdsys/pkg/PLAW-111publ203/pdf/PLAW-111publ203.pdf.

CE (Commission européenne) (2007), Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen, à la Banque centrale européenne et à Europol – *Un nouveau Plan d'action de l'UE (2004-2007) pour la prévention de la fraude sur les moyens de paiement autres que les espèces*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0679:FR:NOT.

CE (2008*a*), « Principaux enjeux de la politique des consommateurs à l'ère numérique », Table ronde sur les questions soulevées par l'ère numérique, discours de Meglena Kuneva, Londres, 20 juin 2008, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/08/347.

CE (2008*b*), *Report on Fraud regarding Non-Cash Means of Payments in the EU: the Implementation of the 2004-2007 EU Action Plan*, document de travail des services de la Commission, SEC(2008)511, Bruxelles, 22 avril 2008, http://ec.europa.eu/internal_market/payments/docs/fraud/implementation_report_en.pdf.

CE (2011), « Preliminary Findings from a Market Study on the Functioning of E-commerce in Goods », présentation à l'Atelier de l'OCDE sur la protection des consommateurs dans les paiements en ligne et sur mobile, le 15 avril 2011, dans les locaux de l'OCDE, Paris.

CE (2012*a*), *Livre vert, Vers un marché européen intégré des paiements par carte, par Internet et par téléphone mobile*, Bruxelles, 11 janvier 2012, COM(2011)941 Final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0941:FIN:FR:PDF

CE (2012*b*), *Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. Un cadre cohérent pour renforcer la confiance dans le marché unique numérique du commerce électronique et des services en ligne*, Bruxelles, janvier 2012, COM(2011)942, http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/COM2011_942_fr.pdf

Réseau CEC (réseau des Centres européens des consommateurs) (2008), *The European Online Marketplace: Consumer Complaints 2007*, mai 2008, http://ec.europa.eu/consumers/redress_cons/docs/ECC_E-commerce_report.pdf.

E-commerce News (2010), Report Finds Disconnect Between Alternative Payment Preferences and Offerings, *E-commerce News*, 22 octobre 2010, http://ecommercejunkie.com/2010/10/22/report-finds-disconnect-between-alternative-payment-preferences-and-offerings/.

EMOTA (European Multi-channel and Online Trade Association) (2010), *Trustmarks Schemes Across Europe*, www.emota.eu/consumer-trust.html.

EPC (Conseil européen des paiements) (2010*a*), *White Paper on Mobile Payments*, 1ère édition, 18 juin 2010, Bruxelles, www.europeanpaymentscouncil.eu/documents/EPC492-09%20White%20Paper%20Mobile%20Payments%20version%202.0%20finalrev.pdf.

EPC (2010*b*), *Driving Forward the SEPA Vision*, rapport annuel 2009, http://www.europeanpaymentscouncil.eu/documents/EPC050-10%20EPC%20Annual%20Report%20v%201.0%20final.pdf.

Facebook (2009), *Spare Change*, foire aux questions, http://apps.facebook.com/sparechange/buyerFAQ.action?page=buyerFAQ, consulté le 6 janvier 2011.

KPMG (2007), *Mobile Payments in Asia Pacific*, 2007, www.kpmginsiders.com/pdf/Mobile_payments.pdf.

FRBB (Federal Reserve Bank of Boston) (2010*a*), *Mobile Payments in the United States at Retail Point of Sale: Current Market and Future Prospects*, 17 mai 2010, Marianne Crowe, Marc Rysman et Joanna Stavins, www.bos.frb.org/economic/ppdp/2010/ppdp1002.htm.

FRBB (2010*b*), *The Mobile Payment Landscape*, présentation de Marianne Crowe, 23 février 2010, www.bosfed.org/economic/cprc/presentations/2010/Crowe022310.pdf.

GAFI (Groupe d'action financière) (2006), *Report on New Payment Methods*, 13 octobre 2006, OCDE, Paris, www.fatf-gafi.org/dataoecd/30/47/37627240.pdf.

GAFI (2008), *Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems*, 18 juin 2008, OCDE, Paris, www.oecd.org/dataoecd/57/21/40997818.pdf.

FeliCa (2010), *A Message from our President*, www.felicanetworks.co.jp/en/company/message.html.

Forrester Research (2009), *Western European Online Retail and Travel forecast 2008-2014*, mars 2009, cité par *Les Echos*, 12 juin 2009, www.lesechos.fr/medias/2009/0612//300355565.pdf.

Forrester Research (2010), *US Consumers Continue To Show Limited Interest in Mobile Payments*, 20 octobre 2010, www.internetretailer.com/2010/10/20/consumers-are-mobile-companies-still-have-catching-do.

FCC (Federal Communications Commission) (États-Unis) (2011), *FCC Proposes Rules to help Consumers Identify and Prevent "Mystery Fees" on Phone Bills, Known as "Cramming"*, communiqué d'information, 12 juillet 2011, http://transition.fcc.gov/Daily_Releases/Daily_Business/2011/db0712/DOC-308351A1.pdf.

FTC (Federal Trade Commission) (États-Unis) (2003), *A Consumer Guide to E-Payments*, mars 2003, www.ftc.gov/bcp/edu/pubs/consumer/tech/tec01.shtm.

FTC (2008), *"Free Software CD" Internet Operation Settles FTC Charges*, communiqué de presse, 11 juin 2008, www.ftc.gov/opa/2008/06/manay.shtm.

Gigaom (2011), *Mobile payments worth $670 billion by 2015*, par Ryan Kim, 5 juillet 2011, http://gigaom.com/2011/07/05/mobile-payments-worth-670-billion-by-2015/

GSM Association (GSMA) (2010), *New Report Predicts Explosive European Growth for Mobile Broadband*, 12 janvier 2010, www.gsmworld.com/newsroom/press-releases/2010/4549.htm.

Innopay (2010), *Online Payments 2010, Increasingly a Global Game*, mai 2010, www.europeanpaymentscouncil.eu/knowledge_bank_download.cfm?file=Online payments 2010 - Report Innopay.pdf.

Innopay (2011), *Mobile Payments 2012, My Mobile, My Wallet?*, September 2011, http://www.innopay.com/publications/mobile-payments-2012-my-mobile-my-wallet.

Internet Retailer (2010*a*), *Credit Cards Are Losing Some Luster with Online Shoppers*, 19 février 2010, www.internetretailer.com/2010/02/19/credit-cards-are-losing-some-luster-with-online-shoppers.

Internet Retailer (2010*b*), *Credit Card Rules Change*, 4 octobre 2010, www.internetretailer.com/2010/10/04/credit-card-rules-change.

Internet Retailer (2010*c*), *US m-commerce sales to hit $2.4 billion this year, ABI Research predicts*, 1er mars 2010, www.internetretailer.com/2010/03/01/u-s-m-commerce-sales-to-hit-2-4-billion-this-year-abi-researc.

Internet Retailer (2010*d*), *U.K. Retailers Feel Ill-Prepared to Handle International Payments*, 8 juillet 2010, www.internetretailer.com/2010/07/08/uk-online-merchants-face-variety-payment-schemes.

Javelin Research (2010), *Online Retail Payments Forecast 2010 – 2014*, février 2010, https://www.javelinstrategy.com/uploads/files/1005.P_OnlineRetailPaymentsForecastSampleReport.pdf.

Juniper Research (2010), *Mobile Payment Transactions to Double in Value to 200 billion USD by 2012*, communiqué de presse, 16 juin 2010, www.juniperresearch.com/viewpressrelease.php?pr=190.

M's Communicate (2010), *Denshi Money*, www.emscom.co.jp/report_detail_76.html (en japonais uniquement).

MacCarthy, Mark et Gain Hillebrand (2010), *Viewpoint: Mobile Payments Call For Clear Consumer Protections*, American Banker, 10 août 2010, www.americanbanker.com/issues/175_152/vp-hillebrand-mobile-protections-1023818-1.html.

McAfee (2008), *Mobile Security Report 2008*, février 2008, www.mcafee.com/us/resources/reports/rp-mobile-security-2008.pdf.

Mallat, Niina (2007), *Exploring Consumer Adoption of Mobile Payments – A Qualitative Study,* Helsinki School of Economics, 2007, http://portal.acm.org/citation.cfm?id=1322013.

Marketwire (2010), *China's Digital Generations 2.0: Digital Media and Commerce Go Mainstream*, Boston Consulting Groupe Report, 6 mai 2010, www.marketwire.com/press-release/Explosive-Growth-Internet-Use-Is-Fundamentally-Changing-Chinas-Economy-Society-Says-1160501.htm.

Microsoft (2009), *Mobile Payments*, *White Paper*, Microsoft, septembre 2009, www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=9997243d-5f1b-405b-b0cb-f14ecdfb8566.

Mobey Forum (2010), *Mobile Remote Payments General Guidelines for Ecosystems, White Paper*, juin 2010, www.mobeyforum.org/files/Remote%20Payments%20White%20Paper%20FINAL.pdf.

Mopay (2010), *Mopay Becomes the First Provider to Enable Mobile Payments for the Purchase of Physical Goods Around the Globe*, communiqué de presse, 18 mai 2010, http://mopay-inc.com/fileadmin/templates/mindmatics/images/pressreleases/en/20100518_PM_physical_goods.pdf.

Morgan Stanley (2010), *Internet trends*, présentation au CM Summit, New York, 7 juin 2010, www.morganstanley.com/institutional/techresearch/pdfs/MS_Internet_Trends_060710.pdf.

New York Times (2010), *PayPal Hopes Open Platform Will Spur Innovation*, Claire Cain Miller, 21 octobre 2009, sommet web 2.0, San Francisco, http://bits.blogs.nytimes.com/2009/10/21/paypal-hopes-open-platform-will-spur-innovation/.

NFC Times (2010), *Report: Japan's M-Payment Players Discover that Points Count*, 11 juin 2010, www.nfctimes.com/news/report-japan-s-m-payment-players-discover-points-count.

Nomura Research Institute (2010), *Denshi Money Ni Kansuru Aanketo Chosa*, 24 août 2010, www.nri.co.jp/news/2010/100826.html (en japonais uniquement).

Noone, Claire (2011), *Consumer Policy Challenges: Regulatory Frameworks*, présentation à l'Atelier de l'OCDE sur la protection des consommateurs dans les paiements en ligne et sur mobile, le 15 avril, dans les locaux de l'OCDE, Paris.

OCDE (Organisation de coopération et de développement économiques) (1998), Conférence ministérielle de l'OCDE *Un monde sans frontières : concrétiser le potentiel du commerce électronique mondial*, Ottawa, Canada, SG/EC(98)14/FINAL www.olis.oecd.org/olis/1998doc.nsf/linkto/sg-ec(98)14-final

OCDE (1999), *Lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique*, OCDE, Paris, 1999, www.oecd.org/dataoecd/17/59/34023530.pdf.

OCDE (2002), *Consumer Protection for Payment Cardholders* [DSTI/CP(2001)3/FINAL], OCDE, Paris, 2002, www.olis.oecd.org/olis/2001doc.nsf/LinkTo/NT0000099E/$FILE/JT00128255.PDF.

OCDE (2005), *Consumer Dispute Resolution and Redress in the Global Marketplace*, OCDE, Paris, 2005, www.oecd.org/dataoecd/26/61/36456184.pdf.

OCDE (2006), *Online Payment Systems for E-commerce*, [DSTI/ICCP/IE(2004)18/FINAL], OCDE, Paris, 2006, www.oecd.org/dataoecd/37/19/36736056.pdf.

OCDE (2007*a*), *Recommandation de l'OCDE sur l'authentification électronique et Orientations pour l'authentification électronique*, OCDE, Paris, juin 2007, www.oecd.org/dataoecd/31/63/38924785.pdf.

OCDE (2007*b*), *Recommandation de l'OCDE sur le règlement des litiges de consommation et leur réparation*, OCDE, Paris, 2007, www.oecd.org/dataoecd/43/49/38960185.pdf.

OCDE (2007*c*), *Le commerce mobile*, OCDE, Paris, 2007, www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2006)7/FINAL&docLanguage=Fr.

OCDE (2008*a*), *Document exploratoire sur le vol d'identité en ligne*, www.oecd.org/dataoecd/3/8/40699509.pdf.

OCDE (2008*b*), *Orientations de l'OCDE pour les politiques sur le vol d'identité en ligne*, OCDE, Paris, 2008, www.oecd.org/dataoecd/51/59/40883671.pdf.

OCDE (2008*c*), *Orientations de l'OCDE pour les politiques concernant les questions émergentes de protection et autonomisation des consommateurs dans le commerce mobile*, OCDE, Paris, 2008, www.oecd.org/dataoecd/51/60/40883688.pdf.

OCDE (2008*d*), *Le rôle de la gestion de l'identité numérique dans l'économie internet : Guide d'introduction a l'intention des décideurs*, OCDE, Paris, 2008, www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2008)10/FINAL&docLanguage=Fr.

OCDE (2009*a*), *Conference on Empowering E-Consumers: Strengthening Consumer Protection in the Internet Economy, Background Report*, OCDE, Paris, 2009, www.oecd.org/dataoecd/44/13/44047583.pdf.

OCDE (2009*b*), *Consumer Education, Policy Recommendations of the Committee on Consumer Policy*, OCDE, Paris, octobre 2009, www.oecd.org/dataoecd/32/61/44110333.pdf.

OCDE (2010*a*), *Guide pour le développement des politiques de consommation*, OCDE, Paris, juillet 2010, www.oecdbookshop.org/oecd/display.asp?lang=fr&sf1=DI&st1=5KS73TB4NCBW.

OCDE (2010*b*), Conférence de l'OCDE *"Des consommateurs plus autonomes et mieux protégés dans l'économie internet". Synthèse des principaux points – Conclusions*, [DSTI/CP(2010)2/FINAL], OCDE, Paris, 2010, www.oecd.org/dataoecd/32/10/45061590.pdf (document en ligne en anglais uniquement).

OCDE (2010*c*), *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, compte-rendu succinct de l'Atelier, OCDE, Paris, 2010, www.oecd.org/dataoecd/8/59/45997042.pdf.

OCDE (2011*a*), *The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them,* OCDE, Paris, 2011, www.oecd-ilibrary.org/docserver/download/fulltext/5kgcjf71pl28.pdf?expires=1312971854&id=id&accname=guest&checksum=A6DFC0B52932638891E80E50EEEBE52B.

OCDE (2011*b*), *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, OCDE, Paris, 2011, www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2010)11/FINAL&docLanguage=En.

OCDE (2011*c*), *OECD Guide to Measuring the Information Society 2011*, OCDE, Paris, 2011, www.oecd.org/sti/measuring-infoeconomy/guide.

OCDE (2011*d*), *Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy, Guidance for Government Policy Makers*, OCDE, Paris, 2011, http://www.oecd-ilibrary.org/science-and-technology/digital-identity-management-for-natural-persons_5kg1zqsm3pns-en

OFT (Office of Fair Trading) (2010*a*), *E-Consumer Protection, A Public Consultation on Proposals*, juillet 2010, www.oft.gov.uk/shared_oft/consultations/eprotection/oft1252con.pdf.

OFT (2010*b*), *Attitudes to Online Markets*, rapport de FDS International pour l'OFT, août 2010, www.oft.gov.uk/shared_oft/consultations/eprotection/oft1253.

OFT (2010*c*), *Investigation into an Online Retailer relating to Non-Delivery of Orders and Failure to Provide Refunds*, affaire close en décembre 2009, www.oft.gov.uk/OFTwork/consumer-enforcement/consumer-enforcement-completed/shop4tek/.

Payments Council (Royaume-Uni) (2010), *The Way We Pay 2010*, www.paymentscouncil.org.uk//files/payments_council/the_way_we_pay_2010_final.pdf.

Payments Administration (Royaume-Uni) (2010), *Card Fraud Facts and Figures*, www.ukpayments.org.uk/resources_publications/key_facts_and_figures/card_fraud_facts_and_figures/.

PayPal (2010), *Conditions d'utilisation du service Paypal™*, 2010, https://www.paypal.com/cgi-bin/webscr?cmd=p/gen/terms-outside.

Report Linker (2010), *China Mobile Payment Survey Report, 2010*, www.reportlinker.com/p0318794/China-Mobile-Payment-Survey-Report.html.

Sénat (États-Unis) (2009), *Aggressive Sales Tactics on the Internet and their Impact on American Consumers*, Commission du Commerce, des Sciences et des Transports, rapport des services de la Commission à son président, J. Rockefeller, 16 novembre 2009, http://commerce.senate.gov/public/?a=Files.Serve&File_id=594bd7e1-c14b-42ac-b473-0ef90330efea.

The Paypers (2010*a*), *Mopay Enables Mobile Payments for the Purchase of Physical Goods,* 19 mai 2010, www.thepaypers.com/news/mobile-payments/mopay-enables-mobile-payments-for-the-purchase-of-physical-goods/741247-16.

The Paypers (2010*b*), *Virtual Goods: the Next Big Opportunity in the US?*, vol. 3, n° 11, 7 juin 2010, www.thepaypers.com/headlines/online_paypers.pdf.

The Paypers (2010*c*), *Alipay reaches 500 million user milestone*, 26 novembre 2010, www.thepaypers.com/news/online-payments/alipay-reaches-500-million-user-milestone/742633-3.

The Paypers (2010*d*), *Mobile Payments Surge in China*, 31 May 2010, www.thepaypers.com/news/mobile-payments/mobile-payments-surge-in-china/741312-16.

The Paypers (2010*e*), *Russian Government Approves E-Payment Bill*, 19 November 2010, www.thepaypers.com/news/online-payments/russian-government-approves-e-payment-bill/742567-3.

Ramezani, Elham (2008), *Mobile Payment*, juin 2008, http://webuser.hs-furtwangen.de/~heindl/ebte-08-ss-mobile-payment-Ramezani.pdf.

Roth, Daniel (2010), *The Future of Money, It's Flexible, Frictionless and (Almost) Free*, 31 mai 2010, www.wired.com/magazine/2010/02/ff_futureofmoney/all/1.

Sage (Royaume-Uni) (2009), *68% of Online Retailers Admit Payment Fraud Threatens Business Growth*, 19 mai 2009, www.sage.co.uk/press_office/payment_fraud.aspx.

Université Simon Fraser (2006), *Privacy Rights and Prepaid Communication Services: A Survey of Prepaid Mobile Phone Regulation and Registration Policies among OECD Member States*, rapport de recherche pour le compte du Commissariat à la protection de la vie privée du Canada, mars 2006, http://www.sfu.ca/cprost/prepaid/docs/Gow-PrivacyRightsAndPrepaidCommunicationServices.pdf.

TACD (Dialogue transatlantique des consommateurs) (2009), *Resolution on E-commerce*, décembre 2009, http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=260&Itemid.

CNUDCI (Commission des Nations Unies pour le droit commercial international) (2010*a*), *Travaux futurs possibles concernant le règlement en ligne des différends dans les opérations de commerce électronique internationales*, Note du Secrétariat, Quarante-troisième session, New York, 21 juin–9 juillet 2010, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/V10/531/01/PDF/V1053101.pdf?OpenElement.

CNUDCI (2010*b*), *Rapport du Groupe de travail III (Règlement des litiges en ligne) sur les travaux de sa vingt-deuxième session (Vienne, 13–17 décembre 2010)*, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/V11/801/49/PDF/V1180149.pdf?OpenElement.

CNUDCI (2011), *Rapport du Groupe de travail III (Règlement des litiges en ligne) sur les travaux de sa vingt-troisième session (New York, 23–27 mai 2011)*, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/V11/834/62/PDF/V1183462.pdf?OpenElement.

CNUCED (Conférence des Nations Unies sur le commerce et le développement) (2009), *Information Economy Report 2009*, New York et Genève, 2009, http://unctad.org/en/docs/ier2009_en.pdf.

Virtual Goods News (2010), *Boku Takes $25M Series C Round*, 19 janvier 2010, www.virtualgoodsnews.com/2010/01/boku-takes-25m-series-c-round.html.

Visa Europe (2009), *Rapport annuel 2009*, http://visa-europe.fr/fr/a_propos_de_visa/rapport_annuel.aspx.