LE PAIEMENT : ENJEU DU E - COMMERCE

par Garance MATHIAS - CEJEM-Paris II
et Jean-Michel SAHUT - INT - CETFI-Université d'Aix-MARSEILLE III

RESUME

Le développement du commerce sur Internet est lié à la confiance des consommateurs dans les systèmes de paiement. L'objet de cet article est d'analyser les solutions de paiement, qui ne relèvent apparemment que de l'application de technologies de l'information et de la communication et de cryptographie sur une architecture de réseau particulière (un réseau ouvert). En fait, le succès des solutions de paiement ne peut se comprendre qu'au travers des stratégies des acteurs du e-commerce.

La multiplicité des offres, et l'absence d'un standard se traduit par un marché très fragmenté des systèmes de paiement électronique, dominé par SSL, et un comportement attentiste des entreprises qui hésitent à investir. Toutefois, il semblerait que SET, soutenu par les émetteurs de cartes Visa et Mastercard, de grandes banques, et des gestionnaires de réseau comme IBM puisse devenir rapidement un standard pour les transactions à base de carte bancaire.
Par contre, en ce qui concerne les micro-paiements, l'avenir est plus incertain. Le concurrent principal des approches propriétaires est le porte-monnaie électronique, lequel est handicapé par l'obligation faite au client de posséder un lecteur de carte pour être utilisé sur Internet.

INTRODUCTION

Les systèmes de paiement électronique existent en France depuis les années 60. Ils ont été développés par les banques et les organismes de crédit afin de satisfaire les besoins liés au développement des échanges internationaux, et à la multiplication des services, notamment financiers. Cependant, ils étaient étroitement encadré par les autorités monétaires et les institutions de crédit, tant au niveau des normes (sécurisation, logiciels propriétaires), qu'au niveau des politiques monétaires. De plus, ces systèmes ont été développés sur la base de réseaux fermés (réservés à ces institutions), et dans l'objectif d'optimiser la sécurité des transactions. En fait, sur ces réseaux (Target, Swift, Réseau d'autorisation Carte Bleue, etc.) les transactions portent sur des montants suffisants pour que le coût de la sécurité des transactions soit acceptable.

Cette situation est remise en cause par le développement du commerce sur Internet, et en particulier par la multiplication des acteurs qui échangent de la monnaie électronique sur Internet, c'est-à-dire sur un réseau ouvert, donc non sécurisé. Par ailleurs, les transactions peuvent être transfrontalières et de faible montant. Ainsi, des banques et des intermédiaires non bancaires (fournisseurs de service de paiement électronique) ont mis en place des systèmes de paiement électronique originaux, pour assurer la sécurité et la facilité des achats, dans un cadre international. L'enjeu du problème des paiements sur Internet est primordial car le développement du commerce électronique est lié à la confiance des consommateurs dans les systèmes de paiement.

L'objet de cet article est d'analyser les solutions de paiement, qui ne relèvent apparemment que de l'application de technologies de l 'information et de la communication et de cryptographie sur une architecture de réseau particulière (un réseau ouvert). En fait, le succès des solutions de paiement ne peut se comprendre qu'au travers des stratégies des acteurs du e-commerce : les consommateurs, les gestionnaires de réseau (de télécommunication, et de paiement), les fournisseurs de service de paiement électronique et les "cybermarchants".

Dans cette perspective, nous étudierons les besoins des utilisateurs en matière de paiement électronique (consommateurs et commerçants), puis nous verrons comment les différents systèmes de paiement répondent à ces attentes. Enfin, nous nous intéresserons aux stratégies des acteurs du e-commerce, et à l'impact de ces solutions de paiement sur le secteur bancaire.

1. LE PAIEMENT : ASPECTS JURIDIQUES

Préalablement à l'examen, des moyens de paiement électroniques qui sur Internet permettent d'éteindre une obligation pécuniaire contractée à l'occasion d'une transaction commerciale électronique, il nous semble indispensable, en raison du nombre d'interprétations et de définitions, de clarifier les différentes notions relatives au paiement.

On notera une règle particulièrement importante pour les nouveaux systèmes de paiement par Internet : le silence du législateur, l'ordre de virement n'est soumis à aucun formalisme. L'ordre peut donc être donné par un écrit quelconque (lettre missive), sans qu'aucune formule sacramentale ne soit requise. Ainsi, il peut être donné par télégramme, procédé informatique comme une bande magnétique, voire oralement notamment par téléphone.

Par conséquent, ce sont principalement des règles d'origine contractuelle qui ont vocation à fixer les conditions d'utilisation des moyens de paiement sur Internet[1].

1.1. Définition

Dans le langage courant, le paiement est défini comme l'acquittement d'une dette d'argent. Dans le langage juridique, la notion de paiement revêt un sens beaucoup plus large. Les articles 1235 à 1270 du code civil édictent que le paiement est un simple mode d'extinction des obligations contractuelles qu'elles soient pécuniaires ou non. La règle fondamentale du paiement est selon l'article 1243 du Code civil que le paiement doit avoir le même objet que celui de l'obligation.
L'extinction d'une obligation pécuniaire libellée en unités de valeur réside dans la remise au créancier de la somme d'argent qui lui était contractuellement due. Le solvens est donc valablement libéré envers l'accipiens dès lors qu'il a réglé sa dette monétaire dans l'unité de valeur (devise) dans laquelle elle est libellée.

Les instruments de paiement sont des moyens[2] de faire circuler des unités de valeur contenues dans un support monétaire ne pouvant pas circuler (tel est le cas de la monnaie scripturale). Ce sont en réalité des mandats de payer. Ils sont transmis à la banque ou à l'établissement de crédit du bénéficiaire de l'ordre de payer qui sera chargé de déposer les unités de paiement libellées en unités de valeur ou de compte sur le compte du bénéficiaire par simple jeu d'écritures.

1.2. Moment et lieu du paiement

Il est difficile de situer le lieu de formation du contrat sur Internet. En effet, les parties ne sont pas présentes physiquement et la rencontre des volontés ne se fait pas de façon instantanée. De plus, le Code civil ne prévoit rien ni quant au lieu ni quant au moment du paiement. En France, la doctrine majoritaire et la jurisprudence considèrent[3] que le moment du paiement est celui où le bénéficiaire du transfert électronique de fonds reçoit le montant qui lui est dû.

Plus particulièrement, concernant le moment du paiement par carte bancaire, on notera que la signature de la facture accompagnée de la présentation de la carte, ainsi que la frappe du code confidentiel n'éteignent pas la créance.
Toutefois, le système de paiement sécurisé distribué par Kleline[4] considère que le moment du paiement peut intervenir avant la réception par le fournisseur du paiement si celui-ci dispose d'un serveur temps qui permet d'identifier le moment exact où l'acheteur a mis en œuvre son moyen de paiement.
Concernant le lieu du paiement, la doctrine considère majoritairement que le lieu du paiement est celui où se trouve situé le porteur de la carte de paiement où l'émetteur de l'ordre de payer.

---

[1] M.Espagnon, « Le paiement d'une somme d'argent sur Internet », JCP ,G, 1999,p.787.

[2] M.Vasseur, « le paiement électronique : aspects juridiques », Banque 1985,p.340

[3] Cass, Civ, I, 22 juin 1993, Bull.Civ, n°229,p.158, "Epoux Rieu" a considéré qu'un "virement bancaire est effectivement réalisé par l'inscription de son montant au compte du bénéficiaire". On peut également cité Michel Vasseur, "le paiement électronique-Aspects juridiques", Revue Banque, 1987, p.3207.

[4] www.kleline.fr

1.2.1 L'irrévocabilité du paiement par carte

L'article 22 de la loi du 11 juillet 1985[5] pose le principe de l'irrévocabilité de l'ordre de paiement transmis par carte bancaire. Il est vrai que la faculté de révocation altère la sécurité du paiement[6]. Ainsi, dès l'accomplissement de la signature électronique composée de la frappe du code secret, le paiement est irrévocable.
Ce principe de l'irrévocabilité des ordres de paiement est reconnu dans le cadre de l'Union européenne[7], au contraire des Etats-Unis, par exemple, où la loi autorise la révocabilité de l'ordre. Il est vrai que cette faculté de révocation altère la sécurité du paiement ; elle a en fait été écartée par application de la règle concernant le droit commun des mandats posant le principe selon lequel tout mandat est révocable sauf si les parties en ont convenu autrement.

La détermination du moment où l'opération devient irréversible marque aussi, par voie de conséquence, le moment de la naissance du droit du bénéficiaire sur la somme, objet de l'ordre de virement.
Pour mémoire, il convient de rappeler que l'irrévocabilité de l'ordre de paiement est un principe juridique distinct de celui de l'inconstestabilité de l'existence de l'ordre de paiement, lorsque le système de paiement n'est pas sécurisé ou/et ne permet pas l'authentification des différents éléments de l'ordre.

1.2.2 Une autre question délicate naît de la nécessité de protéger le consommateur

Si l'irrévocabilité, comme nous l'avons vu, est nécessaire pour assurer la sécurité des transactions, son application peut néanmoins susciter des difficultés dans le cas de la vente à distance réalisée par un consommateur. En effet, ce dernier bénéficie en droit français et européen d'un délai de rétractation de 7 jours au moins[8] qui lui permet de revenir sur une opération commerciale conclue à distance, pour laquelle il a déjà effectué un paiement irrévocable. Dans ce contexte, il appartient alors au client-consommateur de réclamer directement au commerçant le remboursement des sommes versées.

Toutefois, Internet soulève de nombreuses interrogations en matière de détermination de la loi applicable au consommateur[9]. En cas de difficulté d'application du droit, la révocabilité de l'ordre pourrait constituer une solution favorable au consommateur[10]

1.3. Question de la preuve et de la signature électronique

En cas de contestation du client de la réalité ou du montant du débit sur son compte, se pose la question de la preuve. A qui incombe la charge de la preuve ? Quels sont les moyens de preuve autorisés et disponibles ? Quelle est leur force probante ?

1.3.1 Question de la valeur et de la force probante du paiement électronique

En vertu de l'article 1315 du Code civil, qui prévoit que celui qui réclame l'exécution d'une obligation doit le prouver, la charge de la preuve de la réalité de l'ordre de paiement revient à l'émetteur de la carte.
Le droit de la preuve de l'existence d'un engagement ou d'un paiement varie selon que l'existence du contrat est opposée à un commerçant ou à un non-commerçant.

---

[5] L'article 22 de la loi du 11 juillet 1985 consacre le principe de l'irrévocabilité de l'ordre donné au moyen d'une carte de paiement, intégré dans le décret-loi du 30 octobre 1935 par la loi du 30 décembre 1991. L'article 57-2 " l'ordre ou l'engagement de payer donné au moyen d'une carte de paiement est irrévocable . Il ne peut être fait opposition au paiement qu'en cas de perte ou de vol de la carte, de redressement ou de liquidation judiciaire du bénéficiaire ".

[6] J. Huet indique que " l'irrévocabilité permet de donner plus de sécurité à la banque, tout comme au fournisseur de biens et services, car elle implique l'interdiction pour le client de revenir sur son ordre une fois celui-ci émis ", J.C.P 1991, I, 324, " Aspects juridiques du télépaiement ".

[7] Recommandation de la Commission Européenne du 30 juillet 1997 concernant "les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire", Joce , n°L 208/52, 2.8.97

[8] Article L121-16 du Code de la consommation, Directive 97/7 de la Commission Européenne, 20.05.1997 concernant la protection des consommateurs dans le cadre de la conclusion de contrats à distance, Joce n°L144/19, 4.6.97.

[9] Selon la Convention de Rome du 19 juin 1980 sur la loi applicable aux obligations contractuelles, prévoit dans son article 5 que le consommateur doit normalement bénéficier de la protection de sa loi nationale lorsqu'il est sollicité dans son pays.

[10] Selon le Rapport du CNCT " Problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres", mai 1997 ,p.113 .

En droit français, les règles de preuve sont strictes: il faut un écrit, dans les contrats civils, pour tout achat supérieur à 5000 FF[11]. Au contraire, la preuve des contrats commerciaux[12] est libre. Pour couper court à la difficulté, on a songé à introduire dans les contrats une clause prévoyant que certains documents constitueraient la preuve des opérations effectuées. Les conventions sur la preuve sont licites, la règles de l'écrit fixée par le Code civil n'est pas d'ordre public. Par conséquent, les parties peuvent y déroger par contrat. Ainsi, dans un arrêt "Crédicas", la Cour de Cassation admet la validité des clauses déterminant le procédé de preuve de l'ordre de paiement, pour les seuls droits dont les parties ont la libre disposition[13].
On se trouve inéluctablement renvoyé à prévoir et à recommander, pour la sécurité de toutes les parties, l'établissement en double d'une pièce écrite, d'un bon de caisse dont on peut se demander s'il doit, de surcroît, être daté et signé par l'utilisateur, au moins pour les achats supérieurs à 5000 FF.

Le problème de la preuve reste donc entier pour les achats effectués par Internet: de papier , il ne peut être question dans ces cas. Cependant, on peut espérer que l'utilisation généralisée de la carte à puce sur Internet, apportera une solution satisfaisante au problème de preuve. En effet, elle garde en elle-même la preuve de son opération et de son montant.
L'intervention d'un tiers certificateur indépendant, chargé de contrôlé l'accomplissement des transactions électroniques et d'en conserver la trace peut jouer un rôle très important dans le système probatoire. Ainsi la désignation par les parties d'un tiers certificateur qui tiendrait son pouvoir des parties et non de la loi, serait une sorte de « notaire électronique ».

La meilleure solution reste l'emploi systématique d'accusé-réceptions électroniques ; la création d'un véritable formalisme électronique pourra renforcer la validité d'un système reposant sur l'absence de papier.
Adressé à l'émetteur du message, l'accusé-réception lui permet de s'assurer que le message est arrivé à destination (s'il est acheminé par l'intermédiaire d'un tiers devant vérifier qu'il a bien été reçu par l'émetteur), il donnera toute certitude aux parties sur le bon fonctionnement de la communication. Ainsi, l'émetteur sera protégé contre la mauvaise foi du destinataire, qui ne peut répudier la réception effective du message et réciproquement.
L'accusé-réception peut revêtir différentes formes : protocolaires (procédure intégrée à un protocole de communication), impliquer le contrôle quantitatif des messages (réception d'un message de x octets), ou inclure un code secret avec signature électronique (notamment pour certains types de transmission comme les opérations bancaires et boursières). Outre, le fait d'établir son existence, le système de l'accusé-réception permet d'établir la date d'envoi du message[14].

1.3.2 Avant-projet de loi relatif à l'adaptation du droit de la preuve aux nouvelles technologies

En France, un avant-projet de loi relatif à l'adaptation du droit de la preuve aux nouvelles technologies de l'information a récemment été publié. Cet avant-projet a pour objet de réaliser une adaptation du droit de la preuve aux nouvelles technologies. En matière civile, l'assimilation de la preuve par écrit au papier, dans la lecture qui est traditionnellement faite de l'article 1341 du code civil, s'accommode mal des évolutions technologiques qui conduisent de plus en plus fréquemment à la dématérialisation des échanges. Même si, la règle de la primauté de la preuve par écrit a connu de nombreux assouplissements (notamment, la jurisprudence a admis la validité des conventions de preuve), des incertitudes subsistent sur l'admissibilité comme preuve des messages dématérialisés ainsi que sur la force probante.
Ce texte introduit d'importantes innovations dans le droit de la preuve :
- nouvelle définition de la preuve par écrit, qui devient indépendante du support utilisé, et qui englobera les documents électroniques.
- admissibilité comme mode de preuve de l'écrit électronique, auquel il attribue une valeur probante particulière, ainsi que la validité de la signature électronique.

11 Article 1341 du Code civil

12 Article 109 du code de commerce

13 Cass, Civ, I, 8.11.1989, D.1990,p.369 reconnaît que la clause déterminant le procédé de preuve (l'utilisation concomitante d'une carte magnétique et du code confidentiel), fait partie des droits dont les parties ont la libre disposition.

14 Isabelle Pothier, « la preuve dans les transactions financières à distance », revue banque, n°568,p.70,1996.

En effet, l'écrit électronique, afin d'avoir une valeur probante, reste soumis à certaines exigences : elle n'est reconnue qu'à condition que les moyens techniques utilisés donnent des assurances aussi bien en ce qui concerne l'identité de celui dont émane cet écrit et auquel on entendrait l'opposer, que sur la bonne conservation de ce dernier. Par ailleurs , l'avant-projet reconnaît expressément la validité des conventions sur la preuve.
La reconnaissance et l'efficacité du document électronique comme mode de preuve serait privée de toute portée pratique si elle restait subordonnée à leur signature manuscrite, apposée de la main même de son auteur. L'avant-projet apporte donc une définition de la signature qui peut être admise sous forme électronique et précise les conditions qu'elle doit remplir (usage d'un processus fiable et permettant d'établir le lien avec l'acte sur lequel elle porte).
Il ne préserve la prééminence de l'écrit support-papier qu'en cas de conflit avec un écrit électronique et dans la seule hypothèse où les parties n'en auraient pas convenu autrement.
L'utilisation de la carte de paiement sur réseau Internet pose le problème de la signature électronique.

1.3.3 Question de la validité de la signature électronique

La signature est en principe, un instrument qui a une double fonction:
1. identifier les parties
2. authentifier le consentement des parties à être liées suivant les termes et conditions de leur contrat.

Elle s'entend habituellement d'une inscription manuscrite.
La signature manuscrite peut être définie comme une inscription sous forme particulière et consciente qu'une personne fait de son nom pour affirmer l'exactitude, la sincérité de l'écrit et en assume la responsabilité. Actuellement, il n'existe pas de définition de la signature en droit français.
Le développement des techniques a donné naissance à un nouveau type de signature.
La signature électronique est une transposition, une redéfinition de la signature par ses fonctions et non plus par sa forme.
La signature numérique s'accomplit par une procédure technique. Il est donc, pour le moment très difficile sinon impossible de savoir si la signature numérique suffit comme indication du consentement et comme preuve.
Les cocontractants s'en servent donc à leurs risques et périls.
Les problèmes soulevés par cette nouvelle forme de signature touchent:
- la validité du contrat : le contrat ne pourrait ne pas être valide dans certains cas, les cocontractants pouvant ainsi librement ne pas respecter leurs obligations.
- la preuve : cette forme de signature peut ne pas suffire comme preuve du consentement.

La signature électronique, sur réseau, est composée de l'entrée d'un code secret crypté. Elle n'est pas, en l'état actuel du droit, considérée comme équivalente à la signature manuscrite. En conséquence, ni la loi ni la jurisprudence n'ont reconnu la validité de ce type de signature de façon explicite. En principe, pour qu'un acte soit valable en la forme, une seule condition est posée : la signature.
Au niveau communautaire, une proposition de directive sur la reconnaissance de la signature électronique prévoit que celle-ci aura la même force probante et valeur juridique que la signature manuscrite. Actuellement, la signature électronique ne bénéficie pas encore d'une reconnaissance pleine et entière.
Cette proposition de directive donne lieu à une certaine audace juridique en affirmant un principe général de reconnaissance de la signature électronique.
La proposition de directive considère que les Etats membres doivent veiller à ce que les effets juridiques de la signature (force exécutoire, validité juridique) ne soient pas contestés « *au seul motif que la signature se présente sous forme électronique* » (art5-1).

La Commission pose donc un principe général de reconnaissance de la signature électronique. En effet, la valeur juridique de la signature est reconnue même si la signature électronique ne repose pas sur un certificat agréé, ou sur un certificat délivré par un PSC.

Au-delà de ce principe général, la Commission renforce la valeur juridique d'une signature électronique lorsqu'elle repose sur « *un certificat agrée délivré par un PSC qui satisfait aux exigences visées à l'annexe II* » (art5.2).
Dans ce contexte, la signature électronique a la valeur d'une signature manuscrite et elle est admissible comme preuve en justice.

La signature électronique est donc l'équivalent de la signature manuscrite. Cette reconnaissance de la signature en tant que preuve judiciaire est une innovation.
En effet, même si, la force et la valeur de cette preuve judiciaire (preuve parfaite, commencement de preuve par écrit) ne sont pas précisées dans le cadre du texte, ce principe d'admissibilité a des conséquences très importantes dans le droit interne des Etats membres.
En effet, les droits des Etats membres ne reconnaissent pas la valeur juridique de la signature électronique. Ainsi, en l'état actuel du droit français, la signature électronique n'est pas considérée comme équivalente à la signature électronique. En effet, ni la loi, ni la jurisprudence n'ont reconnu la validité de ce type de signature de façon explicite, et donc les règles de preuve traditionnelles s'appliquent[15].
Il convient de préciser que la directive devra être transposée dans les législations nationales dans un délai de 3 ans, c'est-à-dire avant le 1er janvier 2001, suivant les dispositions de l'article 12.

L'objectif de cette importante proposition de directive est d'aboutir à ce que le droit interne des Etats membres reconnaisse à la signature électronique la valeur juridique d'une signature écrite. Cette reconnaissance dans l'Union européenne et hors de l'Union permettrait de résoudre une partie de l'insécurité juridique des transactions électroniques sur Internet et l'investissement dans les services de commerce électronique connaîtrait un fort développement.

En conclusion, le problème de la preuve de l'acceptation de l'ordre de paiement ne peut, en l'état actuel de la législation française, être réglé que par convention expresse préalable entre les parties.

1.4. Le statut applicable aux moyens et prestations de cryptage

Les systèmes de paiement sur Internet reposant sur des transferts de données électroniques, doivent, pour répondre aux impératifs de sécurité précédemment décrits, utiliser des outils de cryptage, logiciel ou matériel qui permettent d'authentifier ou de chiffrer des transactions.

La cryptographie ou le chiffrement est le processus de transcription d'une information inintelligible par l'application de conventions secrètes dont l'effet est réversible[16].

Cette définition générale inclut également les signatures numériques qui constituent une des applications importantes de la cryptographie. Les signatures numériques permettent de prouver l'origine des données (authentification) et de vérifier si les données ont été altérées (intégrité). Le chiffrement permet donc de maintenir la confidentialité des données transmises, et des transactions financières émises (par exemple, le paiement sur réseau).

Actuellement, il existe deux grands types de cryptographie :
- la cryptographie symétrique : la même clé est utilisée pour chiffrer et déchiffrer l'information.
- la cryptographie asymétrique : dans ce cas, l'utilisateur dispose de deux clés différentes (une clé publique et une clé privée). Il communique sa clé publique à tout le monde. En revanche, il garde secrète sa clé privée et lui seul pourra décrypter et lire le message avec la clé privée. Cette application permet ainsi d'assurer la confidentialité des communications sur réseau ouvert. Aussi, cette paire de clés pour être utilisée afin d'authentifier l'émetteur du message. En effet, l'usage de la clé privée, secrète, permet de vérifier l'identité de l'expéditeur.

Dans tous les cas, pour que la méthode de cryptage soit fiable, il est nécessaire que les clés de cryptage soient sûres, c'est-à-dire qu'elles doivent être d'une longueur suffisante (codage de la clé). En effet, la fiabilité du système dépend de la puissance de calcul nécessaire à mettre en œuvre pour casser le code[17].

---

15 Notons à ce propos que l'arrêt de la Cour de Cassation « *Crédicas* » (C.Cass, 1 civ, 8.11.1989, *D. 1990,p.369*) a reconnue de manière ponctuelle la signature électronique. On soulignera que cette reconnaissance n'est intervenue que dans une circonstance d'espèce où les parties avaient convenue contractuellement d'une clause de preuve, alors que l'affaire litigieuse concernait une transaction d'une valeur inférieure à 5000 FF.

16 L'article 28 de la loi 90-1170 du 29.12.90 modifiée définit la cryptographie comme «toutes *prestations visant à rendre à l'aide de conventions secrètes des informations ou signaux clairs en information ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet* ».

17 Valérie Sédallian, « les problèmes posés par la législation française en matière de chiffrement », DIT 98/4.

En France, la cryptographie est soumise à une réglementation complexe et très formaliste. La loi de réglementations des télécommunications du 26 juillet 1996[18] et ses décrets d'application du 24 février 1998[19] autorisent l'emploi des procédés de cryptologie limité à 40 bits (cryptographie dite faible), tout en instituant au-delà de cette limite un système contraignant de dépôt des clés de chiffrement auprès d'un «tiers de confiance ».
Le 17 mars 1999 deux décrets et un arrêté ont porté de 40 bits à 128 bits le seuil en deçà duquel l'utilisation de la cryptologie est libre.

Une analyse succincte de ces textes fait apparaître que le système de déclaration se substitue à celui de l'autorisation pour la fourniture, l'utilisation et l'importation de matériels et logiciels offrant un service de confidentialité mise en œuvre par un algorithme dont la clé est supérieure à 40 bits et inférieure ou égale à 128 bits.
Il convient de noter que l'utilisation et l'importation des procédés de cryptologie sont soumis à déclaration lorsque ces procédés n'ont pas fait préalablement l'objet d'une déclaration par le producteur, fournisseur ou importateur.

En revanche, sont dispensées de formalités l'utilisation et l'importation de matériels et logiciels offrant un service de confidentialité mise en œuvre par un algorithme dont la clef est supérieure à 40 bits et inférieure ou égale à 128 bits à condition d'avoir fait l'objet d'une déclaration auprès du SCSSI[20] par le producteur, fournisseur ou importateur. Dans le cas contraire, la dispense de formalité est limitée aux produits dont la clé est inférieure ou égale à 40 bits.

2. LES SYSTEMES DE PAIEMENT

Après avoir posé les bases juridiques de notre réflexion, nous allons étudier les différentes solutions de paiement électronique sur le marché, et analyser comment elles répondent aux besoins des consommateurs. Enfin, nous nous intéresserons aux conséquences de l'arrivée de nouveaux entrants sur le secteur bancaire.

2.1. Les besoins

Sécurité, coût et facilité d'utilisation sont des critères fondamentaux de la réussite de la mise en place d'une solution de paiement sécurisé sur Internet.

Une sécurité à 5 niveaux *:* identification, authentification, intégrité des données, non répudiation, et solvabilité.

- **Identification** : Pour initier une transaction, il faut d'abord identifier les deux parties, l'acheteur (à cause du risque de non-paiement) et le vendeur (à cause du risque de non-livraison). Cependant, la confidentialité des informations du système de règlement s'avère indispensable. En particulier, le commerçant n'a pas à connaître le numéro de carte bancaire de ses clients, si le fournisseur de service de paiement (tiers de confiance) lui fournit une attestation de paiement en bonne et due forme. Réciproquement, ce dernier ne doit pas être renseigné sur le détail des achats des clients.
- **Authentification** : La transaction électronique doit être authentifiée. En effet, pour être certain de la volonté des parties, il faut vérifier que les parties soient d'accord sur les termes du contrat (caractéristiques du produit, quantité, prix, délais de livraison…).
- **Intégrité des données** : il est ensuite nécessaire de s'assurer que les informations concernant le paiement seront bien transmises dans leur intégralité sans modification par un tiers.
- **Non-répudiation** : le principe de l'irrévocabilité du paiement garantit le commerçant du paiement de la transaction.
- **Solvabilité du client** : Pour être certain d'être payé le fournisseur doit vérifier la solvabilité du client, ou les banques doivent garantir le paiement (par une assurance jusqu'à un certain montant).

Le rapport coût / sécurité : cet enjeu est particulièrement important pour les micro-paiements. En effet, le coût de transaction pour des paiements par carte bancaire nécessite des transactions d'un montant suffisant, étant donné la commission fixe minimale de cinq francs prélevée par les organismes émetteurs de carte tels Visa ou Mastercard.

[18] Article 17 de la loi, JO du 27 juillet 1996

[19] Décrets n°98-101 et n°98-102 du 24.02.98 (JO 24.02.98) complétés par six arrêtés du 13 mars 1998.

[20] Service Central de la Sécurité des Systèmes d'Information

L'utilisation doit rester simple *:* afin de toucher une cible d'utilisateurs la plus large possible, il est nécessaire que le système de paiement soit simple d'utilisation. Les systèmes répondant le mieux à ce besoin sont ceux qui sont transparents pour l'utilisateur, c'est-à-dire ceux intégrés d'origine aux navigateurs (exemples : SSL ou Microsoft Wallet), au contraire d'approches propriétaires, où il est nécessaire d'installer au préalable un logiciel spécifique (ex: Kléline), un périphérique, ou encore de saisir de manière répétée de longs mots de passe.

Les solutions actuelles de paiement électronique ne répondent que partiellement à ces besoins, et mettent souvent l'accent sur un point particulier, en négligeant les autres. En particulier, les approches propriétaires mettent, trop souvent, en avant la protection contre le risque de piratage pour masquer d'autres problèmes, comme la complexité de leur mise en œuvre, ou encore le manque d'inter-opérabilité entre eux.

2.2. Les trois grandes catégories de systèmes de paiement

Malgré la diversité des solutions existantes, nous avons essayé de les regrouper à partir des trois catégories suivantes : la monnaie électronique (monnaie virtuelle, porte-monnaie électronique et porte-monnaie virtuel), les paiements électroniques sécurisés par carte bancaire (SSL, SET et C-SET), et les paiements par chèque électronique.

2.2.1 Monnaie électronique

Selon la Banque des Règlements Internationaux[21], le concept de monnaie électronique se définit comme correspondant aux systèmes électroniques de dépôt d'unités de valeur monétaire en possession du consommateur qui les utilise pour effectuer des règlements. Ces systèmes peuvent être matérialisés sous deux formes : la monnaie virtuelle, et le porte-monnaie électronique ou virtuel.
Alors qu'avec une carte de paiement classique, le débit du compte intervient après la transaction, ces deux types de monnaie électronique reposent sur des systèmes de prépaiement (préalablement à une transaction, une réserve de fonds préalable doit être constituée). Dans le cas de la monnaie virtuelle et du porte-monnaie virtuel, la réserve de fonds est stockée sur le disque dur de l'utilisateur, tandis que pour le porte-monnaie électronique, elle est matérialisée par une carte. Le porte-monnaie électronique se distingue donc par ses usages multiples, puisqu'il peut être utilisé sur Internet et dans la " vie réelle ".

La Monnaie virtuelle : les cyberbucks (Digicash)

Fondé en 1990, Digicash est un pionnier dans le développement de mécanismes de paiement électroniques pour des réseaux ouverts et fermés. L'approche de Digicash consiste à émettre des pièces virtuelles, "les cyberbucks", qui sont des jetons encryptés correspondant à des unités monétaires qui sont stockées sur le disque dur de l'utilisateur. Cela nécessite pour les utilisateurs, l'ouverture d'un compte auprès d'une banque affiliée, ainsi que l'installation d'un logiciel spécifique permettant d'effectuer des transactions.

Lorsqu'un client effectue un achat, le logiciel de paiement prélève les pièces virtuelles nécessaires, et les transfère au bénéficiaire. Celui-ci les envoie à Digicash, qui vérifie les numéros de série et confirme le paiement. La particularité de ce système est de garantir l'anonymat du payeur, le destinataire des fonds étant en revanche identifiable par sa banque lors du traitement de la transaction.
Les pièces virtuelles ne sont pas reliées à un compte bancaire, mais à un établissement bancaire (à la manière des chèques au porteur) qui en garantit la conversion. L'échange de ces pièces entre internautes est alors possible, sans que l'on puisse déterminer d'où elles proviennent.
Cet instrument de paiement comporte trois risques majeurs : la création de faux cyberbucks, le blanchiment de capitaux, et la faillite de l'émetteur. En effet, contrairement aux autres moyens de paiement en ligne, cette monnaie est anonyme, les transactions ne sont donc pas traçables.
De plus, le risque de faillite de l'émetteur est réel. Aux Etats-Unis, suite au rachat de la Mark Twain Bank par la Mercantile Bank, l'argent électronique de Digicash n'est plus commercialisé. En effet, les résultats de cette expérience ont été jugés non rentables par le repreneur. Toutefois, l'expérience initiée par Digicash se poursuit dans de nombreux pays européens (Suède, Allemagne, etc)[22].

---

[21] "Implications pour les banques centrales du développement de la monnaie électronique", Rapport de la BRI, octobre 1996.

[22] Internet Professionnel, n°24, Octobre 1998, p.79.

Le Porte Monnaie Virtuel (PMV)

Le Porte Monnaie Virtuel (PMV) est un logiciel qui permet de stocker sur le disque dur d'un ordinateur, les pièces digitales représentant un pouvoir d'achat issu de la constitution préalable d'une réserve de fonds déposée dans un établissement de crédit.
Le PMV est alors débité au fur et à mesure des achats du client. Ce système est utilisé notamment par Kléline[23] et Cybercash[24].
Ces solutions opérationnelles sont propriétaires, et complexes à mettre en œuvre (un logiciel spécifique doit être installé sur le poste de l'utilisateur et du marchand). Par contre, elles permettent de gérer des micro-paiements, des règlements en plusieurs devises pour le commerçant, et de garantir l'identité réelle des parties en présence (le risque de faux vendeurs disparaît), et surtout la solvabilité des clients (car c'est un système de prépaiement).

Le Porte Monnaie Electronique (PME)

Le Porte Monnaie Electronique (PME) est une carte à microprocesseur dont la mémoire est créditée d'un pouvoir d'achat constitué par une réserve de fonds préalablement déposée dans un établissement de crédit. Cette réserve est débitée à chaque achat indépendamment de la banque.
Il existe actuellement sur le marché de nombreux porte-monnaie électroniques dont certains ont dépassé le stade de l'expérimentation comme Proton[25] en Belgique, ce qui n'est pas le cas de Mondex en Angleterre[26], ou de Passe[27] en France. Le succès de Proton est essentiellement local, avec 4 millions de cartes en circulation, et 23 000 terminaux installés. Cependant, ce système pourrait rapidement s'imposer en Europe ; 30 millions de cartes ont déjà été commandées[28] par des fournisseurs de service de paiement étrangers.

Les avantages de cet instrument de paiement sont multiples : il assure la sécurité des transactions (dans le cadre de l'utilisation d'un support physique, la carte à puce), il supporte les micro-paiements, il est simple à utiliser, et ses usages sont divers. Il peut être utilisé dans la vie réelle pour payer des petites dépenses et pour d'autres applications (carte de sécurité sociale, de fidélité, d'accès à des bâtiments…), ainsi que sur Internet.
Cependant, comme il nécessite l'utilisation d'un lecteur de carte (pin-pad), ces porte-monnaie électroniques ne sont pas encore expérimentés sur Internet. Toutefois, les constructeurs d'informatique prévoient de l'intégrer aux claviers des futurs ordinateurs.

2.2.2 Les paiements électroniques sécurisés par carte bancaire (SSL, SET, et C-SET)

En France, il convient d'opérer une distinction entre les cartes de paiement, les cartes de retrait et les cartes de crédit réel.

- Les cartes de paiement (ou carte de débit), font intervenir deux ou trois partenaires qui sont l'émetteur, le fournisseur agréé et le porteur de la carte. Le porteur de la carte peut retirer des espèces dans les DAB et les GAB[29], mais peut aussi régler les fournisseurs (commerçants et prestataires de services) liés à l'émetteur.
- Les cartes de retrait offrent un service minimum, celui de pouvoir débiter un compte bancaire en dehors des heures d'ouverture des guichets, c'est-à-dire auprès des GAB et DAB. Ce ne sont pas des instruments de paiement.
- Les cartes de crédit permettent à leur titulaire d'obtenir des lignes de crédit utilisables en tenant compte d'un certain plafond.

[23] www.kleline.com Il est important de préciser que Kléline comporte deux systèmes de paiement : un porte-monnaie virtuel (pour les micro-paiements), et un système de paiement par carte bancaire (pour les achats plus importants).
[24] www.cybercash.com
[25] www.proton.be
[26] www.mondex.com. Le transfert de porte-monnaie à porte-monnaie demeure en test.
[27] Le " Passe " de la RATP, qui donne accès au métro et au RER, est actuellement testé comme porte-monnaie électronique à Noisy-le-Grand.
[28] www.proton.be/fr/commercant/proton/index.html
[29] Distributeur Automatique de Billets (DAB), Guichet Automatique de Banque (GAB).

SSL

Sur Internet, la plupart des transactions sont actuellement réglées par carte bancaire, moyen de paiement traditionnel utilisé dans la vente à distance. Il existe deux catégories d'utilisation de SSL, avec ou sans intermédiaire.
Dans sa version standard, c'est-à-dire sans intermédiaire, le consommateur communique le numéro et la date d'expiration de sa carte bancaire au marchand cryptés par le protocole SSL (Secure Socket Layer). Afin d'éviter que les numéros de carte bancaire soient stockés par le commerçant, des intermédiaires ont créé des solutions de paiement, fondées sur ce protocole, dont l'objectif est de gérer le règlement entre le client et le commerçant. L'avantage principal de ces solutions comme Payline, SIPS[30] et Télécommerce (France Télécom), est de vérifier la solvabilité du client en interrogeant le réseau d'autorisation des cartes bancaires.
Cependant, ce système de règlement présente une sécurité sommaire. En effet, la version d'exportation (hors des Etats-Unis) de ce dernier était limitée à une longueur de clé de 40 bits jusqu'en janvier 1999. Or, il existe actuellement des boîtiers capables de casser des clés de 56 bits dans un délai de 2 heures maximum[31.] En fait, le manque de sécurité de ce type de solution ne réside pas dans la longueur des clés de cryptage. La crainte des banquiers n'est pas que le numéro de carte soit piraté lors d'une transaction. D'après G. DALIGAULT d'Europay, il existe deux risques majeurs. Un pirate peut parvenir à générer un numéro de carte qui correspond à un vrai numéro[32], ou s'introduire sur les serveurs insuffisamment protégés des petits commerçants (parce qu'ils n'ont pas la capacité financière de le faire), et récupérer des listes de vrais numéros de carte.

De plus, comme le commerçant est dans l'impossibilité d'authentifier son client à distance, celui-ci peut contester ses achats effectués par carte bancaire. Dans ce cas, la banque doit rembourser le client et le commerçant doit rendre l'argent. Ainsi, le fait de vérifier la solvabilité du client ne prémunit pas le commerçant contre le risque de non-paiement.

SET

Le système SSL n'offre aucune assurance quant à l'identité du commerçant et du client. C'est pourquoi plusieurs sociétés américaines (Visa, MasterCard, IBM, Netscape…) ont développé le protocole SET (Secure Electronique Transaction) afin de sécuriser à moindre coût les transactions par carte bancaire sur Internet. Le système repose sur le chiffrement des informations transmises (comme SSL), mais il délivre également des certificats d'authenticité des transactions électroniques. Le client doit d'abord saisir ses coordonnées bancaires à l'aide d'un programme annexe (plug-in) se greffant sur son navigateur.

Il envoie ensuite le fichier à l'organisme qui gère sa carte, lequel lui renvoie une clé de cryptage. Enfin, le client envoie cette clé au commerçant qui vérifie sa validité auprès de la banque. Avec ce type de solution le risque de faux vendeur ou de faux acheteur disparaît, car le commerçant et le client doivent s'enregistrer avant d'effectuer des transactions. Cependant, la sécurité de SET peut être mise en défaut en s'attaquant aux ordinateurs de consommateurs, car les clés secrètes sont stockées dessus.

C-SET

Afin d'adapter le protocole SET à la carte à puce française, et d'apporter un niveau de sécurité physique supplémentaire, le GIE Carte Bancaire a mis au point le protocole C-SET.

A titre de comparaison, il est important de préciser que grâce à l'utilisation de la carte à puce à la place de la piste magnétique, le taux de fraude sur les cartes bancaires est en France le plus bas du monde : 0,02% des transactions contre 3 à 4% aux Etats Unis.

---

[30] Les systèmes Payline et SIPS sont assez semblables. Ils utilisent le protocole de cryptage SSL pour l'envoi des données bancaires, qui ne sont pas exploitées par le marchand lui-même, mais par un serveur de paiement géré par Experian (Payline) et Atos (SIPS). A chaque transaction pour Atos, ou sur demande pour Experian, le serveur de paiement interroge le réseau carte bancaire pour s'assurer de la validité de la carte, et de la solvabilité du client.

[31] D'après C. HUITEMA, conférence de l'ISOC France, Autrans, 6 au 9 janvier 1999.

[32] La contrefaçon est beaucoup plus facile sur Internet, car les solutions de paiement usuelles ne nécessitent pas l'utilisation d'un support de carte physique. En effet, pour réaliser ce type de contrefaçon dans une boutique ("réelle"), cela nécessiterait d'encoder et d'embosser de vrais visuels de carte.

Le principe de ce système est simple. C'est la transposition de la procédure classique de paiement par carte bancaire: le client insère sa carte à puce dans un lecteur (relié ou incorporé à l'ordinateur), le montant de la transaction apparaît alors sur l'afficheur du lecteur, le client entre son code confidentiel à quatre chiffres (vérification du code par la puce), une demande d'autorisation est déclenchée, puis après confirmation, le ticket est édité.
Les avantages sont nombreux : les achats sont signés, le client n'est pas lié à un ordinateur particulier (car la sécurité du système ne repose pas sur le stockage de clés secrètes), et la banque n'a pas à diffuser les certificats d'authentification comme c'est le cas pour SET.
L'inconvénient principal est le même que celui du porte-monnaie électronique: l'utilisation d'un lecteur de carte[33].

Par ailleurs, C-SET reste compatible avec SET, et permet d'effectuer des paiements en France et à l'étranger grâce à la mise en place par le GIE Carte Bancaire d'un service traducteur entre SET et C-SET.
Le niveau de sécurité de C-SET est tel que, pour les clients français dotés d'une carte à puce, le paiement du commerçant peut être garanti par sa banque (c'est la "garantie commerçant"). Pour les clients internationaux, on distingue deux cas de figure. Soit le client utilise un système compatible avec SET, et dans ce cas le commerçant bénéficie d'un régime intermédiaire entre "la garantie commerçant" et la vente par correspondance. Soit le client a une carte à puce, et a un compte dans une banque qui utilise une solution similaire à C-SET (niveau de sécurité analogue). Dans ce cas, les promoteurs de C-SET prévoient de définir une réciprocité de garantie commerçant pour offrir une garantie de paiement.

En plus de la sécurité physique qu'offre la puce, elle dispose d'un avantage comparatif important par rapport aux cartes à bande : sa capacité de traitement et de calcul. En effet, si l'on compare sa puissance de calcul à celle d'un ordinateur (PC), elle a actuellement les performance d'un processeur 386 d'Intel, et il est prévu qu'elle atteindra celle d'un processeur 486 d'Intel à l'horizon de l'an 2000[34]. De plus, son système d'exploitation actuellement propriétaire va s'ouvrir au monde Java[35] (Javacard), et permettre à n'importe quel développeur d'imaginer de nouvelles applications, financières ou non.
Tous ces avantages expliquent pourquoi certains pays ayant beaucoup de porteurs de cartes, tels que l'Angleterre ou l'Allemagne, s'équipent en cartes à puce et envisagent l'utilisation de C-SET.

2.2.3 Les paiements par chèque électronique

Le chèque de banque se définit comme un écrit par lequel le tireur donne l'ordre au tiré (banque ou établissement de crédit) de payer à vue une somme déterminée à l'ordre du bénéficiaire. C'est un titre de banque négociable à ordre. Le chèque électronique est la transposition de ce mécanisme dans un environnement dématérialisé. La représentation du chèque ne se fait plus sur support papier, seules les informations relatives au chèque sont transmises comme dans la plupart des systèmes de compensation interbancaires.
En général, le client envoie l'ordre de paiement au commerçant qui le présente à l'organisme émetteur de chèque électronique afin de l'authentifier et d'en effectuer la compensation. Les informations relatives au chèque et au bénéficiaire sont alors transmises au système de compensation interbancaire. Ensuite, la procédure bancaire de transfert de fond, entre les comptes est analogue à celle d'un " chèque papier ".

Les deux avantages principaux de ce système résident dans les qualités intrinsèques même du chèque, auquel s'ajoute le bénéfice d'une complète dématérialisation:
- le mécanisme de paiement des chèques est bien compris par le grand public, qui l'utilise majoritairement en France.
- les chèques sont potentiellement moins chers, notamment pour les commerçants, car il n'y a pas de commission à payer comme pour les transactions par carte.

Toutefois, cet instrument de paiement est loin derrière les autres solutions de paiement sécurisé en matière de développement du commerce sur Internet.

---

[33] On peut espérer que les lecteurs de carte à puce pourront lire à la fois les cartes bancaires et les PME.

[34] D'après Gemplus, conférence IIR sur les " Cartes Prépayées ", Paris, 1998.

[35] L'avantage essentiel de ce langage de programmation est sa " portabilité ". En effet, les logiciels construits sur des langages classiques, comme le C, sont utilisables par un type particulier de machine (PC sous Windows 95 par exemple). Avec Java, on programme pour une machine " virtuelle ", et c'est ensuite l'ordinateur qu'on utilise qui traduit le code de la machine virtuelle dans son propre langage. Ainsi, des applications existantes en Java (applications financières pour PC par exemple) peuvent déjà fonctionner sur des Javacards.

2.3. Les stratégies des acteurs du e-commerce en matière de paiement

Afin d'analyser les stratégies des acteurs du commerce électronique, nous établirons tout d'abord un bilan du marché français, puis nous étudierons les conséquences de l'arrivée de nouveaux entrants sur le secteur bancaire.

2.3.1 Un marché fragmenté

Afin de dresser un état du marché français, nous nous sommes référés à l'annuaire le Web Marchand[36] qui répertorie les sites français de commerce électronique.
En août 1998, sur les trois cent quarante trois sites Web français, seulement 40% autorisent une transaction en ligne intégrale, et un tiers d'entre eux n'offre aucune sécurisation. Pour les deux tiers restants, la répartition entre les systèmes de paiement est la suivante :

- 39 % pour SSL (sans intermédiaire, via un logiciel de serveur Web)
- 10% pour Payline
- 5% pour Kléline
- 3% pour C-SET

Cette étude montre tout d'abord que le marché français est très fragmenté, puisque le leader des solutions de paiement SSL n'en représente que 39%, et que les quatre principales solutions ne totalisent que 57% des solutions existantes sur le marché.

Tout d'abord, on peut se demander pourquoi SSL domine encore le marché français, malgré les insuffisances de ce système en matière de sécurité. Cet état est dû à deux raisons : il est simple à utiliser, et les entreprises hésitent à investir dans une technologie qui n'est pas encore un standard (on a un effet de rendement croissant d'adoption). En revanche, le faible pourcentage obtenu par C-SET s'explique par le fait que cette solution n'est qu'au stade de l'expérimentation.

De plus, la position des solutions de paiement dans ce classement ne dépend pas uniquement de la qualité de ces systèmes mais également du rôle de prescripteur que jouent les sociétés de services informatiques et notamment celles qui hébergent des sites Web. Par exemple, 39% des sites marchands hébergés par FranceNet ont préféré SIPS à PayLine, le plus souvent sur la recommandation de la société de service ayant réalisé le site, alors que ces deux solutions sont équivalentes en terme de sécurisation et de services offerts.

D'autre part, on observe actuellement un développement des approches fédératrices (SET, C-SET, ou les portes monnaies électroniques) par rapport aux approches propriétaires (comme Kléline, CyberCash, ou Digicash). Ce retournement de tendance a plusieurs origines. Tout d'abord, la nécessité de définir et de promouvoir un standard à l'échelle internationale. Ensuite, l'importance des investissements à réaliser dans un tel projet, dont la rentabilité est incertaine et lointaine. Enfin, l'arrivée de Microsoft sur ce marché avec sa proposition de standard, afin de toucher une commission sur chaque transaction, a effrayé les fournisseurs de service de paiement et les a incités à s'unir d'avantage. Cependant, ces approches fédératrices n'ont pas encore dépassé le stade de l'expérimentation.

Ce retournement de tendance pose le problème de la viabilité des approches propriétaires, lesquelles sont handicapées par la difficulté d'atteindre une masse critique d'utilisateurs, et par la complexité de leur mode de fonctionnement. En effet, tant qu'une solution de paiement n'a pas été adoptée par de nombreux clients, il y a peu d'intérêt pour les commerçants de la choisir. Et inversement, si le moyen de paiement est proposé par un faible nombre de commerçants, les clients sont peu enclins à utiliser ce type de solution compliquée (un logiciel spécifique doit être installé). Cela pose le problème des externalités de réseau. On peut citer l'exemple de Kléline qui rencontre des difficultés d'implantation à l'étranger.

[36] www.web-marchand.com

2.3.2 Conséquences sur le secteur bancaire

L'Internet est pour les banques une source de risques et d'opportunités. L'arrivée de nouveaux entrants sur le marché des moyens de paiement remet en cause leur position. Dans le but d'analyser l'impact de cette nouvelle concurrence, nous aborderons tout d'abord les enjeux pour le secteur bancaire, puis le problème de la création monétaire.

Les enjeux

Les enjeux du paiement sur Internet sont de trois ordres : stratégique, marketing et technologique. Stratégique car les systèmes de paiement sur Internet remettent en cause la position des banques et à ce titre apparaissent comme une modalité privilégiée d'entrée sur ce marché pour des agents non bancaires. Marketing car le nouveau mode de servuction qu'ils définissent correspond à de nouveaux positionnements fondés sur de nouveaux moyens de paiement pour les clients en même temps que l'adéquation avec les solutions de paiements existantes comme la carte bancaire. Technologique parce que les investissements nécessaires sont d'abord technologiques et doivent être compatibles avec les systèmes actuels de paiement inter-bancaires pour permettre les opérations de compensation et de règlements entre systèmes.

a) L'enjeu stratégique

L'impact d'Internet est de deux types : il modifie les relations existantes avec la clientèle, soit en les renforçant, soit les détruisant et il modifie les compétences requises des personnels[37]. L'obtention de la masse critique en termes de clients, nécessaire pour rentabiliser un système de paiement, requiert une analyse critique de la stratégie actuelle et future. Il faut du temps pour que cette masse soit atteinte et elle requière un suivi détaillé[38].
Internet apparaît ainsi comme un moyen privilégié pour les nouveaux entrants d'accéder au marché de la gestion des moyens de paiement. L'avantage concurrentiel peut être fondé sur la possession d'un réseau, sur l'accès à la clientèle ou la connaissance de la clientèle. Or ces entrants ne sont pas faciles à identifier en raison des sources multiples.

Cependant, nous proposons de les regrouper en quatre catégories :

1. Les entreprises (en particulier les SSII, et les gérants de systèmes de billetterie[39]). Les ressources de ces entreprises résident dans leur connaissance technologique et de l'industrie, ainsi que dans leurs relations.
2. La grande distribution : leurs ressources sont des fonds importants, la possession de réseaux, leur connaissance des clients et l'accès à ces derniers.
3. Les gestionnaires de réseaux E.D.I. : les gestionnaires de réseaux E.D.I. sont des concurrents potentiels. Ils maîtrisent les infrastructures et les informations circulant sur le réseau[40]. C'est là que réside leur avantage.
4. Les fournisseurs d'accès à Internet ou de contenu sur Internet : l'avantage concurrentiel des fournisseurs d'accès réside à la fois dans l'accès et la connaissance de leur clientèle d'abonnés. En revanche, les fournisseurs de contenu essayent de créer des points de passage indispensables pour les internautes, les "portails" (exemple : un moteur de recherche, ou encore une communauté virtuelle), et proposent sur ces sites de nombreux services. Leur avantage s'appuie sur la connaissance des utilisateurs de leurs services. Certaines banques cherchent d'ailleurs à devenir des fournisseurs de contenu. Par exemple, UFB Locabail, filiale de Paribas, a développé une communauté virtuelle destinées aux industries graphiques. L'objectif de cette initiative est de devenir le plus rapidement possible le site de référence de cette filière professionnelle, en proposant à ses membres des services d'informations gratuits, et transactionnels (bancaires ou non). Les communautés

---

[37] ABERNATHY W.J., CLARK K.B., " Comment établir une carte stratégique des innovations dans un secteur industriel ", 1988, *Culture et technique*, mars, n°18.

[38] Le problème de la masse critique renvoie aux externalités de réseaux indirectes. La masse critique de clients à atteindre est d'autant plus importante que les coûts fixes sont élevés. L'utilité pour un client est fonction du nombre de clients total qui joue sur les services proposés. On pourra aussi distinguer entre l'effet de parc lié aux équipements disponibles et l'effet de contenu lié aux services proposés.

[39] On peut citer l'exemple la RATP, qui cherche à renouveler son système de billetterie. Dans ce but, cette société teste actuellement une carte à puce, appelée "Passe", comme moyen de contrôle pour passer les portillons automatiques et accéder à son réseau. Cette carte peut également servir de PME.

[40] Une des fonctions offertes par les réseaux E.D.I. est le stockage des messages sur un site différent de l'émetteur et du récepteur pour conserver une trace du message.

virtuelles apparaissent ainsi aux entreprises qui les ont initiées ou fédérées comme le moyen d'instaurer une barrière à l'entrée pour un type de marché.

Tableau 1 : Les nouveaux concurrents des banques selon les marchés

	MARCHES	
FONCTION	Les entreprises	Les ménages
Gestion des moyens de paiement	*Gestionnaires de réseaux E.D.I.*	*Grande distribution* *SSII* Fournisseurs d'accès ou de contenu

L'étude des nouveaux entrants sur le marché de la gestion des moyens de paiement montre que la concurrence est plus vive sur le segment de marché des ménages. En particulier pour les micro-transactions, de nombreuses solutions de porte-monnaie électronique sont expérimentées actuellement (une vingtaine en Europe). Ces systèmes fondés sur des cartes à puce, mais sur des standards différents sont incompatibles entre eux. Cette compétition amène chaque entrant à proposer sa carte, alors que justement, pour améliorer la rentabilité de ces cartes, il est nécessaire d'y loger des applications multiples. Cela nécessite la conclusion de partenariats entre ces acteurs. On assiste d'ailleurs actuellement à un début de convergence entre les systèmes de PME, mais plutôt sous l'impulsion des pouvoirs publics.

Un autre enjeu majeur est lié aux pertes commerciales subies par les commerçants à cause du manque de sécurisation des transactions. En effet, comme les commerçants n'ont pas encore la possibilité d'identifier leurs clients, ces derniers peuvent contester leurs achats par carte bancaire. En Europe, 47% des litiges liés à la carte bancaire concernent Internet, alors que ce média pèse moins de 1% des transactions par carte[41]. Cela n'inquiète pas les banquiers pour deux raisons. D'une part, parce que les litiges portent sur des petits montants, et d'autre part, car le risque est assumé par le commerçant. Les banquiers cherchent donc juste à minimiser le coût de traitement des réclamations. C'est pourquoi certaines banques, à l'image du Crédit lyonnais, préfèrent automatiser ce type de procédure sans vérifier la bonne foi du client. La résolution de ce problème revient à se demander qui, du commerçant ou de la banque, doit assumer le risque de non-paiement.

La réponse à cette question est vitale pour le développement du commerce électronique. Le "Livre Blanc de la CEE[42]"' affirme que pour assurer la sécurité d'un système de paiement, les organisations qui exploitent ce système (banques, opérateurs de carte…) doivent avoir la responsabilité légale et financière des erreurs et des faiblesses du système.

Enfin, pour la France, un enjeu spécifique est de développer l'usage des cartes à puce dans la "vie réelle" et sur Internet, afin de préserver et d'exploiter l'un de ses rares points forts dans les technologies de l'information (T.I.C). Rappelons que Gemplus est le leader mondial dans les cartes à puce.

b) L'enjeu marketing

Les enjeux marketing sont importants. Internet présente un risque très grand de banalisation de l'offre des moyens de paiement. La gestion des moyens de paiement sur Internet correspond à un mode spécifique de servuction qui remet en cause les stratégies traditionnelles des banques. De plus, afin de différencier, les gestionnaires de cartes bancaires comme Visa ou Mastercard mettent en place des accords de cobranding avec des "portails". Visa a sorti en février dernier, une carte de crédit Visa-Yahoo. Cette carte est diffusée par le spécialiste américain des cartes de crédit First USA. Elle donne également accès à des programmes de fidélisation auprès de certains cybermarchands (comme Amazon, CD Now…).

c) L' enjeu technologique

L'évolution rapide des T.I.C. et leur traduction en de nouvelles applications nécessitent qu'on réfléchisse à leur intégration à l'existant. A l'image du secteur bancaire, il est clair que des accords entre fournisseurs de service de paiement sont nécessaires afin de permettre des opérations de compensation et de règlement entre les différents systèmes de paiement.

41 C. Maussion, "Le cybercommerce pousse à la fraude", Libération, 4 mai 1999.

42 ebusiness-europe.com/Public/CEE/Chapitre9.html

Cela suppose que ces acteurs s'entendent au niveau des normes techniques à respecter[43] (formats de donnée des informations transmises, sécurisation, logiciels). Dans le cas contraire, il y a un risque d'émiettement du système de paiement national. On peut observer ce phénomène dans certains pays où les cartes bancaires (sauf en France grâce à l'interbancarité) sont cantonnées à des usages spécifiques.

Le problème de la création monétaire

Lorsqu'on s'intéresse à la monnaie électronique, et à la possibilité pour des agents économiques non financiers d'en émettre, très rapidement se pose la question de la création monétaire. Dans les économies de marché financier, le régime monétaire repose d'une part sur le cours légal et forcé de la monnaie, et d'autre part sur la création de cette monnaie par les institutions de crédit, lesquelles sont contrôlées par la banque centrale (par des mécanismes de réserves obligatoires et les taux directeurs), qui est prêteur en dernier recours.

Tout d'abord, il convient de définir à quel moment il y a création monétaire. Dans ce but, on peut s'appuyer sur l'exemple des cartes privatives du commerce (la carte Pass de Carrefour, la carte Cofinoga commune aux Nouvelles Galeries, aux Galeries Lafayettte, et au BHV, la carte Kangourou de la Redoute, etc.). Si elles sont utilisées comme des instruments de paiement, ces cartes ne créent pas de la monnaie. En revanche, à partir du moment où il y a un crédit, il devient difficile de distinguer cette opération de la vraie monnaie.

Il en est de même pour la monnaie virtuelle. Si cette monnaie est adossée à la monnaie scripturale bancaire, c'est-à-dire lorsque l'ouverture d'un compte en monnaie virtuelle nécessite pour contrepartie un débit sur le compte bancaire du client, alors il n'y a pas de création monétaire sur l'Internet. Actuellement, les solutions proposées reposent sur ce principe d'adossement. Cependant, il est possible que certains fournisseurs de service de paiement électronique, en proposant des formules de crédit à leurs clients, se mettent à créer une quantité de monnaie électronique supérieure à leurs dépôts en monnaie bancaire. Dans ce cas, il y a alors création monétaire. Les conséquences directes sont la perte du contrôle de la création monétaire par les banques centrales, et le risque de faillite de l'émetteur, ce qui peut fragiliser l'ensemble du système monétaire d'un pays (risque systémique).
Afin d'éviter tout risque de faillite, il est nécessaire d'une part que des accords de coopération entre les fournisseurs non bancaires et les banques interviennent (pour les règlements internationaux notamment), et d'autre part qu'ils aient l'obligation de détenir des disponibilités suffisantes pour honorer les demandes de paiements de leur clients.

CONCLUSION

La multiplicité des offres et l'absence d'un standard se traduisent par un marché très fragmenté des systèmes de paiement électronique, dominé par SSL, et un comportement attentiste des entreprises qui hésitent à investir. On peut s'interroger sur les conséquence d'un tel comportement pour l'ensemble du secteur. Le risque est que des solutions promues par les banques françaises (comme C-SET) ne deviennent jamais un standard.

Toutefois, il semblerait que SET, soutenu par les émetteurs de cartes Visa et Mastercard, de grandes banques, et des gestionnaires de réseau comme IBM puisse devenir rapidement un standard pour les transactions à base de carte bancaire.
Par contre, en ce qui concerne les micro-paiements, l'avenir est plus incertain. Le concurrent principal des approches propriétaires est le porte-monnaie électronique, lequel est handicapé par l'obligation faite au client de posséder un lecteur de carte pour être utilisé sur Internet.

Par ailleurs, un autre enjeu majeur apparaît celui de la convergence entre les solutions de paiements et de banque électroniques. Le commerce électronique et la banque sur Internet sont actuellement traités comme des sujets différents. En effet, les solutions de banque à distance via Internet se focalisent sur le fait de fournir aux clients un accès à leur compte au travers d'Internet (relevé de compte, virement entre deux comptes, achat/vente de titres). Or il y a aucune raison qui justifie que les consommateurs utilisent deux systèmes complètement différents sur Internet pour accéder à leur compte et pour réaliser des paiements électroniques.

[43] La bagarre technologique oppose principalement les deux géants américains : Visa (avec la JavaCard) et MasterCard (avec Multos).

TYPOLOGIE DES SYSTEMES DE PAIEMENT ELECTRONIQUE

Catégorie	Système de paiement	Gestionnaire du système	Sécurité	Mode de paiement	Numéro de carte bancaire stocké par	Interro-gation en ligne (*)	Révoca-tion
Monnaie électronique	**Monnaie virtuelle**						
	Cyberbuck	Digicash	logicielle	prépaiement	pas de stockage	oui	non
	PME:						
	Proton	Banksys	matérielle	prépaiement	pas de stockage	non	non
	Mondex	Mondex International Ltd	matérielle	prépaiement	pas de stockage	non	non
	VisaCash	Visa	matérielle	prépaiement	pas de stockage	non	non
	Passe	RATP	matérielle	prépaiement	pas de stockage	non	non
	PMV:						
	Klebox (micro-paiement)	Kléline	logicielle	prépaiement	Kléline	non	non
Paiement par carte bancaire	**Protocole SSL:**						
	Logiciel de serveur web	sans intermédiare	logicielle	débit / crédit	le marchand	non	oui
	Telecommerce	France Telecom	logicielle	débit / crédit	France Telecom	oui	oui
	Payline	Experian-INTRINsec	logicielle	débit / crédit	Experian-INTRINsec	option	oui
	SIPS	Atos	logicielle	débit / crédit	Atos	oui	oui
	Klebox	Kléline	logicielle	débit / crédit	Kléline	oui	oui
	SET	Visa, Mastercard,IBM …	logicielle	débit / crédit	pas de stockage	oui	non
	C-SET	GIE carte bancaire	matérielle et logicielle	débit / crédit	pas de stockage	oui	non
Paiement par chèque	ChekFree	ChekFree Corporation	logicielle	débit / crédit	pas de stockage	oui	non
	NetChex	Net1 Incorporated	logicielle	débit / crédit	pas de stockage	oui	non

(*) du serveur du gestionnaire du système de paiement ou du réseau carte bancaire (pour les paiements par carte bancaire)

BIBLIOGRAPHIE

Alberganti M. " L'argent virtuel s'utilisera presque comme l'argent physique ", Le Monde, 18 juin 1997

Alberganti M., " La France lance un porte-monnaie électronique sur Internet ", Le Monde, 26 septembre 1996

Alberganti M., " Le Passe sans contact de la RATP devient porte-monnaie électronique ", Le Monde, 19 mars 1998

Bresse P., Beaure d'Augeres G., & Thuillier S., " Paiement numérique sur Internet ", International Thompson Publishing, 1997

Rapport du CNCT « Problèmes liés à la dématérialisation des moyens de paiement et des titres », mai 1997, documentation française

Espagnon,M, « Le paiement d'une somme d'argent sur Internet », J.C.P,G, p.787,1999

Faraggi B., " Commerce électronique et moyens de paiement ", Dunod, Paris, 1998

Ferret B., " Internet relance la carte à puce ", Internet professionnel n°6, février 1997

Guttman R., " Cybercash : the implications of a new money form ", *working papers*. University of Paris-Nord, 1997

Humphert D.B., Pulley L.B. & VESALA J.M., " Cash, paper and electronic payments : a cross-country analysis ", *Journal of money, Credit and Banking*. Vol.28, n°4, p.914-939, 1996

Huet, J , « Aspects juridiques du télépaiement »,J.C.P, G,1991,p.324

Kosiur D., " Comprendre le commerce électronique ", Microsoft Press. 1997

LACKER J.M., " Stored value cards : costly private substitutes for government currency ", *Federal Reserve Bank of Richmond Economic Quartely*, Vol.82/3 (Summer), p.1-25, 1996

LACKER J.M. & SCHREFT S.L., " Money and credit as means of payment ", *Journal of Monetary Economics*, Vol.38, p.3-23, August 1996

MARIMON R., " Electronic money : the end of inflation ? ", discussion paper 122. Institute for Empirical Macroeconomics, *Federal Reserve Bank of Minneapolis*, August 1997

McKie M.. & White K., " Evaluating and selecting digital payment mechanisms ", in Rosston, G.L. et Waterman D. (Eds) *Interconnexion and the Internet*, 1997

McKnight Lee W, " Internet Economics ", edited by Lee W. McKnight and Joseph P. Bailey. - London : MIT, 1997

Nakayama Y., Moribatake H., ABE M., & FUJISAKI E., " An electronic money scheme ", IMES discussion paper series. *Institutes for monetary and economic studies*. Bank of Japan, 1998

Okawa M. & Van der Bergh P., " Monnaie économique : implications pour les autorités ", Banque n°589, février 1998

Picory C., *Electronic commerce, industrial organization and financial issues*. Report for the G7 Pilot Project n°10 " A global marketplace for the SMEs " Esprit network of Excellence Working group n°22454 Contributing to the EU definition of the G7 Pilot Project n°10 G7 WG., 1997

Pothier, I, « la preuve dans les transactions financières à distance », revue Banque,n°568,p.70 ;1996

Prideaux J., " Les cartes des années 2000 ", Banque n°584, Septembre 1997

Radeck L.J. & Weinninger J., " Paying electronic bills electronically " Current Issues in economics and finance, January 1998

Radoux Y., " Le paiement sur réseaux ouverts ", Banque n°586, Novembre 1997

Reboul P., " Les systèmes de paiement électronique ", Internet Professionnel n°6, Février 1997

Salzman C., " Les enjeux de la monnaie électronique ", Problèmes économiques n°2.524, 11 juin 1997

Sedallian, V, « Les problèmes juridiques posés par la légisaltion française en matière de chiffrement », DIT 98/4.

Sitruk H., " Enjeux européens de la carte bancaire ", Banque n°578, Février 1997

Vasseur M., "le paiement électronique-Aspects juridiques", Revue Banque, p.3207, 1987.

Yepes C. & Demarolles A., " La monnaie électronique aux Etats-Unis ", Problèmes économiques n°2.553, 28 Janvier 1998

SITES INTERNET

" A survey of existing e-commerce solutions ",
adresse : http ://www.internet-banking.com/ecom.html

" Becoming a Visa Merchant ",
adresse : http ://www.visa.com/fb/merch/become/main.html

" Cybercash ",
adresse : http ://www.internet-banking.com/ecommerce/cybercsah.htm

" E-commerce, digital currency ",
adresse : http ://www.internet-banking.com/ecommerce/digsummary.html

" Electronic (Credit Card) Payment Systems ",
adresse : http ://www.internet-banking.com/ecommerce/elecsummary.html

" Electronic Money ",
adresse : http ://www.emich.edu/public/coe/nice/rlece1.html

" Environnement insuffisamment favorable à la création et à l'utilisation des nouvelles techniques d'information et de communication ",
adresse : http ://www.tregouet.org/senat/ntic/original/Tome1-Fcontents.html

" Kleline et ses partenaires ",
adresse : http ://www.kleline.fr/FR/kleline/securite.html

" La sécurité ",
adresse : http ://www.galilee.sat.sligos.fr :85/securite.htm

" Paiement sécurisé ",
adresse : http ://www.alternetive.asso.fr/securite/payment.htm

“ Paiements sur Internet ”,
adresse : http ://www.cyberstrat.net/cyberstrat/Paiements_par_Internet/paiements.htm

“ The effect of Internet value transfer systems on monetary policy ”,
adresse : http ://www.econwpa.wustl.edu :8089/eps/mac/papers/9607/9607004.html

“ Shop Online : SET ”,
adresse : http ://www.mastercard.com/shoponline/set/