L'ÉCONOMIE DE LA SÉCURITÉ DES PAIEMENTS EN LIGNE

CHARLES GOLDFINGER *

Dans toutes les discussions et analyses du commerce électronique et des paiements en ligne, la sécurité des transactions apparaît comme le problème critique. Pourtant, il ne semble pas que l'on ait beaucoup progressé pour l'élucider. Les discussions restent marquées par de forts désaccords et, surtout, par une grande confusion sur la nature et la gravité du problème. La sécurité constitue-t-elle un obstacle à l'essor du commerce électronique et à son acceptation par les consommateurs ? Les paiements en ligne sont-ils moins sûrs que d'autres systèmes de paiement ? Quels sont les risques que les paiements en ligne engendrent pour les systèmes de paiement, leurs opérateurs et les autorités de surveillance ? Quelles sont les approches qui permettraient d'accroître la sécurité et de réduire les risques ? Sur ces questions, les avis restent partagés, voire polarisés. Plus grave encore, l'écart entre les positions officielles et l'évolution du marché ne fait que s'accroître. Les autorités insistent sur l'étendue du problème, certains spécialistes allant jusqu'à affirmer qu'« aujourd'hui, la sécurité des paiements sur Internet n'existe pas »[1]. À l'appui de ces affirmations, ils citent des statistiques alarmantes sur l'étendue de la fraude sur Internet ainsi que de nombreuses enquêtes d'opinion qui montrent que les consommateurs considèrent l'absence de sécurité comme la raison principale de leur réticence à effectuer des achats sur Internet. En même temps, dans un climat économique maussade, le commerce électronique, tant du côté du grand public (Business-to-consumers - B2C) que celui de l'inter- entreprise (Business-to-business - B2B) continue de croître rapidement. Ainsi, selon Forrester Research, les achats en ligne des consommateurs européens lors de la période de Noël ont progressé

* Directeur général de Global Electronic Finance, société de conseil spécialisée et auteur de plusieurs livres sur la nouvelle économie

de plus de 85 % en 2002 par rapport à 2001, pour atteindre 7,6 Md€. Aux États-Unis, la croissance était moins forte mais néanmoins significative, 15 %, et le montant des ventes en ligne pour la même période était de 9,4 Md€.

Il y a donc un paradoxe de la sécurité des transactions en ligne : on reconnaît qu'elle constitue un problème important, mais cette reconnaissance n'a pas empêché le commerce électronique de connaître un grand succès et de devenir un phénomène de masse. Il y a aussi un paradoxe connexe, concernant les paiements en ligne : alors que ceux-ci ont été souvent considérés comme un domaine privilégié de l'innovation dans le commerce électronique voire une *killer application*, les différents projets et initiatives ont pour la plupart échoué.

Dans ce papier, nous cherchons à apporter des éléments d'explication à ces paradoxes et à clarifier les termes du débat. Pour ce faire, nous allons aborder la sécurité sous l'angle de son économie. Notre postulat de départ est que la sécurité n'est pas un bien absolu mais un attribut relatif d'une transaction. Elle est valorisée par rapport aux autres attributs, tels la rapidité, la convivialité d'usage ou la facilité du suivi. Le consommateur est prêt à payer un certain prix non pour chaque attribut séparément mais pour l'ensemble. Or, ce qui change dans le monde virtuel, c'est leur positionnement. La sécurité devient plus visible et apparaît dissociée d'autres attributs, ce qui amène les opérateurs des systèmes virtuels à demander un paiement spécifique. Les consommateurs ne sont guère réceptifs à cette idée. Plus fondamentalement, ils ne valorisent pas la sécurité de la même manière que les opérateurs. En effet, la sécurité est un bien de réseau (*network good*), avec de fortes externalités de consommation. Il y a donc une différence entre son coût privé (pour chaque consommateur) et son coût social d'ensemble. Cette différence est difficile à capter directement et à éliminer, ce qui explique les contradictions du comportement des consommateurs, ainsi que les appréhensions des opérateurs et des autorités réglementaires.

Ainsi, nos conclusions sont les suivantes :

- la sécurité ne constitue pas un facteur déterminant pour le consommateur de services en ligne. Il n'est pas prêt à la payer plus cher (directement ou indirectement) que la sécurité des transactions financières classiques ;
- les spécificités de la sécurité des paiements sur Internet posent des défis majeurs aux opérateurs de systèmes et aux autorités de réglementation. Ces défis concernent d'une part l'économie de la sécurité et d'autre part, la transition vers une nouvelle architecture des systèmes basée sur l'environnement Internet.

Le plan de l'article est le suivant. Nous allons d'abord discuter les caractéristiques spécifiques de la sécurité des systèmes de paiement en ligne, par rapport aux systèmes « classiques ». Ensuite, il nous paraît

instructif de mieux comprendre la dynamique d'ensemble des paiements en ligne et notamment les raisons de leur faible taux de réussite. Après, nous allons analyser les attitudes des consommateurs et des opérateurs vis-à-vis de l'économie de la sécurité, notamment la réticence des premiers à en payer le coût. En conclusion, nous allons présenter les défis que la sécurité pose aux opérateurs et aux autorités de réglementation.

LES PAIEMENTS EN LIGNE : L'HYPERBOLE ET LA RÉALITÉ

Peut-on avoir le moindre doute que la sécurité des paiements en ligne est bien moindre que celle des paiements « traditionnels » ? Les données sont apparemment sans appel. Ainsi, selon Gartner, la société d'études réputée, en 2001 les pertes provoquées par la fraude sur les transactions en ligne ont été vingt fois plus élevées que les pertes dues à la fraude « traditionnelle ». Elles représentaient un montant de plus de 700 M$, 1,14 % de la valeur des ventes en ligne. Plus de 5 % des consommateurs ont été victimes d'une fraude sur leur carte de crédit et près de 2 % ont eu leur identité volée. On estime qu'en 2002, l'ensemble des commerçants en ligne aux États-Unis a subi un préjudice dû à la fraude de l'ordre de 3 % de leur chiffre d'affaires (2,5 % pour Amazon)[2]. Ce pourcentage est resté stable par rapport à 2001 mais a baissé en comparaison à 2000 (où il était de 4 %).

En Europe, les contestations des achats en ligne par les consommateurs (*chargebacks*) ont représenté près de la moitié du total des *chargebacks*, alors que les achats en ligne n'en constituent que 4 % de l'ensemble.

Au vu de ces statistiques, est-il surprenant que pour de nombreux analystes la fraude est la plus grave menace pesant sur le commerce électronique en ligne et que les enquêtes auprès des consommateurs montrent régulièrement que la sécurité représente une préoccupation sérieuse pour ceux qui achètent en ligne ?

Et pourtant, malgré ce canevas apocalyptique, le commerce électronique connaît un essor extraordinaire, ce qui suggère, qu'aussi bien pour les commerçants que pour les consommateurs, les avantages sont supérieurs aux risques. Dès lors, l'appréciation du problème doit peut-être être nuancée. Il faut ainsi prendre en compte l'effet d'hyperbole qui affecte tout ce qui touche à Internet : paré de toutes les vertus lors de sa montée, le commerce électronique a été chargé de tous les vices lors de sa descente. Cet effet est amplifié par sa jeunesse et sa nouveauté, donc le manque de précédents et d'expérience de nombreux acteurs, et plus encore par le succès même du commerce électronique : sa croissance débridée a forcé le développement et le déploiement rapides de solutions

ad hoc dont la robustesse ne pouvait être testée exhaustivement, compte tenu des délais de mise en œuvre. Ces solutions étaient souvent complexes, entraînant la confusion chez les commerçants et les consommateurs, et donc augmentant les risques d'erreur et d'exaspération.

Les statistiques citées doivent aussi être interprétées avec une certaine prudence. Prenons le cas de *chargebacks*. Ceux-ci étaient très concentrés dans un secteur, celui de la pornographie. Les marchands de la chair virtuelle utilisent de nombreux subterfuges pour obtenir les numéros de carte. De leur côté, les consommateurs hésitent souvent à reconnaître leurs plaisirs numériques. Or, la pornographie représente probablement[3] le secteur le plus important du commerce électronique, indubitablement plus profitable, et donc le plus actif sur le plan transactionnel. Il n'est pas sûr qu'en dehors du secteur « adulte », l'incidence des *chargebacks* dans le commerce sur Internet soit plus importante que dans d'autres formes du commerce à distance, la vente par correspondance, par courrier, par téléphone ou par des systèmes télématiques comme le Minitel.

Or, ce sont ces formes, plus que le commerce traditionnel en dur, qui constituent l'univers de référence du commerce en ligne. Le dispositif de sécurité pour le commerce à distance par téléphone ou par Minitel est souvent qualifié de rudimentaire. Pour autant, ces supports ne sont pas considérés comme des foyers d'insécurité. Au contraire, dans la longue histoire du minitel, il n'y a pas eu de cas de fraude majeure imputable à la technologie. Même si des comparaisons détaillées manquent, il n'apparaît pas qu'Internet soit moins sûr que le téléphone ou le Minitel. On pourrait même affirmer qu'il offre, du moins potentiellement, un niveau de sécurité supérieur. En effet, les outils de protection de l'échange et des données (notamment diverses applications de cryptage) qui font partie de la panoplie Internet, ne sont pas non plus facilement disponibles ou intégrables sur d'autres supports.

On peut formuler une autre remarque concernant les comparaisons des statistiques de sécurité. Il n'est pas sûr que les données soient totalement comparables. En effet, les données sur la sécurité des paiements en ligne les plus souvent citées couvrent toutes les transactions contestées ou invalidées, y compris celles qui sont dues à l'erreur humaine (du client ou du commerçant), les problèmes logistiques, les vulnérabilités technologiques... Ces données sont rapprochées des statistiques de fraude sur les cartes de crédit dans le commerce traditionnel. Or, non seulement ces statistiques n'incluent pas tous les incidents de paiement, mais surtout ne couvrent qu'un instrument de paiement. Or, si plus de 95 % des transactions en ligne sont payées par une carte de crédit, ceci n'est pas le cas pour les transactions traditionnelles où d'autres instruments tels le chèque ou le cash sont utilisés aussi souvent.

Ainsi, en France, la carte (débit et crédit) représente un peu moins d'un tiers des transactions de détail. Les banques encouragent l'usage plus intensif de la carte, précisément parce qu'elle est plus sûre que les autres instruments. Si l'on veut comparer réellement la sécurité des paiements en ligne avec celle du commerce traditionnel, il faut la mesurer contre les incidents et la fraude sur l'ensemble des instruments de paiement utilisés dans celui-ci. Sans vouloir préjuger des résultats d'une telle comparaison, on peut penser qu'elle sera moins défavorable aux paiements en ligne que les comparaisons utilisées actuellement.

L'objectif de ces observations n'est pas de nier le problème de la sécurité des paiements en ligne, mais de le ramener à ses justes dimensions, celles d'un problème sérieux mais pas catastrophique ou épidémique.

Le problème est sérieux, tout d'abord parce que toutes les transactions à distance sont plus risquées et incertaines que les transactions face à face. Il faut authentifier aussi bien le consommateur que le commerçant. Ni l'objet de la transaction ni les instruments de paiement ne peuvent être physiquement et simultanément appréhendés par les parties concernées. Le décalage entre la livraison et le paiement est inhérent à la transaction à distance et ne peut pas être éliminé.

À ces risques communs à toutes les formes de commerce à distance, internet ajoute des risques spécifiques. Il dématérialise encore davantage la transaction. Internet dissocie l'infrastructure physique du réseau de communications : le cheminement d'un message n'est jamais déterminé à l'avance. Ce qui veut dire que dans l'environnement Internet, le moyen classique de protection, à savoir la séparation physique des communications sensibles à travers des lignes dédiées, n'est plus applicable. Alors que la plupart des systèmes de transactions à distance sont nationaux, Internet est global et traverse allègrement les frontières. Contrairement à l'idée extrêmement répandue qu'il est le vecteur de la désintermédiation, Internet renforce le besoin d'intermédiation. Sa chaîne transactionnelle est plus complexe et implique de nouveaux participants, tels les portails et les agrégateurs de contenu. Sa technologie est ouverte et standardisée, ce qui veut dire largement accessible et donc apparemment facile à répliquer. Mais la notion du réseau ouvert va bien plus loin. Dans un réseau classique, chaque utilisateur est facilement identifié et lié à l'opérateur par un ensemble de relations (contrat d'abonnement, facture...). Internet est le réseau des réseaux, où les relations classiques coexistent avec des rapports beaucoup plus flexibles, occasionnels et sans liens contractuels. Ainsi un abonné aux services d'un FAI comme Wanadoo ou AOL peut accéder à des services qui ne font pas partie de son abonnement et, inversement, quelqu'un qui n'est pas abonné peut néanmoins butiner sur le site de Wanadoo ou d'AOL.

Les concepts d'abonné et d'utilisateur ne sont plus synonymes et les concepts eux-mêmes changent profondément de nature. Ainsi, Yahoo affirme avoir plus de 200 millions d'utilisateurs, mais sur ceux-ci, 1 % seulement, 2 millions, utilisent les services payants et quelque 93 millions se sont enregistrés sans payer.

L'Internet constitue un mélange déroutant entre systèmes et structures traditionnels, d'une part, et systèmes et structures innovants voire inédits, d'autre part. C'est ce mélange qui requiert une approche spécifique de la sécurité. Celle-ci doit mettre l'accent sur l'authentification qui comporte plusieurs étapes. Dans le monde Internet, il convient de s'assurer que les parties à la transaction sont bien celles qu'elles affirment être. Il faut vérifier et garantir leur identité. Ensuite, il faut authentifier leurs messages concernant la transaction, c'est-à-dire confirmer que ces messages n'ont pas subrepticement été modifiés lors de la transmission. Cet ensemble de procédures constitue ce que l'on appelle l'infrastructure de confiance, qui doit fonctionner à très grande échelle et en temps réel, d'une manière transparente pour l'utilisateur. Son développement et déploiement posent d'énormes défis conceptuels et technologiques. Pour que l'infrastructure de confiance soit réellement efficace, il faudrait qu'elle soit étroitement, voire organiquement, intégrée à l'Internet. Mais une telle intégration est difficile. Alors que le protocole TCP/IP est une norme mondiale universellement acceptée rendant les réseaux Internet réellement interopérables, il n'y a pas de consensus comparable sur les normes d'authentification, et plus particulièrement sur les techniques de cryptage. Les techniques traditionnelles, testées et aguerries à l'usage, ne sont pas adaptées aux réseaux ouverts dans la mesure où elles fonctionnent sur le postulat que les parties à la transaction électroniques se connaissent au préalable. De nouvelles techniques ont été inventées depuis la Seconde guerre mondiale pour pallier ce défaut et permettre des transactions sécurisées entre les interlocuteurs qui ne se connaissaient pas avant. Ces techniques font appel à la méthodologie de la clé publique. Celle-ci est très séduisante sur le plan conceptuel, mais, sur le plan opérationnel, elle est encore loin d'être complètement rodée. Elle peut être instrumentée de plusieurs manières, qui ne sont pas nécessairement interopérables entre elles. Sa mise en œuvre est alambiquée, reposant sur une hiérarchie de certificats et de clés qui s'emboîtent les uns dans les autres un peu comme les poupées russes. Elle est aussi complexe pour l'usager final, qui doit, soit disposer d'un moyen d'accès dédié comme une carte à puce, soit maîtriser des procédures lourdes qui prennent beaucoup de temps et de puissance de calcul. Pour compléter ce tableau des difficultés, ajoutons des obstacles réglementaires. Dans de nombreux pays, notamment aux États-Unis, la clé publique est assimilée à une arme de combat et donc soumise à des contraintes et restrictions

légales, qui par exemple interdisent l'exportation de ses formes les plus avancées.

On comprend dès lors pourquoi l'infrastructure de confiance basée sur la clé publique (*Public key infrastructure - PKI*) n'a toujours pas été déployée à grande échelle, ni au niveau national, ni *a fortiori*, au niveau international. C'est ce défaut de déploiement qui fait dire (ou écrire) à de nombreux experts que les paiements sur Internet ne sont pas sécurisés. Cette affirmation présuppose que hors PKI, point de salut. Ses partisans pensent que son déploiement généralisé n'est qu'une question de temps. D'autres analystes sont plus sceptiques, certains allant jusqu'à persifler que PKI restera éternellement une application d'avenir. Nous reviendrons sur les perspectives du déploiement de la PKI plus loin, après l'analyse des attitudes des consommateurs et des opérateurs vis-à-vis de la sécurité.

L'HISTOIRE INSTRUCTIVE DES PROJETS INNOVANTS DE PAIEMENTS EN LIGNE : ENTRE LE PARCOURS DU COMBATTANT ET LE CIMETIÈRE

Les difficultés de la PKI ne sont pas un cas isolé. Plus encore que d'autres domaines de la boule dot.com, les projets innovants des paiements en ligne forment un paysage de désolation : l'échec y a été la règle ; le succès, une - très rare - exception. Pourtant, les tentatives étaient nombreuses. On peut même distinguer deux grandes vagues d'initiatives et de projets innovants. Au milieu de la décennie 1990, au moment du démarrage du commerce électronique, il était clair pour des analystes avertis que l'essor de celui-ci allait nécessiter des systèmes de paiement adaptés, qui ne pouvaient pas être fournis par les banques traditionnelles, trop lentes et empêtrées dans leurs technologies d'antan (Bill Gates lui-même ne les a-t-il pas traitées de dinosaures ?). De même que ceux qui avaient fait fortune lors de la ruée vers l'or en 1949 ne furent pas les chercheurs, mais ceux qui leur avaient fourni des outils pour chercher, les entrepreneurs qui allaient offrir le support transactionnel aux commerçants en ligne connaîtraient gloire et fortune. Sur ces arguments, de nombreux projets ont été lancés. Ils étaient menés par des équipes prestigieuses, bénéficiaient de financements importants et d'une couverture médias favorable. Des sociétés comme CyberCash sont entrées en Bourse et ont atteint des valorisations de plusieurs milliards de dollars. Mais le succès fut de courte durée. Ainsi, Digicash, dirigée par le promoteur infatigable d'E-cash, David Chaum, et dont le Conseil d'administration incluait Nicolas Necroponte, a été mis en liquidation judiciaire en septembre 1998. CyberCash a dû changer de stratégie et de direction à plusieurs reprises, s'est retiré de la cotation sur Nasdaq au

début 2001 avant d'être mis en liquidation en mai 2001. Ses actifs ont été vendus aux enchères pour un total de 20 M$. En France, Kleline, lancée en 1997 pour capter le marché de l'acquisition des transactions en ligne, a été fermée par sa maison mère BNP Paribas au printemps 2000. Aujourd'hui, il ne reste plus aucun survivant de la première vague.

Cela n'a pas empêché le démarrage de la seconde vague de projets innovants en 1999 et 2001. Ces projets ont attiré beaucoup de capitaux et d'énergie entrepreneuriale. Par rapport à la première, ils couvraient une large gamme de solutions et d'approches, allant du micropaiement, passant par les schémas de fidélisation, jusqu'aux solutions pour les transactions B2B. Jusqu'à la mi-2001, les nouveaux projets avaient le vent en poupe, mais à partir de cette période, ils ont été pris dans le reflux généralisé des entreprises Internet. Pour la plupart, les projets ont été abandonnés ou drastiquement réduits et ralentis. Ainsi, Flooz et Benz, deux initiatives ambitieuses de fidélisation, ont été fermées. Earthport, une société britannique, qui voulait offrir une solution intégrée pour les transactions grand public et interentreprises sur tout terminal (PC, GSM, télévision...), n'a pu échapper à la liquidation qu'en réduisant fortement sa voilure et en se concentrant sur la technologie plutôt que sur un service intégré.

PayPal : une exception spectaculaire

Cette fois pourtant, il y avait une exception à la règle d'échec, et une exception spectaculaire - PayPal. Fondée en fin 1999 dans la Silicon Valley par un groupe de jeunes entrepreneurs, PayPal a démarré sur les chapeaux de roue et son succès ne s'est jamais démenti. Au premier trimestre 2002, il avait plus de 16 millions de clients dans 38 pays et traitait 200 000 transactions pour un montant de 12 M$ par jour. Il a généré un revenu de 48 Md$ (en augmentation de 250 % par rapport à la période comparable en 2001) et, surtout, un profit de 1,2 M$. PayPal est entré en Bourse en février 2002, en pleine déprime du Nasdaq. Pourtant, il fut valorisé à près de 800 M$, c'est un multiple de douze fois ses ventes. Cinq mois plus tard, il a été racheté par E-Bay pour 1,4 Md$, une appréciation de 75 % par rapport à la valeur d'introduction.

PayPal a été le pionnier des paiements interpersonnels (person-to-person - P2P). La demande pour ce type de paiement est apparue suite au développement de ventes aux enchères en ligne, qui mettaient en relation des vendeurs et des acheteurs occasionnels, ayant besoin de systèmes de paiement sûrs et efficients pour les transactions d'un montant réduit. Le succès de PayPal a été étroitement lié à la réussite d'E-bay, le leader des ventes aux enchères en ligne. Ainsi, E-Bay était à l'origine de

près des deux-tiers du business de PayPal et, réciproquement, PayPal était utilisé pour régler un quart des transactions sur E-Bay. L'acquisition du premier par le second est une conséquence logique de cette interdépendance.

Toutefois, contrairement aux espoirs des initiaux, le marché potentiel du P2P apparaît limité en dehors de son segment de prédilection. Aucun autre fournisseur (y compris E-Bay lui-même) n'a réussi une percée similaire.[4]

PayPal avait des ambitions plus larges et, à un moment de son histoire, s'est associée avec une banque en ligne pour créer une nouvelle institution financière. L'essai n'était pas concluant et PayPal s'est recentré sur la technologie. Son approche finale est innovante sans être révolutionnaire, dans la mesure où PayPal s'appuie sur l'infrastructure bancaire existante pour effectuer les transferts de fonds.

En conclusion, il ne semblait pas que l'on puisse considérer PayPal comme le précurseur d'un bouleversement de la structure existante des systèmes de paiement et de l'éviction des banques et des réseaux interbancaires de cartes.

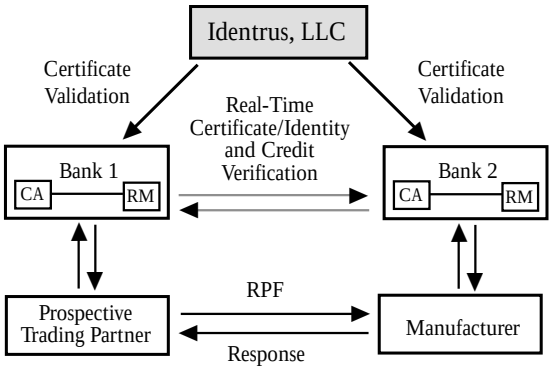
Les projets interbancaires : un bilan mitigé

Si ces réseaux peuvent être considérés comme les grands bénéficiaires de l'essor du commerce électronique, puisqu'ils ont capturé la quasi-totalité des paiements pertinents, leurs efforts pour déployer des solutions spécifiques ne furent pas concluants pour autant. Ainsi, la norme SET (*Secure electronic transactions*), pourtant soutenue par les deux géants globaux, Visa et MasterCard, ainsi que par IBM et Microsoft, et qui visait à combiner le protocole de protection standard des communications sur Internet (SSL) et la PKI, s'est heurtée à une réticence prononcée des commerçants, des utilisateurs et des banques elles-mêmes. Après quelques essais pilotes peu convaincants, SET a été discrètement abandonnée au profit de normes plus simples comme 3-D Secure de Visa.

En France, le projet Cyber-comm, lancé par le groupement des cartes bancaires et visant à utiliser la carte à puce pour les transactions en ligne, a connu un sort similaire et a été mis en veilleuse en 2002.

Un autre projet interbancaire, centré exclusivement sur la PKI et le commerce interentreprises, Identrus, n'est guère mieux loti. Lancé au début de 1999 par un consortium de grandes banques internationales (Deutsche, HVB, Royal Bank of Scotland, ABN Amro, Chase, Barclays, HSBC et Citibank), Identrus vise à créer une infrastructure globale de confiance. En complément de l'application informatique, mettant en œuvre une hiérarchie des certificats, Identrus a créé un cadre légal, offrant un ensemble uniforme et cohérent de règles, de contrats et de pratiques commerciales.

Graphique n° 1
Architecture d'Identrus



Identrus est devenu opérationnel en décembre 2000, et en février 2002, il comptait 50 institutions financières, ayant des clients dans 133 pays, comme membres. Toutefois, il est encore peu utilisé par les entreprises et, plus inquiétant, ses actionnaires hésitent sur son avenir. L'équipe dirigeante et certaines banques cherchent à étoffer les services, craignant que la gestion des certificats ne soit pas économiquement viable. D'autres banques craignent que cette expansion ne fasse entrer Identrus en concurrence avec d'autres entités interbancaires, notamment Swift. Les deux organisations ont signé un accord de coopération, mais leurs relations restent ambiguës, voire tendues. À moyen terme, il n'est pas certain qu'Identrus reste indépendant.

Les partisans des paiements en ligne ont beaucoup misé sur le succès de la facturation et du débit direct électroniques (*Electronic bill presentment and payment*, EBPP). Microsoft lui-même, en association avec le plus important prestataire de services de traitement des paiements, First Data, a lancé une *joint venture* spécialisée, suivi par plusieurs banques. Là encore, force est de constater que l'acceptation populaire ne fut pas au rendez-vous et le taux d'utilisation de ce service reste en-deçà des prévisions[5].

COMPRENDRE LES COMPORTEMENTS DES ACTEURS

Les raisons des échecs

Quelles sont les raisons de cette série d'échecs ?

La principale raison est le décalage entre la sophistication technologique et la rusticité, pour ne pas dire la naïveté, de l'approche économique. Autant les projets brillaient par leur ingéniosité technique, mobilisant

les méthodes de transmission et de cryptage les plus avancées, autant ils ont péché par un manque généralisé d'attention au comportement des utilisateurs et des commerçants. S'agissant d'instruments de paiements et donc d'échanges monétaires, les utilisateurs sont plutôt conservateurs. Même s'ils se plaignent des banques, ils ont une certitude raisonnable que les paiements émis et reçus seront crédités et débités correctement, dans les délais et à un coût acceptables. En l'absence d'avantages économiques manifestes - une réduction notable des prix, une nette amélioration des services - ils sont réticents à changer leurs habitudes financières. Cette réticence est renforcée par l'effet cumulatif de réseau : on hésite à utiliser un service que peu de gens utilisent. Or, un service peu utilisé est cher puisqu'il ne bénéficie pas des économies d'échelle. L'effet de réseau crée ainsi un piège circulaire de l'œuf et de la poule : les commerçants ne veulent accepter de nouveaux instruments de paiement, qui nécessitent souvent une infrastructure spécifique, que s'ils sont assurés que les consommateurs vont les utiliser ; or, ceux-ci ne peuvent le faire que si les commerçants veulent bien accepter les nouveaux instruments. C'est pour cette raison que l'acceptation de nouveaux instruments est un phénomène non linéaire, souvent lent au départ, mais s'accélérant rapidement une fois la masse critique des commerçants et des consommateurs atteinte. Ce fut le cas de la carte bancaire, qui a mis une dizaine d'années pour s'imposer[6].

Le problème essentiel de la plupart des projets de paiements en ligne est qu'ils n'offraient pas d'avantages manifestes aux consommateurs. La complexité d'usage n'était pas compensée par le faible coût ou des fonctionnalités immédiatement attirantes. Souvent, les nouveaux instruments apparaissaient comme une solution à la recherche d'un problème à résoudre. Elles souffraient de l'absence de la proportionnalité, de l'inadéquation entre la sophistication technologique et les enjeux économiques. Pour le cash « physique », le niveau de sécurité d'une transaction est relatif à la somme à payer. Un commerçant jettera un coup d'œil rapide sur la pièce d'un euro, alors qu'il scrutera avec attention un billet de 500 €. Par contre, dans le système e-cash, le niveau de sécurité est constant et aligné sur le haut. Il en résulte une forte disparité entre les techniques de cryptage très sophistiquées, basées sur une implémentation brevetée de la clé publique, et les montants des transactions qui portent sur quelques centimes. Cette disparité a échappé aux concepteurs et promoteurs d'e-cash, mais non aux utilisateurs potentiels, qui avaient du mal à comprendre pourquoi on leur proposait d'utiliser un marteau-pilon pour tuer des mouches.

La sophistication technologique est souvent justifiée par la baisse radicale des coûts de traitement, due à l'explosion de la puissance de calcul, sous l'effet de la loi Moore. Cette justification n'est que partielle-

ment correcte. Tout d'abord, il y a l'effet du « périphérique », dans lequel toute augmentation de la capacité suscite une croissance de la demande. Ainsi, chaque fois que l'on ajoute une voie de circulation sur le boulevard périphérique de Paris, on provoque l'afflux des automobilistes, qui auparavant laissaient leur voiture au garage. Le résultat est que la congestion ne diminue pas. De même, l'accroissement de la puissance des microprocesseurs incite les programmeurs à introduire de nouvelles fonctionnalités - la couleur, un algorithme plus complexe - qui, en définitive, n'améliorent ni la performance ni la convivialité, comme tout utilisateur des versions successives de Windows ou de Word peut en témoigner. Il n'est pas sûr que l'internaute qui doit attendre une minute ou plus la fin du calcul de la clé publique de 128 kbytes pour l'achat d'une chanson d'une valeur de quelques euros apprécie pleinement la prouesse technologique sous-jacente. Toutefois, la faiblesse principale de la justification est ailleurs : les coûts de traitement ne représentent qu'une partie, souvent faible, du coût total de la transaction. La complexité des procédures et la nécessité d'un support technique permanent peuvent compenser, et même au-delà, la réduction des coûts de traitement. À cet égard, on peut noter qu'en termes relatifs, les nouveaux instruments sont souvent tarifés au prix fort. Ainsi, Digicash demandait une commission de 5 % pour les transactions d'e-cash. Une des raisons de la profitabilité de PayPal est que son niveau moyen de commission d'acquisition était de 3,1 % (à titre de comparaison, le niveau moyen de telles commissions sur les transactions des cartes bancaires en France est inférieur à 1 %).

Ces niveaux de tarification expliquent notamment la réticence des commerçants, dont les marges sont souvent réduites.[7]

Et n'oublions pas les coûts d'investissement et d'établissement des nouveaux systèmes et de leurs composants, telles l'infrastructure de confiance et les applications de sécurité qui y sont associées. Ces coûts sont loin d'être négligeables. Naturellement, les promoteurs des systèmes cherchent à récupérer ces coûts auprès des utilisateurs et des commerçants. Cette récupération s'avère particulièrement ardue, notamment auprès des consommateurs. La raison essentielle est que, pour eux, la sécurité n'est pas un service facultatif, mais un attribut indissociable de tout système de paiement largement utilisé. De même que l'on ne peut pas envisager un système de distribution de l'eau qui ne garantirait pas que l'eau soit potable à tous les points de sa consommation par les ménages, il est difficile de concevoir qu'un système de paiement, opéré par les institutions financières, supervisé à son tour par les autorités officielles, n'offre pas un niveau de sécurité nécessaire pour assurer la bonne marche de toutes les opérations usuelles. Dans les systèmes traditionnels, le coût d'une telle sécurité est inclus dans le prix total de l'opération. Habitués

à une tarification forfaitaire ou indirecte des opérations de paiement, les consommateurs ont du mal à comprendre pourquoi il n'en serait pas de même pour la sécurité des paiements en ligne.

La sécurité et le commerce électronique : un nouvel éclairage

Ces considérations permettent de jeter un nouvel éclairage sur la relation entre le commerce électronique et la sécurité des paiements. Cette relation est étroite, mais pas dans le sens où on la présente habituellement. Le consommateur est concerné, moins par l'absence supposée de sécurité que par le supplément de coût qu'on lui demande de payer directement (à travers une tarification spécifique) ou indirectement (en l'obligeant à utiliser des procédures complexes ou un équipement dédié). Comme il ne perçoit pas clairement des avantages compensatoires, il refuse de payer et/ou d'utiliser les nouvelles procédures. Aussi longtemps que les données de ce calcul économique ne seront fondamentalement pas modifiées, il y a fort à parier qu'il ne changera pas de comportement, quel que soit l'effort d'explication ou de persuasion.

Les commerçants et les institutions financières qui contrôlent les systèmes de paiement agissent en conséquence. Sachant qu'ils ne pourront pas transférer aux consommateurs les coûts additionnels des paiements en ligne, les commerçants résistent aux pressions des opérateurs. À leur tour, ceux-ci hésitent à investir massivement dans les nouveaux systèmes et applications de sécurité. C'est cette dynamique qui explique l'état embryonnaire du déploiement de l'infrastructure de confiance.

Le principe de la proportionnalité

À partir de cette analyse, nous pouvons tirer une conclusion simple. Pour faire avancer le dossier de la sécurité, tant au plan conceptuel qu'opérationnel, il faut appliquer le double principe de la proportionnalité et de l'intégration. Pour être accepté par les utilisateurs, tout déploiement d'une application de la sécurité en ligne doit être proportionnel aux enjeux économiques. Les consommateurs et les commerçants concernés doivent, non seulement percevoir clairement les avantages de ce déploiement, mais aussi être convaincus que ces avantages sont clairement supérieurs aux coûts directs et indirects. Ce qui veut dire que la sécurité en ligne doit pouvoir être modulée en fonction de l'importance et de la valeur de la transaction. Plutôt que de chercher le raffinement mathématique des algorithmes de cryptage, les opérateurs doivent privilégier la flexibilité et la convivialité de l'usage. En même temps, la sécurité doit être pleinement intégrée dans le système de paiement pertinent : son usage et sa tarification doivent être transparents à l'utilisateur.

Ce double principe n'est pas réellement révolutionnaire. En fait, il est déjà mis en application par les leaders du commerce électronique, notamment les banques et les *brokers* en ligne. Les institutions financières jouent en effet un double rôle : d'une part, elles fournissent l'appui et le support transactionnel, en particulier les paiements, d'autre part, elles génèrent directement un courant important d'affaires. L'utilisation de l'Internet pour les services financiers est un des grands succès du commerce électronique. Ainsi, selon Jupiter Research, le nombre d'utilisateurs de la banque Internet en Europe a été de 41 millions en 2001 et devait croître de plus de 30 % en 2002 pour atteindre 54 millions, ce qui représente un taux de pénétration de près de 50 % des internautes européens[8]. La banque Internet est donc devenue un phénomène de masse, qui fait désormais partie intégrale des systèmes de distribution bancaire.

Bien entendu, les banques ont mis en place des procédures de sécurité pour les transactions en ligne. Mais celles-ci sont largement invisibles à l'utilisateur. Au niveau de l'interface clients, elles ne diffèrent guère de celles utilisées par d'autres commerçants en ligne comme Amazon et E-Bay. L'accès est contrôlé par le couple classique : nom d'utilisateur et mot de passe. Aucun des leaders de services financiers en ligne n'a apparemment ressenti le besoin de déployer la clé à grande échelle. Ainsi, Nordea, la banque scandinave reconnue comme le n° 1 mondial de la banque sur Internet, affirme que ses services en ligne n'ont pas connu d'incidents majeurs de sécurité ou de fraude. Ses dirigeants continuent d'investir dans la technologie de ces services, mais insistent sur le fait que tout déploiement d'une nouvelle technologie doit satisfaire aux critères rigoureux du *business case* (autrement dit de la proportionnalité).

LES DÉFIS

Si notre analyse aboutit à fortement relativiser les affirmations alarmistes sur la sécurité des paiements en ligne, elle ne permet nullement de conclure que tout est pour le mieux dans ce domaine et que la sécurité ne pose aucun problème. Elle en pose, mais il s'agit moins de la confiance des consommateurs que des défis liés à la mutation vers Internet.

Une mutation est inévitable : tout simplement, d'ici quelques années, il n'y aura plus de distinction entre les services financiers en ligne et les services financiers « traditionnels ». Internet, en tant que protocole de télécommunication et l'architecture applicative, fournira une plateforme d'ensemble de développement et de production, tant pour les systèmes centraux et locaux que pour les réseaux de distribution. Ce qui implique que les systèmes de paiement, y compris les systèmes interbancaires, tels Swift ou G-SIT en France, vont aussi migrer vers Internet.

Même si elle est d'essence technologique, cette mutation entraînera nécessairement des transformations de la structure industrielle, du cadre réglementaire et des relations concurrentielles. Les principaux défis que soulèvent ces transformations sont au nombre de trois : les réseaux ouverts, l'interopérabilité et de la co-opétition intersectorielle.

Les réseaux ouverts

Les systèmes de paiement traditionnels sont basés sur les normes propriétaires et les réseaux privatifs. L'accès y est strictement contrôlé et hiérarchisé. Dans certains cas, il est restreint aux institutions financières, dans d'autres, les non-banques peuvent y accéder sous des conditions bien définies. De toute façon, l'évolution des normes d'accès et de communication, ainsi que les choix technologiques stratégiques, sont déterminés par les banques exclusivement.

Par dessein, Internet est indépendant de l'infrastructure spécifique, ses normes sont élaborées et mises en œuvre par des processus publics, très ouverts et qui échappent largement à l'emprise sectorielle ou réglementaire. Internet permet la création de groupes d'usagers fermés et de réseaux privatifs, mais ceux-ci sont souvent fluides et instables. Les utilisateurs d'Internet ont rapidement découvert que son principal attrait est la possibilité de créer rapidement et économiquement, non pas des Intranets, mais des Extranets, qui relient les interlocuteurs auparavant séparés. Les principales différences entre les deux approches sont présentées dans le graphique n° 2 ci-dessous.

Graphique n° 2
Internet payments : deux approches

Systèmes traditionnels	Internet
Réseau fermé	Réseau fermé
Infrastructure dédiée	Infrastructure dédiée
Accès restreint	Accès étendu
Mono-industrie	Multi-industries

Source : GEF

Cette vision n'est pas universellement partagée. Ainsi, Swift a lancé un nouveau réseau, SwiftNet, qui est basé sur les normes IP, mais utilise une infrastructure dédiée. Ses promoteurs assurent que la migration vers le nouveau réseau n'entraînerait pas de bouleversements radicaux d'organisation interne des banques. Toutefois, on peut se demander si cela sera réellement le cas et si l'on peut pleinement bénéficier des avantages de l'architecture Internet sans épouser totalement le modèle du réseau ouvert.

L'interopérabilité

Dès l'origine, Internet a été bâti sur le principe de l'interopérabilité. Plus récemment, le développement du protocole XML a facilité l'intégration des données et des applications d'origine différente. Mais dans les systèmes de paiement, l'interopérabilité est un sujet délicat, voire même litigieux. Nonobstant les professions de foi enflammées sur les vertus de la standardisation, de très nombreux systèmes restent incompatibles. C'est le cas notamment des grands réseaux de cartes ainsi que de la quasi-totalité des porte-monnaie électroniques. Même si la technologie sous-jacente est parfois similaire ou même identique, les opérateurs ont du mal à se mettre d'accord sur les procédures et la répartition des coûts et des charges. Le passage de l'interopérabilité technique à l'interopérabilité commerciale a toujours été ardu. Ainsi, en Europe, il a fallu une décennie pour obtenir l'interopérabilité entre les différents réseaux nationaux de distribution des billets des banques (DAB). Dans le domaine de la sécurité, on peut déjà relever les problèmes d'interopérabilité entre les différentes approches de l'infrastructure de confiance. Il peut aussi noter que s'il existe de nombreux groupes de travail sur les applications de XML au secteur financier, il y en a pratiquement pas sur les systèmes de paiement.

La co-opétition intersectorielle

Les banques reconnaissent la dépendance croissante des systèmes de paiement sur la technologie de l'information et la nécessité d'une coopération toujours plus étroite avec les fournisseurs de technologie. Mais cette collaboration transforme les fournisseurs en partenaires qui doivent être traités sur un pied d'égalité et associés aux décisions importantes. En même temps, le rôle crucial des systèmes de paiement est de plus en plus affirmé. Pour les Banques centrales, ils sont au cœur du système financier. Pour les analystes et consultants, ils constituent le levier d'un avantage concurrentiel durable dans le commerce électronique[9]. Les banques doivent chercher à en conserver le contrôle et la maîtrise. Ces mêmes consultants considèrent les fournisseurs de technologie, notamment les opérateurs de réseau de télécommunication, comme les concurrents les plus sérieux dans ce domaine.

La mutation vers Internet renforce à la fois l'impératif de coopération et la menace concurrentielle. On le voit bien dans le cas des paiements sur les réseaux mobiles. Jusqu'à maintenant, le commerce mobile n'a pas soulevé d'engouement populaire. On attribue son échec aux limitations de la technologie de GSM. L'avènement des technologies 3G doit éliminer ces limitations et créer un environnement d'Internet mobile à large bande passante. Dans un rapport publié en mai 2001, Forrester

Research projette que les revenus du commerce mobile vont croître de 1,76 Md€ en 2002 à 25,87 Md€ en 2005. Une telle croissance ne pourra pas se faire sans le développement correspondant des systèmes de paiement mobiles. Qui doit en assumer la responsabilité ? Pour les banques, Internet mobile constitue une extension naturelle de leurs réseaux de distribution. Pour les opérateurs de téléphonie mobile comme Vodafone ou Hutchinson, les services financiers et les paiements constituent un moyen persuasif pour encourager leurs clients à migrer vers le 3G et une source potentielle de revenus supplémentaires. Les uns et les autres cherchent à s'assurer une position privilégiée dans la course à la prééminence. Le résultat en est la prolifération des initiatives, certaines pilotées par les banques, d'autres part, les opérateurs, d'autres encore par les réseaux de cartes. Toutes professent leur support aux standards et leur quête d'interopérabilité, mais leur multiplication témoigne que la confiance ne règne pas parmi les différents acteurs.

Les institutions financières ont une longue habitude de l'art difficile de la co-opétition, un équilibrage délicat entre la coopération et la concurrence. Mais, dans les systèmes de paiement, la co-opétition était pratiquée à l'intérieur du secteur bancaire. Dans le monde de la cyberfinance, les banques et les systèmes de paiement existants devront apprendre à développer de nouvelles formes de co-opétition avec les nouveaux partenaires, notamment les fournisseurs de technologie.

NOTES

1. Conseil économique et social, « L'impact des nouvelles technologies sur les services financiers » (Pierre Simon, rapporteur), octobre 2002.

2. CyberSource, 2002 Online Fraud report, décembre 2002.

3. Les études de marché sur ce sujet sont rares et la pornographie n'est pratiquement jamais incluse dans les estimations de la popularité de différents secteurs. Pourtant, les analystes avisés reconnaissent tous l'importance de ce secteur « honteux » et sa contribution décisive à la profitabilité du commerce électronique.

4. Le système des micropaiements par carte à puce, Mondex, qui appartient à MasterCard, a dès le début offert cette fonctionnalité comme un élément de différentiation par rapport aux autres systèmes. Toutefois, Mondex n'a jamais connu de succès commercial. E-Bay avait créé une *joint-venture* avec la banque Wells Fargo pour concurrencer E-Bay. Cette *joint-venture* a été abandonnée au profit de l'acquisition de PayPal.

5. Stefanadis, C. « Why Hasn't Electronic Bill Presentment and Payment Taken Off, » *Current Issues in Economics and Finance*, Federal Reserve Bank of New York, juillet-août 2002.

6. Evans, D. and Schamlensee, R., *Paying with Plastic: The Digital Revolution in Buying and Borrowing*, MIT Press, 1999.

7. Dans le cas de PayPal, les commerçants sont le plus souvent des individus, pour qui les ventes constituent un revenu d'appoint. Par ailleurs, PayPal offre un service unique, qui n'a que peu de concurrents.

8. Jupiter Research, *Online Financial Services Forecast*, Jupiter Research, novembre 2002.

9. Boston Consulting Group, *Global Payments 2002*.