Le commerce électronique : de la sécurité à la confiance

Les nombreuses questions qui assaillent le potentiel cyberconsommateur désirant acheter sur le Net relèvent essentiellement de trois ordres : la sécurité physique du moyen de paiement, la sécurité juridique de la transaction et la confiance qu'il peut avoir dans l'interlocuteur virtuel. Quelle est, ou serait une sécurité acceptable sur les réseaux ? La sécurité juridique est-elle l'enjeu véritable d'une sécurisation réelle des transactions ? La confiance, enfin, ne ressort-elle pas de la capacité de l'interlocuteur virtuel à inspirer des reflexes lui assurant une certaine crédibilité ?

par Ivan Faucheux et Cyril Sniadower

Sécurité et confiance sont deux notions qui sont, dans les relations humaines, intimement liées. La sécurité est définie, par *Le Robert*, comme « l'état d'esprit confiant et tranquille d'une personne qui se croit à l'abri ». La sécurité, qui dans ce cas ne se définit pas comme une situation, mais comme le sentiment ou l'appréhension d'une situation donnée par une personne, suppose un état de confiance.

La relation qui existe entre la confiance et la sécurité n'est pas à sens unique. C'est une relation où les sentiments de sécurité et de confiance se nourrissent mutuellement et où une faille réelle ou vécue dans l'une des deux notions entame la seconde.

Le commerce, comme champ d'application de ces deux notions, n'en est pas absolument tributaire : les Bédouins du désert n'avaient pas, dans leurs premiers périples, une confiance aveugle et un sentiment de sécurité dans leurs traversées du désert ; les premiers Portugais qui, au début du XV^{e} siècle, se sont élancés à la conquête maritime de l'Afrique, croyaient les eaux peuplées de monstres marins prêts à les dévorer. Le commerce s'est développé dans des conditions de sécurité effectives sans commune mesure avec ce que nous connaissons aujourd'hui. Force est de constater, cependant, que l'argument de la sécurité du consommateur, du client, de l'usager final a pris, dans les réflexions sur les transactions commerciales, une importance considérable.

La sécurité, dans le cas de phénomènes de masse, tels que la consommation de produits courants, les modes de paiement, les transports ou le système de santé, relève d'une problématique de gestion du risque. Ces champs relèvent d'une prise en compte de la diversité des situations personnelles ainsi que de la réponse appropriée pour diminuer « dans des proportions raisonnables » ce risque : principe de précaution pour la définition de la réponse appropriée, ou principe « pollueur payeur » pour la définition des responsabilités. Ils relèvent essentiellement des prérogatives de la puissance publique. Dans le domaine du commerce et de l'industrie, où règne le principe de liberté des acteurs, la sécurité n'est pas - ou n'est plus - un pré-requis nécessaire, et le degré d'exigence n'est plus le même.

Les transactions électroniques

Pour ce qui concerne le commerce électronique BtoC (en direction du consommateur), le raisonnement présenté est souvent simple, ou simpliste : la sécurité est une condition nécessaire et suffisante du développement de la confiance dans ce domaine. Une telle conception du développement de la confiance est à la fois fort ambitieuse, mais également sans effet : sécuriser de façon absolue les transferts informatiques est une tâche sans fin. Les spécialistes informatiques considèrent que le nombre de failles techniques est sans limite : la sécurité relève plus d'une affaire d'organisation que de technique. Mata-Hari n'était pas, en son temps, spécialiste des serrures, ou du moins pas des serrures physiques.

La confiance est, de plus, un phénomène d'une extrême complexité : si beaucoup de livres tentent d'en cerner les contours (« La société de confiance » d'Alain Peyrefitte, « Vers une société de confiance » de Pierre Pettigrew…), aucun ne donne une définition précise de cette notion. De plus, les auteurs n'attachent, au travers de leurs réflexions, que peu d'importance à la situation de sécurité : si preuve devait en être donnée, la société américaine peut être considérée, à plusieurs titres, comme une société de confiance. Or le taux de criminalité des rues de San Francisco, Dallas ou Miami - et, dans une moindre mesure, New York - est

sans commune mesure avec celui des grandes métropoles européennes.

Dans le domaine de la sécurité des transactions électroniques, le même constat peut être fait : le volume des transactions frauduleuses aux Etats-Unis est de l'ordre du pourcentage ; en France, il dépasse à peine 0,05 % des transactions. Ceci n'empêche pas les Américains de consommer allègrement sur le Web, à un rythme bien plus soutenu que leurs homologues internautes européens et, plus spécialement, français.

La question de la confiance dans le domaine des transactions BtoC relève de la question fondamentale d'un consommateur qui se retrouve face à un marchand, contre lequel il ne se sent aucun recours en cas de fraude ou de défection de la part de ce dernier. En effet, dans le cas d'un marchand physiquement établi, que l'on a vu et identifié de visu, s'établit automatiquement une confiance minimale : celle de pouvoir aller s'expliquer « entre hommes » en cas de différend. Dans le cas d'un marchand virtuel, cette confiance minimale n'existe pas !

Le volume des transactions frauduleuses aux Etats-Unis est de l'ordre du pourcentage ; en France, il dépasse à peine 0,05 % des transactions

En ce qui concerne les transactions électroniques entre entreprises (commerce BtoB), qui représentent près de 90 % du volume total des transactions (voire près de 98 % en considérant les transactions financières entre établissements bancaires), la question devient autre : ici la confiance n'est pas occasionnelle, elle est institutionnelle. C'est la relation entre entreprises qui crée cette confiance et non une confiance spontanée qui ferait apparaître la relation commerciale. De façon générique, les modes de commerce entre entreprises ressemblent plus souvent à des solutions sur mesure, taillées pour des dialogues entre institutions. La relation électronique ne repose pas sur la confiance entre un vendeur et un acheteur physiquement identifiés, mais procède de la capacité de deux sociétés à rationaliser et minimiser les coûts de transactions entre ces dernières.

On pourrait donc, en première approche, penser que les deux mondes n'ont rien à voir l'un avec l'autre. Mais ce qui a été dépeint est une vision des extrêmes : d'un côté, de grandes multinationales capables d'établir des marketplace ou des relations BtoB dans un unique but de maximisation des profits ; de l'autre, un consommateur égaré dans les méandres de la cybertoile, en butte aux angoisses du voyageur égaré. Les liens entre ces deux mondes s'établissent de plusieurs manières, mais sont aujourd'hui ténus.

Les acteurs intermédiaires sont nombreux : la petite entreprise est, elle aussi, potentiellement une consommatrice de services du Net ; incapable de développer une solution sur mesure pour elle seule, et au sein d'un réseau vaste d'acteurs de même taille et qu'elle ne connaît pas, elle devrait, elle-aussi, être au cœur du développement du commerce électronique.

Les solutions développées pour les grandes entreprises pourraient être valorisées pour les applications grand public : cette idée est généreuse, car il pourrait être tiré parti de la notoriété de ces entreprises ainsi que de leurs capacités à sécuriser leurs transactions, pour donner confiance aux solutions appliquées pour le commerce BtoC ; or, dans ce domaine, les grandes entreprises sont discrètes, soit pour ne pas attirer l'attention des pirates potentiels sur leurs enjeux, soit pour cacher des solutions sans grande sécurité (1).

Le développement des échanges électroniques pousse au développement des capacités des réseaux, et au développement des infrastructures. Ce développement devrait permettre de développer, pour les particuliers, des offres de télécommunication à haut débit à des coûts moindres et, donc, des usages et de l'offre commerciale sur le Web pour les consommateurs finaux. Or, dans ce domaine, on n'observe que peu d'opérateurs de télécommunication pour les entreprises, qui sautent le pas vers les consommateurs finaux, et, pour ceux qui le font (Noos, Free, etc), force est de constater que l'offre ne tend pas, en termes de prix, vers un niveau jugé satisfaisant par les consommateurs !

Lors des transactions électroniques entre entreprises, la confiance n'est pas occasionnelle, elle est institutionnelle

Dans le présent article, essentiellement consacré au commerce BtoC, nous allons d'abord tenter de définir ce qui est, ou serait, une sécurité acceptable sur les réseaux (ce qui implique qu'il est impossible d'atteindre, à terme, la situation idéale d'une sécurité absolue). Nous tenterons, ensuite, de définir en quoi la sécurité juridique, enjeu majeur des futures lois et décrets sur la société de l'information, n'est pas, dans le cas du commerce électronique, l'enjeu véritable d'une sécurisation réelle des transactions. Enfin, nous essaierons d'analyser en quoi la confiance est, pour ce commerce, une question bien plus immatérielle et virtuelle que ne le sont les réseaux qui le permettent.

Sécurité des réseaux : la mission impossible

L'ordinateur, qu'il soit PC ou MacIntosh, est devenu un objet relativement familier. Au bureau, le nombre de cadres équipés aujourd'hui d'un tel outil avoisine les 100 %, et le taux d'équipement des entreprises est proche des 80 %. Pour les foyers, le taux reste encore faible, aux alentours de 19 %. Mais avant de se lancer dans un achat sur le Net, plusieurs questions assaillent le potentiel cyberconsommateur : « Vais-je être connecté au bon site ? Le site est-il l'œuvre d'une personne sérieuse, ou d'un escroc ? Vais-je voir mes coordonnées distribuées sur toute la planète, et me faire inonder de prospectus ? Est-il normal qu'on me demande mes goûts musicaux quand je commande un paquet de lessive ? Que puis-je faire en cas de non-correspondance entre ce qui est commandé et ce qui est reçu ? Mon numéro de carte bleue sera-t-il intercepté ?

(1) Les transactions entre traders se font toujours sur de simples lignes téléphoniques, enregistrées depuis moins de vingt ans : la confiance aveugle de l'opérateur n'a, dans ce domaine, pas complètement disparu, pour le malheur de quelques grandes banques opérant en Asie.

La liste pourrait être allongée, mais les interrogations relèvent essentiellement de trois ordres :
- le premier concerne la sécurité physique du moyen de paiement ;
- le deuxième concerne la sécurité juridique de la transaction ;
- le troisième concerne, enfin, la confiance que je peux avoir dans l'interlocuteur virtuel, c'est-à-dire de sa capacité à inspirer les réflexes pouvant lui assurer une certaine crédibilité.

Les failles de sécurité sont, dans les systèmes informatiques, particulièrement nombreuses. Celles qui sont techniques sont à la fois les plus simples à résoudre, mais également les plus nombreuses. Depuis les émissions d'ondes électromagnétiques par le clavier et l'écran d'un ordinateur (qui permettent de savoir ce que l'on voit et ce que l'on écrit) jusqu'aux virus complexes (comme le récent *I Love You*, qui a fait prendre conscience de la rapidité de déploiement de tels programmes via Internet), l'ordinateur et la toile à laquelle il est relié apparaissent singulièrement dépourvus de défense.

Même au cœur des logiciels les plus courants peuvent se cacher des fonctionnalités insoupçonnées (comme, par exemple, Word 97 où se cache un flipper !), et les navigateurs, qui intègrent aujourd'hui des scripts de plus en plus élaborés, se révèlent des portes d'entrées particulièrement efficaces. Les évolutions technologiques laissent l'utilisateur moyen face à un sentiment rageant d'impuissance ; la sensation de maîtrise de l'outil informatique est faible, ce qui, au regard du problème de la sécurité, est crucial. S'il est possible, aujourd'hui, de donner confiance dans une voiture en vantant les dernières avancées technologiques (ABS, contrôle électronique du freinage…), aucun fabricant de logiciel n'a encore, à ce jour, vanté les mérites de la sécurité de son produit.

Plusieurs raisons peuvent être mises en avant pour expliquer ce manque apparent.

La première est que, face aux informaticiens « hackers » en tous genres, aucun fabricant de logiciels ne peut être sûr de la sécurité de son produit. S'il faut poursuivre l'analogie automobile, les tests réalisés sur la Mercedes Class A, qui avait révélé un défaut de conception et une faille de sécurité dans la tenue de route, doivent être multipliés par les millions de pirates informatiques à travers le monde, qui travaillent, non seulement pour le gain, mais également pour la gloire, à briser les systèmes de sécurité. Et l'on se souvient de l'effet désastreux que la publication des tests avaient eu sur le lancement de la Class A…

La deuxième raison tient au fait que la sécurité ne représente pas, en l'état actuel des usages par les internautes moyens, un véritable enjeu de vente des ordinateurs et logiciels. Le PC, vendu avec ses multiples accessoires, son système d'exploitation et ses fonctionnalités n'est pas censé être une forteresse capable de résister aux assauts acharnés des hordes de "hackers" (venus du froid et d'ailleurs), mais un outil ludique convivial et ergonomique. C'est, a contrario, aux banques qu'il appartient de démontrer la robustesse des solutions informatiques de paiement, qui ne représentent pas le seul motif d'inquiétude de la part des consommateurs. Dans le cas des automobiles, cette solution reviendrait à ce qu'il appartienne aux pétroliers de démontrer la fiabilité et la sécurité des voitures consommant leur essence (ou gasoil).

La sécurité ne représente pas, en l'état actuel des usages par les internautes moyens, un véritable enjeu de vente des ordinateurs et logiciels

La sécurité technique des systèmes informatiques est, pour le grand public, une inconnue, dont il ne sait pas décrypter les tenants et les aboutissants. Il peut être dit tout et (souvent) n'importe quoi sur ce sujet, il est impossible, pour un consommateur moyen déjà perdu entre les systèmes d'exploitation et les pannes de sa machine, de déceler les éléments de langage qui font argumentaire. Face à cette lacune, ou cette absence de sens du langage dans le domaine de la sécurité, il est illusoire de pouvoir accrocher à un tel élément des bribes de confiance. La situation serait comparable à celle d'un navigateur du XV^{e} siècle, à qui l'on tenterait d'expliquer, nonobstant l'anachronisme, la sûreté du fonctionnement d'un GPS : il n'y comprendrait rien, mais l'utiliserait. Et lui donner confiance dans la mission dont il est investi (découvrir une nouvelle route vers les Indes, par exemple) sur la base de cet élément ne serait pas la meilleure solution pour le voir larguer les amarres : « Dieu et le Roy » seraient des arguments bien plus appropriés.

Sécurité juridique : le faux problème

Si la technique ne peut être considérée comme une bouée de sauvetage pour le malheureux internaute se lançant à la découverte du Web, l'environnement juridique pourrait alors être le moyen de donner une certaine confiance. Las, les récentes jurisprudences disent et se contredisent, montrant l'extrême flou dans lequel la Justice évolue actuellement. Pour exemple, le 30 janvier 2001, la Cour de Cassation annule un arrêt de la Cour d'appel de Papeete du 9 mars 2000 qui lui-même modifiait les termes d'un jugement antérieur sur le problème de prescription lors d'une publication sur le Net. De l'autre côté de l'Atlantique, le 2 mars, la Cour suprême de Virginie a refusé l'octroi d'un subpoena (citation à comparaître) contre la compagnie AOL, demandeur et défendeurs demeurant anonymes, ce qui conduit à un véritable procès en diffamation entre anonymes !

Le récent comité interministériel sur la société de l'information a confirmé le souhait du gouvernement de voir aboutir un grand chantier législatif, dont les premiers jalons ont été posés par la libéralisation de la cryptologie et la récente publication du décret d'application sur la signature électronique. Ces deux évènements, avec près de deux ans d'écart, ont ceci d'analogue : ils témoignent d'un retard conséquent de la France par rapport à ses principaux partenaires et concurrents économiques dans le domaine. L'enjeu de ces textes réglementaires est le même : favoriser le développement de l'usage des technologies de l'information et de la communication au sein des habitudes de consommation, c'est-à-dire

faire en sorte que les Français utilisent de façon plus intensive le Net.
La confusion et l'aspect extrêmement compliqué de l'application de la législation au domaine des nouvelles technologies tient non seulement à la nouveauté de la matière, mais également au fait que l'internationalité de la toile mondiale pose de façon aiguë le problème du croisement des droits nationaux. L'aspect très technique et nouveau des TIC rend la sécurité juridique des faits et gestes sur la toile tributaire d'éléments non maîtrisés : ainsi, les fichiers temporaires qui stockent l'ensemble des pages visitées doivent-ils être considérés comme des fichiers téléchargés de façon volontaire ? Si oui, comment prouver que l'on peut arriver de façon involontaire sur des pages au contenu illicite, en ayant fait confiance à des moteurs de recherche d'une sélectivité aujourd'hui peu avérée pour les plus connus ? Ce sont autant de questions qui ne se régleront que devant une juridiction.

Nécessité de la réforme législative

Sur deux aspects majeurs que recouvre l'actuel chantier législatif, à savoir la nécessité de sécuriser l'acte d'achat par la signature d'une part, et par la protection de la confidentialité des données échangées d'autre part, plusieurs remarques peuvent être faites.
Les éléments qui ont conduit le législateur a engager le chantier réglementaire, sur la signature, apparaissent majeurs. En effet, la fonction d'une signature est triple. Elle affirme la volonté du signataire ; elle est un élément de preuve ; elle est un élément de formalisme. Dans ce dernier cas, la signature manuscrite reste requise et ne saurait être remplacée par une signature électronique. Par contre, la législation doit être adaptée pour que la signature électronique puisse satisfaire les deux premières fonctions.
En France, à l'heure actuelle, la preuve est libre, avec une exception particulièrement notable. En effet, l'article 1341 du Code civil dispose : « Il doit être passé acte devant notaires ou sous signatures privées de toutes choses excédant une somme ou une valeur fixée par décret (…) et il n'est reçu aucune preuve par témoins contre et outre le contenu aux actes… » La somme a été fixée à 5 000 francs par un décret du 15 juillet 1980. Au vu de l'évolution des masses monétaires en circulation et des réalités économiques, une telle limite devrait évidemment être réévaluée. Il est néanmoins plus intéressant de constater qu'aujourd'hui, la loi elle-même rend les documents électroniques irrecevables comme mode de preuve, et ce à double titre : au-delà de 5 000 francs, une preuve écrite doit être préconstituée ; quelle que soit la somme, l'écrit prime tous les autres moyens de preuve.

L'internationalité de la toile mondiale pose de façon aiguë le problème du croisement des droits nationaux

Toutefois, cet article n'est pas d'ordre public. En conséquence, les parties peuvent y renoncer. La jurisprudence est constante sur ce point. L'article 1341 s'impose au juge seulement lorsque les parties n'y ont pas explicitement ou tacitement renoncé. En particulier, les conventions de preuve sont parfaitement admises, comme le proclame le fameux arrêt Crédicas, relatif à la preuve d'un ordre de paiement donné par utilisation d'une carte magnétique et composition concomitante du code confidentiel. La Cour de cassation a en effet jugé en l'espèce que les parties peuvent, par contrat, accorder une valeur de preuve à un document dépourvu de signature manuscrite. Dans son rapport annuel de 1989, la Cour de cassation a confirmé ce point de vue, en estimant que « ce procédé moderne présente les mêmes garanties que la signature manuscrite, laquelle peut être imitée tandis que le code secret n'est connu que du seul titulaire de la carte ».
D'autres difficultés existent. Le Code civil mentionne à plusieurs reprises l'obligation d'une signature. L'article 1322 sur les actes sous seing privé, l'article 1325 sur les contrats synallagmatiques ou l'article 1326 à propos des reconnaissances de dettes imposent ainsi le recours à l'écrit. Il est fort probable que la modification de ces articles soit prochaine, afin de conférer aux actes électroniques une validité équivalente à celle des actes écrits.

Le tiers de certification, un acteur primordial dans les transactions de demain

Les tiers de certification remplissent donc une fonction essentielle : formaliser et assurer le lien qui existe entre une personne physique ou morale et une paire de clefs asymétriques. Pour vérifier l'identité du signataire d'un message, le destinataire doit récupérer sur un serveur spécialisé la clef publique de l'expéditeur du message. Le destinataire est alors sûr que seul le détenteur de la clef privée correspondante a pu signer le message. Malheureusement, il n'est pas garanti que le détenteur de cette clef privée soit effectivement la personne avec qui il souhaite communiquer. Il se peut que la clef publique ait été déposée frauduleusement par une autre personne, qui souhaite se faire passer pour l'expéditeur du message. Il s'agit, par conséquent, de prévenir cette usurpation d'identité. Le tiers de certification a pour mission – et cette mission est essentielle si l'on veut garantir la sécurité des transactions commerciales – d'assurer que la clef publique récupérée appartient effectivement à la bonne personne. D'une certaine manière, le tiers de certification joue donc, vis-à-vis du commerçant, le rôle d'une préfecture de police délivrant une carte d'identité, et vis-à-vis du consommateur le rôle d'un registre du commerce permettant d'identifier avec précision la société cocontractante.
Le rôle du tiers de certification est donc fondamentalement d'émettre des certificats. Le certificat est simplement un message électronique délivré par le tiers de certification qui a pour fonction d'établir un lien entre une personne physique ou morale dûment identifiée et une clef publique. Il sert donc à l'identification du titulaire de la clef privée correspondant à la clef publique mentionnée dans le certificat pour la signature.
L'importance évidente des tiers de certification dans les transactions commerciales amène à s'interroger sur leur responsabilité. Il faut que les utilisa-

teurs soient attentifs au niveau de sécurité garanti par les autorités de certification. Il faut également être renseigné sur le sérieux technique et organisationnel du tiers de certification, en particulier sur la façon dont celui-ci gère le délicat problème de la suspension ou de l'annulation des certificats. Dans tous les cas, et nous y reviendrons, le tiers de certification ne garantit que l'identité de l'interlocuteur et non son honnêteté.

Le tiers de certification ne garantit que l'identité de l'interlocuteur et non son honnêteté

Un autre point important est le statut de ce tiers de certification. Il peut être considéré, disions-nous, dans une certaine mesure, comme un registre du commerce ou comme un organisme délivrant des pièces d'identité. Faut-il par conséquent qu'il soit public ? A l'inverse, on peut avancer que les tiers de certification ne sont que de simples intermédiaires, que de simples intervenants dans un circuit purement commercial. Peut-on, dans ce cas, admettre que les tiers de certification soient de pures sociétés privées issues du marché ? La solution n'est pas évidente. Les organismes privés ont la faveur du projet de directive, qui admet même des organismes non agréés par les pouvoirs publics comme tiers de certification. C'est là une solution audacieuse. Si cette directive était adoptée, il faudrait donc espérer que le marché sache sélectionner des autorités de certification sérieuses, ou que les Etats puissent octroyer, par leur agrément, un avantage commercial suffisant à des sociétés auxquelles ils auraient imposé un cahier des charges exigeant.

Une telle fonction n'existe aujourd'hui que de façon embryonnaire. Une réflexion, notamment sur le rôle de l'Etat dans ce domaine - les cartes d'identité sont des documents administratifs officiels, servant néanmoins, dans le cas de paiement par chèques, à sécuriser ce paiement et cette démarche ne vaut, certes, que pour le vendeur - est nécessaire, car il n'est que peu probable qu'une infrastructure de ce type soit à même d'apparaître spontanément en peu de temps.

De la confidentialité

La peur, aujourd'hui couramment répandue, lors d'un achat sur Internet est de voir son numéro de carte bleue interceptée et utilisée pour d'autres achats. Or, à l'heure actuelle, les banques françaises sont tenues de rembourser leurs clients qui contestent une transaction payée par carte bleue, lorsque seuls le numéro de carte bleue et sa date d'expiration – et non le code secret ou la signature manuscrite – ont été nécessaires pour effectuer le paiement. C'est le cas sur Internet, où le code secret n'est jamais exigé. Un développement massif du commerce électronique accompagné d'un essor massif de la fraude mettrait en péril le système actuel de tarification de la carte à puce, et donc sa viabilité. Il est donc évident que les banques sont intéressées au premier chef par le développement de la sécurité sur Internet.

Les banques sont intéressées au premier chef par le développement de la sécurité sur Internet

Malheureusement, il n'est pas sûr que le consommateur y attache la même importance. Nous en voulons pour preuve ces ventes par téléphone, de type Téléachat, où le client donne en clair son numéro de carte bleue et sa date d'expiration à un employé qu'il ne connaît pas et qu'il n'a jamais vu. Des risques existent également pour les paiements classiques par carte bleue : il suffit de regarder le récépissé d'un paiement effectué chez un commerçant pour s'apercevoir que le numéro de carte bleue et sa date d'expiration y apparaissent entièrement et en clair.

Pourtant le téléachat s'est développé, et personne n'hésite à régler un commerçant par carte bleue. Ces deux exemples, combinés au cas des Etats-Unis, où la fraude est importante et le commerce florissant, nous amènent à penser que la sécurité n'est pas la condition primordiale pour le développement du commerce électronique.

Au total, si la sécurité juridique apparaît comme un élément nécessaire d'un développement des relations commerciales sur le Net, elle est loin d'être suffisante. Le champ des problèmes que pose aujourd'hui le développement du commerce électronique dépasse largement les deux enjeux de sécurité juridique et de confidentialité développés dans cette partie : pourront, en outre, être cités les enjeux d'internationalisation et d'homogénéisation des règles applicables dans ce domaine, les enjeux de protection du consommateur contre les sollicitations de toute part, les problèmes de ventes de contenus illicites via le Net (comme des bébés, par exemple). Mais ils ne constituent pas la base des problèmes qui doivent d'abord être résolus : le client qui, aujourd'hui n'hésite pas à acheter ses cigares directement sur un site de Cuba

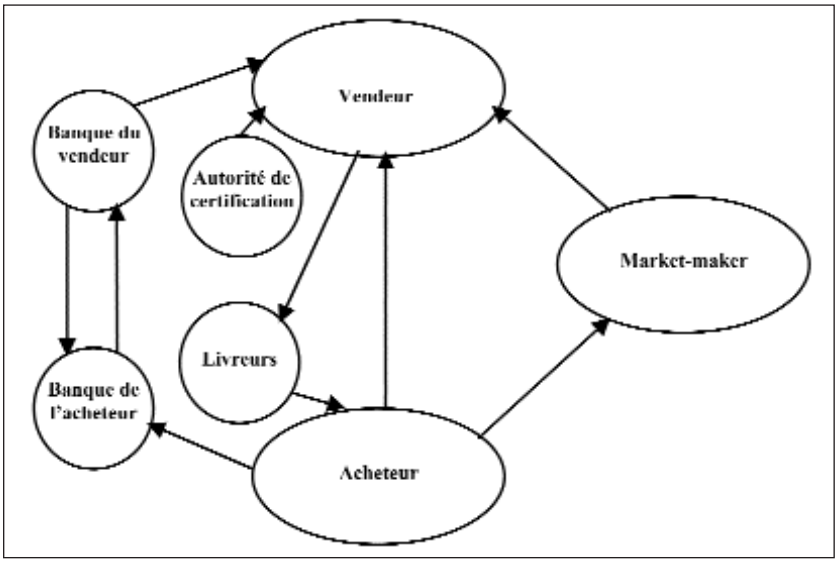

Fig. - 1. Les différents modes de transactions.

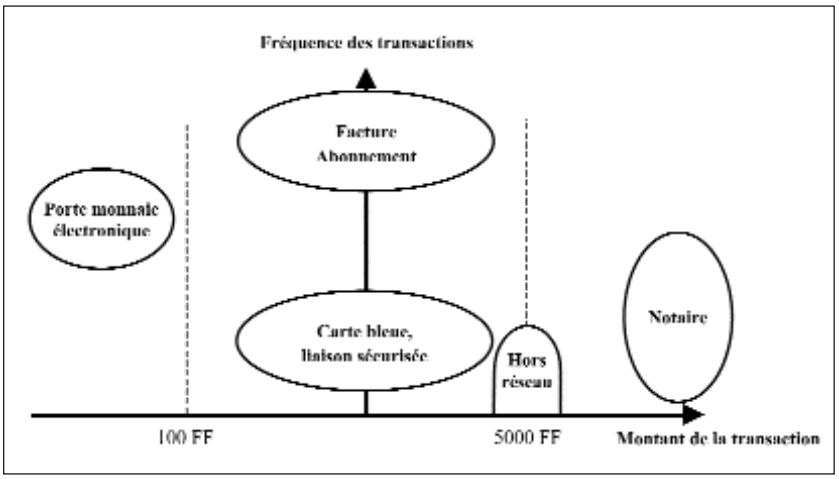

Fig. - 2. Les différents acteurs de la transaction

ne s'embarrasse que peu de ces questions et ne représente pas la majorité de l'espèce internaute… Cette dernière, avant de se lancer à l'assaut du monde, armée de sa carte bleue, veut d'abord s'assurer qu'elle peut aller acheter en bas de chez elle en toute sécurité.

La confiance : l'enjeu d'une démarche et non d'un décret

L'enjeu, pour le consommateur, est avant tout le niveau de sécurité. C'est alors au vendeur de le convaincre que ce niveau est tout d'abord suffisant et, en deuxième lieu, atteint. La figure 1, ci-avant, représente diverses solutions envisagées en fonction de l'intensité et de la fréquence des transactions.

L'autre élément de la confiance est aujourd'hui tributaire des autres acteurs qui sont engagés dans l'acte d'achat. Nous nous sommes, pour des raisons de simplicité, limités à un schéma simpliste ou le consommateur potentiel était seul, face à son ordinateur, et avait un souhait déterminé. Or, d'autres partenaires entrent en jeu. Il a été question, notamment, du tiers de certification, dans le domaine de la signature, et du banquier, dans le domaine du paiement. Ce sont deux fonctions qui, de façon singulière, occupent dans la vie quotidienne - si l'on fait un parallèle osé entre le tiers de certification et un notaire - des rôles bien plus importants que le simple service de dépositaire d'argent ou de signatures… Il arrive bien souvent que le banquier soit, aujourd'hui, dans la vie quotidienne, un homme de confiance, à qui l'on confie bien au-delà de ce qui devrait concerner son strict intérêt professionnel. Et le notaire de famille est une figure emblématique de la personne à qui l'on a recours en cas de problèmes.

Au-delà de ces deux fonctions, existent également d'autres acteurs, tels que les assureurs, les livreurs, les market-makers (2), etc. Il est d'ailleurs remarquable que la publicité sur les sites de commerce électronique mettent de plus en plus en avant de telles fonctions. Pour les sites de *trading*, ce sera l'assureur, pour le site de commerce de supermarché, ce sera le livreur, et pour les sites de commerce artisanal, ce sera plutôt le banquier. Les figures 1 et 2 tentent de décrire la chaîne complexe des relations entre ces acteurs.

Le jeu d'acteurs, qui se noue aujourd'hui autour de l'acte d'achat sur Internet apparaît compliqué, lui aussi, ce qui ne va malheureusement pas dans le sens de la création d'un sentiment de confiance. La récente publicité de la Poste (« ce que l'avenir vous promet, la Poste vous l'apporte »), qui met en avant l'incongruité d'un monde virtuel où la fonction de livraison serait absente (3), est à ce titre emblématique de ce simple rappel : Internet ne simplifie pas forcément les choses, bien au contraire. Mais il ouvre des opportunités qu'il appartient de pouvoir saisir.

Au total, la question du développement de la confiance dans le commerce électronique peut s'analyser comme la capacité à ce que des systèmes compliqués puissent être présentés de façon simple et non simpliste. Facile à dire, moins à réaliser. Par conséquent, les professionnels auront certainement intérêt à présenter les questions de sécurité comme étant réglées. Ils devront aussi se souvenir que, seule, la sécurité n'est pas un argument de vente. L'essentiel de leur effort sera de réussir à se faire connaître, à susciter la confiance des consommateurs et à faire en sorte que cela se sache auprès des autres consommateurs potentiels. Le système du « satisfait ou remboursé », qui a contribué de façon importante au succès de la vente par correspondance classique, devra être transposé au commerce électronique. Les moyens de communication traditionnels, plus éprouvés et touchant un plus large public, devront être utilisés de façon beaucoup plus intensive qu'aujourd'hui. Bref, il semble que le marché soit ouvert pour quelques intermédiaires, peu nombreux, mais ressentis comme sûrs par le public, qui garantiront les transactions et amèneront les consommateurs et les vendeurs en confiance vers le commerce électronique de masse. ●

(2) Market-maker : intermédiaire commercial référençant des vendeurs et s'en portant garant dans une certaine mesure.

(3) On pourra remarquer à ce titre que le facteur remplit, comme le banquier ou le notaire, des fonctions sociales majeures en regard de sa simple fonction de distribution du courrier...