Le télépaiement sur le Web pour les entreprises et les particuliers: perspectives françaises & québécoises

Thierry Piette-Coudol et Yvan Lauzon (*)

Introduction

Le Commerce électronique sur Internet ne peut devenir une réalité tant que les opérations commerciales ne s'achèvent pas par des paiements. En effet, il est peu pratique d'utiliser un système télématique tel Internet pour commander des produits et un autre système manuel, ou même automatisé, pour effectuer le paiement.

Le secteur bancaire avec la monétique offre déjà le paiement électronique, souvent effectué à partir de systèmes privés de télécommunication. Mais les utilisateurs d'Internet veulent accéder à des services de téléachat et de télépaiement directement sur le Web. Des initiatives apparues sur le Web ces derniers mois vont d'ailleurs dans ce sens. Elles ont pour nom CyberCash, DigiCash, First Virtual ou Global OnLine.

Le paiement n'est pas une opération isolée : pour tout paiement, il y a une cause. La cause la plus banale est un achat d'un bien ou d'un service. Cet achat s'analyse juridiquement dans un cadre déterminé : celui du «contrat de vente». Ce contrat doit permettre d'élargir la problématique juridique des télétransactions d'affaires. Ainsi pourront naître de nouvelles idées génératrices de nouveaux service de télépaiement.

Nous exposerons dans ce texte dans quel contexte juridique les initiatives de télépaiement peuvent se développer. En alliant la simplicité pour l'utilisateur, la sécurité technique et la sécurité juridique, les services de téléachat et de télépaiement pourront trouver leur positionnement sur les autoroutes de l'information pour le plus grand bénéfice de tous.

Nous présenterons tout d'abord les services de télépaiement existants en les situant dans leur perspective juridique. Puis, nous proposons de relier le télépaiement à la "vente à distance" (ou téléachat), en montrant les distinctions entre les transactions n'impliquant que des particuliers et celles impliquant à la fois des particuliers et des entreprises.

1. DU PAIEMENT ELECTRONIQUE AU TÉLÉPAIEMENT SUR LE WEB

1.1 Le paiement électronique : Définition et caractéristiques

1.1.1. Paiements électroniques : Transferts électronique de Fonds et cartes bancaires

Le paiement est une opération qui consiste à fournir une contrepartie monétaire contre la remise d'un bien ou encore l'obtention d'un service. Des moyens de paiement non-monétaires peuvent également être utilisés, comme le chèque. Cependant, plus récemment les technologies de l'information permettaient de nouveaux moyens comme les transferts électroniques de fonds (TEF) ou la monétique.

Avec le support des télécommunications, les banques ont déjà mis au point des systèmes de paiement interbancaires qui leur permettent d'assurer la compensation entre leurs créances et leurs dettes, il s'agit du transfert électronique de fonds (TEF). Le système international SWIFT est un bon exemple d'un tel système TEF, en permettant l'échange dans un contexte extrêmement sécurisé de messages standardisés (ex: lettre de crédit) entre les principaux pays industriels. SWIFT a permis le transfert quotidien de centaines de millions de dollars. Mais un tel système international n'est pas ouvert aux particuliers, ni aux entreprises. Il ne sera donc pas directement transposable à Internet où le Commerce électronique doit profiter tant aux particuliers, qu'aux entreprises.

Pour les particuliers, les banques ont développé il y a 35 ans déjà la "monétique" autour de l'utilisation de cartes de crédit à piste magnétique. Les cartes VISA, MASTERCARD & AMERICAN EXPRESS en sont de bons exemples.

Plus récemment, la technologie des cartes à puce (ou cartes à mémoire) a été introduite dans l'expérience MONDEX de Swinton en Angleterre et celle de Guelph en Ontario. Au Canada, le consortium Mondex est formé de la banque Royale, de la banque CIBC et de la Banque Honk Kong du Canada. Le Mouvement Desjardins procède également à une expérience en site réel au Complexe Desjardins de Montréal. Les autres expériences en cours portent le nom de Visa Cash, Mastercard Cash, Danmont, Proton, etc.

Développée au Japon au début des années '70, puis brevetée en France, la carte à puce de silicium est intéressante parce qu'elle utilise des algorithmes de sécurité. Mais la carte à puce est utilisée dans le cadre d'une opération de paiement où les acteurs sont physiquement présents : l'acheteur paye en introduisant sa carte dans un terminal spécialisé chez le vendeur. Dans ce cas, tous les questions juridiques attachées au paiement sont correctement gérés. Mais dans le cas de l'Internet elles se posent différemment les acteurs ne sont pas physiquement présents.

1.1.2. Carte à puce, signature et authentification

En France, la jurisprudence a admis en 1989 dans le cadre de l'affaire CREDICAS que l'emploi d'une carte à puce, comportant l'identification du porteur et la fourniture d'un code secret, équivalait à une signature électronique. Depuis, la signature électronique a été considérablement développée par les technologues. Elle présente désormais un avantage sur la signature manuelle, soit la garantie d'intégrité. L'intégrité est la qualité d'un document qui n'a pas été altéré volontairement ou involontairement pendant les traitements informatiques.

Au Québec, la législation et la réglementation ne proposent pas encore de définition précise de la notion de signature électronique, contrairement à ce que l'on observe depuis 1995 dans certains états américains comme la Floride ou l'Utah (Utah Digital Signature Law). Cependant, le nouveau code civil entré en vigueur en janvier 1994, propose néanmoins des éclaircissements sur les fonctions et les caractéristiques à respecter d'une signature (tant manuscrite, qu'électronique), et apporte également une ouverture importante en matière de

preuve des documents informatisés. Il faut tout de même souligner que nous ne disposons pas à l'heure actuelle de jurisprudence nous permettant de situer de façon éclairée l'interprétation des tribunaux québécois et canadiens face à la signature électronique, puisqu'aucun procès n'a encore eu lieu. La signature électronique est pourtant un élément fondamental pour assurer le déploiement rapide du commerce électronique.

Signalons à ce propos qu'une étude sur la signature électronique est actuellement en cours de publication aux éditions Yvon Blais. Cette étude innovatrice a été réalisée par le Centre de Recherche en Droit Public (CRDP) de l'Université de Montréal pour le compte d'un consortium formé d'organismes gouvernementaux et d'entreprises québécoises.

Par ailleurs, il est intéressant d'observer les cas d'utilisations actuelles de la signature électronique dans un contexte de télécommunications lors de la simple télétransmission de fichiers par exemple, ou encore lors de l'échange de documents informatisés (EDI) ou de l'utilisation du courrier électronique. Dans chaque cas, le document peut être altéré durant la télétransmission, soit par des actions humaines, soit par la simple intervention de la technologie.

Le contrôle de l'identification de l'émetteur d'un message et de l'intégrité de celui-ci apporté par la signature électronique arrive donc à point nommé pour garantir que le document n'a pas été altéré ou «pollué» pendant la télétransmission.

Puisque le système des cartes bancaires emprunte les réseaux informatiques internes des vendeurs, puis les réseaux de télécommunications fermés ou «privés» pour joindre les établissements bancaires, il serait intéressant de penser à adapter un tel système au télépaiement. Mais utilisé dans le cadre d'activité de télétransactions d'affaires, le système montre ses limites :

> l'authentification de la carte fonctionne pour l'acheteur. Par contre, le vendeur ne fait l'objet d'aucune vérification d'authentification : le paiement se déroule chez lui. Mais sur Internet, la question de l'authentification est double : elle est exigée du coté acheteur comme du coté vendeur. Il en est ainsi parce que les deux ne sont pas en présence physique l'un de l'autre ; des services frauduleux pourraient proposer de fausses ventes pour empocher de vrais paiements.
>
> les informations confidentielles des cartes, comme le numéro de la carte bancaire et le code secret, peuvent être écoutés sur le réseau et reproduits pour provoquer de faux paiements. Le Code secret est un identifiant composé principalement de la fusion (ou concaténation) du numéro de série de la carte, du numéro de carte bancaire et de la date d'expiration de la carte. Le tout est codé par un algorithme de clés publiques de type RSA. (Voir le texte : «L'EDI est-ce sécuritaire ?» publié dans Micro-Gazette de juin-juillet 1995). Ce code est un bon moyen d'authentification. Mais il n'est pas une signature électronique, car il lui manque la garantie d'intégrité. Par opposition avec la signature électronique qui change selon le contenu du message, le code secret lui reste toujours identique.

Il ne faut pas perdre de vue qu'il existe deux grandes approches dans la protection des informations sur les autoroutes de l'information. On peut tenter de sécuriser l'ensemble du réseau de transmission (ce qui est impensable actuellement dans le cas des réseaux très ouverts tel INTERNET), ou encore, sécuriser ou «blinder» les messages eux-mêmes. Cette exemple vaut également pour les autoroutes automobiles où il est préférable de ne pas trop s'aventurer dans certaines régions reculées riches en brigands, sans y «sécuriser» au préalable son véhicule en s'assurant à tout le moins de son bon fonctionnement.

1.1.3. Signature et chiffrement (cryptologie)

La signature électronique est un moyen de sécurité des transactions électroniques aussi bien au niveau technique que juridique. A son tour, la signature peut être sécurisée par l'usage de la cryptologie.

La cryptologie ou chiffrement permet de rendre illisibles les informations contenues à moins d'un traitement approprié. En terme de sécurité, la cryptologie peut apporter plusieurs garanties:

- si elle permet de rendre illisible le contenu d'un message, elle en garantit la confidentialité ;

- si elle permet de rendre infalsifiable le contenu d'un message, elle en garantit l'intégrité ;

- si elle permet de rendre infalsifiable le contenu d'un message et permet en même temps l'ajoût d'un identifiant garantissant l'identité de l'émetteur, elle en garantit alors l'authentification;

Mais la garantie de confidentialité ne va pas sans poser de problèmes juridiques puisqu'elle empêche la lecture légitime du message par des personnes autres que l'émetteur et le destinataire, à savoir l'Etat, l'armée et la police. Aussi certains pays possèdent des législations plus ou moins restrictives sur l'utilisation de la cryptologie. Aux Etats-Unis elle est considérée comme une technologie stratégique à exportation contrôlée. En France, la récente loi du 26 juillet 1996 sur la réglementation des télécommunications réclame une autorisation du Premier ministre, sauf si l'utilisateur passe par les services d'un «tiers certificateur». Au Québec et ailleurs au Canada, la cryptologie n'est pas encore affectée par de telles restrictions.

1.2 Le télépaiement sur Internet

1.2.1. Particularités de paiement sur Internet : l'absence et la présence de tiers

La situation juridique est simple lorsque les personnes échangeant un document ou des informations transactionnelles sont en présence. Les relations juridiques peuvent se dérouler dans un environnement sûr. En effet, le contrôle du bon déroulement des opérations et de leur régularité peut être fait sans difficulté par l'oeil des personnes.

Au contraire, l'absence physique rend incertains les éléments juridiques suivants : la capacité et la compétence, l'accord des acteurs sur l'opération en cours, la datation de l'opération, la preuve pour ne mentionner que ces éléments.

Une autre pratique actuelle dont il faut tirer des enseignements existe implique l'intervention des tiers. L'utilisation de signature électronique suppose assez largement l'intervention de tiers, soit pour décoder la signature électronique, soit pour mettre à disposition du public les clés publiques, lorsque la signature électronique est codée par un système de cryptologie à clé publique, tel RSA.

La Commission de Bruxelles, qui s'intéresse à ces questions depuis plusieurs années, a développé un programme d'études de «Tiers Certificateurs» ou «autorité de certification», appelé aussi "Trusted Third Party" lors de la conférence de BARCELONE tenue en 1994.

Ces travaux ont un équivalent aux Etats-Unis avec la commission CyberNotary ou DigiNotary (ou notaire électronique) de l'American Bar Association.

1.2.2. L'offre de services sur Internet et essai de typologie

On peut tenter de dresser la typologie suivante des services disponibles sur le Web en matière de télépaiement:

1) Nouveaux mode de paiement

- "Monnaie électronique" : l'exemple de DIGICASH. Le client est crédité d'une somme d'argent en CyberBucks, stocké sur son disque dur, comme dans un porte-monnaie. Pour paiement de toute somme, l'acheteur prélève sur son crédit, disponible sur son disque dur et crédite le vendeur.

- Porte-monnaie électronique et carte bancaire : l'exemple de «Global OnLine (GOL)» de France. C'est un service avec deux modes de fonctionnement. Les petites sommes sont gérés par un système de porte-monnaie électronique. Les sommes plus importantes sont payés par le système bancaire via le service GOL. Les messages de paiement de l'acheteur sont cryptés et ne comprennent pas d'identifiant bancaire, mais l'identifiant GOL.

2) Prolongement du système bancaire et de carte à puce

- Alliance du WEB et des cartes : l'exemple FIRST DATA / NESTCAPE Il s'agit de l'adaptation à Internet du paiement par Carte bancaire. Le site WEB du vendeur reçoit la transaction de paiement authentifiée par la carte bancaire de l'acheteur. La transaction générée par le navigateur Netscape a été préalablement cryptée.

- L'adaptation de la carte bancaire à Internet : l'exemple de VISA / MasterCard - EuroCard. Le système consiste à "prolonger" les moyens existants. Ainsi le système des cartes à puce peut être adapté pour être employé plus efficacement sur le réseau (norme commune SET, Secure Electronic Transactions).

3) Intermédiation avec le système bancaire

- Interface avec le système bancaire : l'exemple de CYBERCASH. Le client envoie une requête cryptée au centre serveur CyberCash. Le centre serveur se connecte à la banque comme un "Terminal Point de Vente" (TPV) classique pour validation du paiement.

- Intermédiation avec le système bancaire : l'exemple de FIRST VIRTUAL (F.V.). Le vendeur adresse un message électronique au site WEB de First Virtual. Le serveur de F.V. interroge le client par courrier électronique sur la transaction de paiement : refus ou acceptation ? Si le paiement est accepté, le paiement est transmis à F.V. par le circuit bancaire traditionnel.

- Paiement dans la boutique virtuelle : l'exemple de OPEN MARKET Le service de Open Market (O.M.) est une véritable boutique électronique. Le client effectue son paiement crypté au site WEB de O.M. à partir de son navigateur et de sa carte bancaire.

2. LES SERVICES TRANSACTIONNELS DE L'AVENIR : UNE RÉCONCILIATION ENTRE LE PAIEMENT ET LA VENTE

La prise en compte de la vente, antérieure au paiement, alimente une réflexion qui distingue les entreprises et les particuliers.

2.1. Le régime de la vente

2.1.1. La vente et l'absence physique des parties

Toute vente est un contrat c'est-à-dire un échange de volonté entre les parties, qu'elle implique des personnes physiques (particuliers) ou les personnes morales (entreprises). Le contrat de vente se caractérise d'un côté par la fourniture d'un bien, ou d'un service et de l'autre par le paiement. La fourniture d'un bien ou d'un service et l'activité de paiement sont donc directement liés dans le processus normal des affaires.

Lorsque les personnes sont présentes, la sécurité juridique est grande : le contrôle visuel permet des vérifications à priori qui sont généralement suffisantes. Par exemple, un premier niveau d'identification (âge, fonction, appartenance à l'entreprise, etc...). Ce niveau d'identification est souvent suffisant pour éviter tout besoin d'authentification additionnel.

On peut signaler que le contrat de vente n'est pas obligatoirement écrit, la simple rencontre des volontés suffit pour lier les parties et créer un contrat. De même, l'usage commercial peut pallier à l'établissement d'un contrat écrit. Par exemple, lorsque l'on consomme à un restaurant il est d'usage de payer avant de quitter les lieux même si cela ne figure habituellement pas de façon explicite dans les textes législatifs.

Mais lorsque le contrat est écrit, il est signé. La signature est un élément important de la validité du contrat et ultérieurement de sa preuve. Lorsque le contrat est conclu par écrit entre les personnes présentes, le contrôle visuel permet encore de constater que le vendeur est aussi le signataire. Le contrôle est le même pour l'acheteur.

2.1.2. Typologie sommaire des ventes

Les ventes peuvent être classées de différentes façons. On ne retiendra ici que la typologie dépendant de la qualité des personnes. Les systèmes juridiques de "droit civil" attachent habituellement plus d'effets à la «qualité» des personnes, que les systèmes juridiques de "common law". En effet, les systèmes de droit civil, particulièrement en France, qualifient de :

- «contrat civil», les ventes entre particuliers et les placent sous l'empire d'un "droit civil". Ce droit fait souvent référence à un écrit obligatoire.

- «contrat commercial», les ventes entre entreprises et les placent sous l'empire d'un "droit commercial". Ce droit laisse place à une plus grande liberté.

Pour remédier à une situation défavorable pour les particuliers face aux professionnels de la vente, les États élaborent souvent un "Droit de la Consommation" qui protègent les consommateurs.

On mesure la difficulté d'auditer une situation de téléachat qui mettrait en présence entreprise et particulier, d'une part, et pays de droit civil et pays de common law, d'autre part. Quant au droit des consommateurs, qui doit sécuriser l'acheteur vis à vis d'un vendeur professionnel, il devient généralement inapplicable si le vendeur appartient à un pays différent.

La situation de l'acheteur-consommateur est donc précaire dans un téléachat avec un vendeur d'un autre pays, puisqu'aucune loi n'arrive à s'appliquer directement. Il y a une grande différence de situation entre particulier en entreprise dans la pratique de la vente : le particulier se trouvera souvent dans une relation d'affaire occasionnelle et dans un achat unique ; l'entreprise quant à elle, peut se trouver plus souvent dans une relation d'affaire continue et dans des opérations d'achat fréquentes.

Entre entreprises en relations d'affaires continues, on peut identifier ses partenaires et se doter d'un cadre juridique sur mesure, même dans un contexte international, un contrat spécifique. Le contrat vient suppléer la loi inexistante. Toutefois il peut s'ensuivre, comme dans les pays de common law, une "bataille des formes" (battle of forms) entre les conditions générales de vente de l'un et les conditions générales d'achat de l'autre.

En pratique, il est nécessaire de distinguer le télépaiement entre entreprises et celui qui intervient entre entreprise et particulier.

2.2 Vers de nouveaux services et une nouvelle intermédiation

2.2.1 Le paiement dans le Commerce électronique entre entreprises.

Comme le concept d'Autoroute de l'Information, le concept de «commerce électronique» a d'abord émergé aux États-Unis. Il a été utilisé pour la première fois en octobre 1990 à l'University of Southern California. Il a été par la suite largement utilisé par le ministère américain de la défense (US-DOD). Mais c'est véritablement le vice-président américain Al Gore qui l'a rendu public lors de la campagne électorale de 1992.

Le commerce électronique repose actuellement sur les technologies inter-organisationnelles suivantes :

. EDI & EDI Financier

. Télécopie & serveur de télécopie (ex: télécopie de formulaires à la demande)

. Courrier électronique public

. Babillard électronique

. Commande électronique (catalogue électronique, audiotex, ...)

. Code à barres (ex: pour le contrôle des inventaires)

. Production / Livraison "juste-à-temps"

. Intranet & Internet

Signalons que ces technologies peuvent être utilisées de façon complémentaires afin de contribuer à relever les défis actuels de gestion, c'est à dire : produire de façon plus rapide et plus efficace des biens et services de meilleure qualité, et ce, au moindre coût possible.

Le commerce électronique est géré directement entre les entreprises partenaires. Comme pour l'EDI où la communication électronique est gérée par un contrat spécifique ou «accord d'interchange», le commerce électronique peut être régulé par un contrat. Classiquement, ce contrat spécialisé sera une «Convention pour le commerce électronique».

Pourtant ce type de procédé contractuel comporte des limites en soi. En effet, le contrat est conclu entre partenaires qui se connaissent. Le contrat s'accorde mal dans le cas des relations électroniques "ouvertes" où les acteurs sont en contact pour la première fois et peut être même pour la dernière fois. Ainsi, émerge pour l'entreprise le besoin d'énoncer à l'avance de façon unilatérale les circonstances et le contexte dans lesquels elle acceptera l'utilisation des technologies. Elle ne commercera qu'avec l'entreprise qui acceptera préalablement ces conditions.

Il faut dès lors mettre à la disposition des entreprises les moyens de déclarer à l'avance ces prérequis. Ces moyens devront se prêter ultérieurement à l'incorporation par référence dans l'instrument juridique qui réglera leurs relations. C'est la vocation des «Profils de commerce électronique».

Une bibliothèque (physique et/ou virtuelle) pourrait bientôt être mise en place afin de réunir les «Profils de commerce électronique» permettant à chacun de s'y référer pour connaître les détails de la pratique du commerce électronique par les entreprises. Cette bibliothèque devrait être accessible sur un site WEB appartenant à une «Agence de gestion du commerce électronique». Cette agence serait une véritable «Autorité d'Enregistrement et de Certification» au sens des études de la Commission de l'Union Européenne et des travaux de l'association des juristes américains (American Bar Association).

Quelques initiatives sont en cours actuellement au Canada afin de favoriser dans un avenir prochain: (1) l'accès à l'identification exacte et la description des entreprises dans des répertoires électroniques (ou annuaires) de type X.500, (2) l'enregistrement électronique des entreprises auprès des autorités compétentes, tel l'Inspecteur général des institutions financières du Québec, (3) le paiement des transactions via l'obtention de lettre de crédit électronique, par exemple, et finalement, (4) l'émergence d'autorité d'enregistrement et de certification des transactions. Signalons simplement les travaux de la Chambre des Notaires du Québec sur ce dernier point.

2.2.2 De nouveaux services pour garantir les consommateurs

Parmi les acheteurs potentiels des services Web, les simples particuliers peuvent être les plus dépourvus. Face à la «jungle» des affaires, ils bénéficient normalement de la protection des

consommateurs. Mais comment faire appliquer une loi nationale spécifique sur le marché international que constitue la "toile mondiale" (WEB) et le «village global». Pourtant la protection des consommateurs peut être facilitée par une nouvelle catégories d'intermédiaires techniques.

Depuis 1985, la Commission Européenne (Directive du 20 déc. 1985) a arrêté les principes généraux de la protection des consommateurs dans le cas de contrats négociés en dehors des établissements commerciaux. Ces principes sont passés progressivement dans la législation des États européens. Aussi un intermédiaire installé dans un pays européen pourrait proposer des garanties respectant la législation européenne et qui mettrait en confiance un acheteur de bien sur un site Web extra-européen.

Un principe majeur de la protection du consommateur est le suivant : le consommateur ne sera pas définitivement engagé tant qu'il n'aura pas expressément accepté une offre précise faite par le vendeur après le premier contact à distance. En général, les juristes considèrent que cette confirmation prend la forme d'un écrit signé par l'acheteur. Mais les lois ne sont généralement pas aussi précises.

Si la protection du consommateur exige une confirmation écrite signée après une "intention" de téléachat, le WEB commercial aura du mal à prendre son envol. En appliquant une attitude novatrice, on aboutirait à la procédure suivante, qui serait susceptible de garantir le consommateur :

- la prise de commande du consommateur sur le WEB du vendeur entraînerait l'émission d'un message de courrier électronique du vendeur au consommateur.

- Ce dernier pourrait tout simplement le retourner (fonction quasi-automatique des gestionnaires de courrier électronique) au vendeur par un courrier électronique, revêtu d'une signature électronique.

La protection du Code de la Consommation en France comporte aussi des dispositions sur le paiement. Sans celles-ci, la protection serait étriquée, car elle ne couvrirait pas le portefeuille du consommateur. La protection du consommateur lui permet de renoncer à son achat et même dans certains cas, de renvoyer le bien. Dans ce dernier cas, si un paiement a été effectué, il doit être restitué au consommateur. La situation est similaire au Québec avec les lois et règlements touchant à la protection des consommateurs.

Les services de télépaiement actuels ne semble pas capables d'assurer cette opération. Pourtant un service d'intermédiation électronique pourrait proposer une consignation du paiement électronique pendant le délai de repentance du consommateur. Ce délai est habituellement de 10 jours ouvrables au Québec. Cette fonctionnalité aurait l'avantage de protéger le consommateur et d'assurer l'application de la loi du consommateur même pour un site Web situé à l'étranger.

Conclusion

Comme on le voit, des opportunités de services de télépaiement nouveaux apparaissent dès qu'on intègre l'aspect télépaiement à la problématique plus large du commerce électronique. Il est formateur de distinguer les cas où les entreprises et des particuliers ont transigé ensemble dans des pays ayant des régimes juridiques et des fuseaux horaires différents. A partir de cela, on peut construire une argumentation juridique en faveur du télépaiement lié à la vente à distance.

Il est certain que le commerce électronique sur Internet ne pourra devenir une réalité tant que les opérations commerciales ne s'achèveront pas par des paiements. Des services de télépaiement sur INTERNET émergent tous les mois, pourtant ils ne semblent pas bénéficier pour le moment de la confiance des consommateurs et des gens d'affaires. Cette confiance est une condition essentielle au succès des télépaiements sur le Web.

ANNEXE # 1

Évolution des moyens de paiement

- Échange par Troc
- Paiement avec des objets (ex: perles, billes, etc)
- Monnaie d'entreprise
- Monnaie nationale
- Chèque bancaire
- Mandat et traite bancaires
- Carte à piste magnétique
- Carte à puce

ANNEXE # 2

Propriétés des cartes à puce utilisées pour le paiement

- Échange de fonds de «personne à personne»
- Échange de fonds de «personne à entreprise»
- Multifonctions (crédit, débit, monnaie électronique)
- Plusieurs monnaies accessibles simultannément
- Messages multilingues avec les utilisateurs
- Protection possible par mot de passe, si désirée
- Recharge à l'aide de téléphones publics, de guichets bancaires ou de terminaux point de vente
- Utilisation simple, pratique et peu coûteuse

ANNEXE # 3

Caractéristiques à respecter des moyens de paiement

- Utilisation simple et pratique
- Support peu coûteux à reproduire
- Durabilité du support
- Valeur négociable au porteur
- Valeur reconnue par l'ensemble de la société

ANNEXE # 4

Sécurisation des informations sur les inforoutes

- Disponibilité (continuité) des systèmes d'information
- Contrôle d'accès aux systèmes
- Identification de l'émetteur et du récepteur du message
- Confidentialité des informations
- Intégrité des informations
- Authentification du message
- Non-répudiation par l'émetteur

Cybernews Volume 2, numéro 2 (printemps 1996)

(*) M. Thierry PIETTE-COUDOL est avocat au Cabinet André Bertrand & Associés, Paris (FRANCE)
M. Yvan LAUZON agit à titre de coordonnateur EDI au gouvernement du Québec (SCT). Il est également chargé de cours à l'Université de Montréal

---

 ISSN 1201-7302