Le paiement électronique
(expérience québécoise et française)

Madadi Abdelkader
C.U. KHEMIS MILIANA

Résumé:

Les mécanismes de paiement électronique sont analysés ici. Aussi, même si d'un point de vue strictement juridique le paiement correspond à toute exécution d'une obligation, il sera plutôt abordé comme le simple paiement d'un montant d'argent au commerçant par le consommateur. Cette définition plus restrictive convient mieux à la situation du commerce électronique.

Entendu de cette façon, le paiement est caractérisé par deux principes fondamentaux.

Tout d'abord, celui-ci doit être exact. Il n'est donc pas possible de forcer le créancier à recevoir autre chose que ce qui était prévu entre les parties. Ensuite, le paiement doit être total et en un seul versement. Les paiements échelonnés ne sont donc possibles que si le créancier y consent. Le paiement effectué dans ces circonstances est libératoire, c'est à dire qu'il éteint l'obligation.

Ces deux caractéristiques soulignent la nature essentiellement consensuelle du paiement.

En effet, même si certaines règles encadrent son déroulement en cas de silence des parties, celles-ci ont presque toujours la possibilité d'en convenir autrement. De plus, l'obligation sous-jacente au paiement joue également un rôle important dans la détermination des règles qui lui sont applicables. Ainsi, le paiement s'effectuant dans le cadre d'un contrat de vente peut être soumis à des règles différentes que le paiement résultant d'un contrat de service. Le paiement apparaît donc comme un mécanisme juridique relativement souple, capable de faire face aux exigences du commerce électronique.

Introduction

Notre étude porte sur une présentation des exemples de payement électronique dans deux pays (France et canada), on a traité les points suivants :

Introduction :

1. **présentation d'exemples concrets ;**
2. **e-paiement par carte de crédit ;**
3. **Coûts de transaction et rapidité d'exécution ;**
4. **Chèques électroniques ;**
5. **Coût de communication ;**

Conclusion.

1. présentation d'exemples concrets :

Encadré 01 : Exemple de la vente à distance en droit québécois

Au Québec, le contrat de vente à distance constitue une exception majeure au principe de la liberté contractuelle relative au moment du paiement. L'article 22 de la Loi sur la protection du consommateur prévoit que «[…] le commerçant qui sollicite la conclusion d'un contrat à distance ou qui conclut un tel contrat ne peut demander un paiement partiel ou total au consommateur ou lui offrir de percevoir un tel paiement avant d'exécuter son obligation principale.». Le moment du paiement est donc spécifiquement repoussé après la livraison du bien ou de la prestation du service prévus dans le contrat. Néanmoins, le commerçant peut déroger à cette disposition s'il dépose une caution suffisante auprès de l'Office de protection du consommateur du Québec.

Encadré 02 : Exemple de quittance électronique

Le roi du machin Inc.
1234 Rue du marais
Montréal, Québec A1B 2C3
(514)012-3456 Fax: (514)789-1011
De 9:00 am à 17:00 pm
de commerçant :
Reference:
Adresse de l'acheteur: Adresse d'envoi:
Pierre-Paul Lemyre Pierre-Paul Lemyre

1234 Boissy 1234 Boissy
Laval, Québec Laval, Québec
Z0Y 9X8 Z0Y 9X8
Canada Canada
E-Mail: lemyrep@lexum.umontreal.ca
Tel: 514 098-7654
Fax:
Information sur la Commande:
Date : 01/06/00 Num de Commande: 10302
Facture #: 10302 Add IP : 64.228.204.114

_____
__
Description de la commande
Qu Code du Produit Description Prix unité Prix

_____
__
1 1003150 SUPER MACHIN 3150 77.99 77.99

_____
__
Sous-Total: 77.99 $
Poste: 0.00 $
Manutention: 0.00 $
TAXES: 11.72 $
TOTAL 89.71 $
MONTANT PAYÉ 89.71 $
BALANCE DÛE 0.00 $
Méthode de paiement:
Chèque
C.O.D.
X Visa
Master Card

American Express
En Route / Diners Club
Nom: Pierre-Paul Lemyre
Num: 4530XXXXXXXX8010
Exp: 0001
Votre devise monétaire est: Canadian Dollar

Votre taux de change est: 1$ CDN= 1.00000 Canadian Dollar
Le total dans votre devise est (89.71 * 1.00000) = 89.71 Canadian Dollar

2. e paiement par carte de crédit :

Le paiement par carte de crédit a l'avantage d'être simple et rapide, ce qui permet au commerçant de recevoir la confirmation du paiement avant d'exécuter son obligation.

Pour avoir la possibilité d'offrir ce mode de paiement à sa clientèle, le commerçant doit contacter les compagnies émettrices de cartes de crédit par le biais d'une banques ou directement par leur site Web. Pour assurer le fonctionnement du mécanisme, ces compagnies encadrent leurs relations avec le commerçant et le détenteur de la carte par différents contrats. Ces ententes permettent la mise en place d'un mécanisme de transfert de créance. Ainsi, pour le consommateur, l'utilisation d'une carte de crédit ne constitue pas véritablement un moyen de paiement puisque celle-ci lui permet de remettre le coût de ses achats à plus tard en lui procurant du crédit. Toutefois, pour le commerçant, il s'agit d'un paiement car l'émetteur de la carte lui remet ce qui lui est dû. En agissant de la sorte, la compagnie émettrice acquiert la créance du commerçant envers le consommateur.

Au premier abord le paiement par carte de crédit semble parfaitement adapté au contexte du paiement sur Internet puisque ce mécanisme ne nécessite pas la présence physique des parties. Il suffit, pour compléter la transaction, que le consommateur fournisse le numéro et la date d'expiration de sa carte au commerçant. Ce dernier n'a plus qu'à transmettre ces informations à sa banque qui lui confirme la transaction. Cette façon de procéder est utilisée depuis de nombreuses années dans le cadre de la vente par correspondance et de la vente à distance. Toutefois, dans la mesure où les renseignements fournis ne contiennent aucune information spécifique au client, rien ne prouve que le consommateur est le détenteur réel de la carte utilisée. Ceci représente un risque important pour le commerçant car la législation lui fait assumer les pertes de l'opération en cas de fraude.

En France, la personne victime d'un vol de carte de crédit a quatre-vingt-dix jours pour annuler les transactions frauduleuses. Au États-Unis ce délais est de trente jours et la loi limite la responsabilité du consommateur à 50$. Dans ces circonstances les commerçants craignent le non-paiement de leur marchandise, ce qui constitue un frein au développement du commerce électronique. Malgré tout, certaines mesures de sécurité peuvent être

utilisées par le commerçant afin de réduire au minimum les risques de fraude par carte de crédit.

Encadré 24 : Mesures à prendre pour s'assurer de la validité d'une transaction par carte de crédit

La fraude par carte de crédit est un problème auquel tous les commerçants électroniques font face un jour ou l'autre. Comme la responsabilité de vérifier la légitimité de la transaction repose principalement sur le commerçant, il est important que celui-ci connaisse les mesures à prendre pour s'assurer de sa validité.

Il faut d'abord comprendre que le lorsqu'une transaction se déroule sur un site Web, l'affichage "TRANSACTION APPROUVÉE" ne garantie pas au commerçant que la transaction se déroulera sans problème.

Cette réponse de la banque implique seulement que le numéro de la carte est valide et que la limite de crédit de celle-ci n'est pas excédée.

Par contre, rien n'indique que la personne effectuant l'achat est bel et bien le détenteur de la carte.

Le code de réponse AVS constitue un outil beaucoup plus important.

Tous les systèmes de paiement par carte de crédit ne produisent pas automatiquement un tel code. Il appartient donc au commerçant de s'informer sur la manière d'obtenir cette information essentielle. AVS signifie Address Verification Service (Service de vérification d'adresse).

Ce code indique si l'adresse entrée par le consommateur est la même que l'adresse du détenteur de la carte. Si les deux adresses sont identiques et que la commande doit être livrée à cette même adresse, il n'y a généralement pas de raison de douter de la validité de l'achat et les chances que le détenteur de la carte conteste l'achat sont minces.

Par contre, si les deux adresses ne correspondent pas, le commerçant est justifié d'effectuer des démarches supplémentaires.

Dans cette situation, le commerçant devrait communiquer lui-même avec la compagnie émettrice de la carte et demander le numéro de téléphone de la banque du détenteur. En appelant à cette banque et en demandant une vérification du détenteur de la carte, le commerçant a la possibilité de vérifier à nouveau l'adresse fournie avec, cette fois, les données de la banque. Parfois, la différence est simplement causée par de l'information désuète. La banque peut également comparer le nom et le numéro de téléphone du détenteur de la carte, ce qui donne plus d’assurance quant à

l'information fournie par le consommateur. Il est alors plus facile pour le commerçant de décider s'il prend le risque d'envoyer la marchandise.

Néanmoins, il faut comprendre que même si l'adresse fournie est identique à celle du détenteur de la carte, il peut tout de même s'agir d'une fraude. En effet, il arrive que les fraudeurs aient accès à l'information concernant l'adresse de la victime. Le commerçant doit donc être vigilant lorsque le consommateur désire faire livrer sa marchandise à un autre endroit. Il faut porter une attention particulière aux biens commandés ainsi qu'aux quantités. Les commandes frauduleuses concernent presque toujours des achats coûteux. La méthode de livraison choisie constitue un autre indice. Les fraudeurs désirent mettre la main sur les biens le plus tôt possible et ils choisiront généralement l'option la plus rapide qui leur est proposée. L'adresse de courrier électronique du consommateur révèle aussi des signes. En cas de doute il est possible de vérifier si celle-ci est valide et, si le nom d'une personne y figure, de vérifier si ce nom correspond à celui du détenteur de la carte. Chaque commerçant doit donc établir sa propre politique de vérification et décider dans quelles situations il refusera d'envoyer la marchandise commandée.

En résumé, la procédure suivante devrait être suivie :

1) Vérification de l'autorisation par l'institution de crédit

2) Vérification du code AVS

A) Réponse négative :

i) Communiquer avec l'institution de crédit afin d'obtenir le numéro de téléphone de la banque

ii) Communiquer avec la banque afin d'obtenir une vérification du détenteur de la carte

B) Réponse positive :

i) Vérification de l'adresse de livraison

ii) Vérification du type et de la quantité de biens commandés

iii) Vérification de la méthode de livraison

iv) Vérification de la validité de l'adresse de courrier électronique fournie.

Toutefois, le principal obstacle à l'utilisation des cartes de crédit dans les environnements électroniques est la peur qu'ont beaucoup de consommateurs de se faire voler les informations relatives à leur carte. Les consommateurs redoutent surtout l'interception de ces renseignements au moment de leur transmission sur le réseau. Pourtant, lorsqu'un procédé cryptographique est utilisé, ce risque est pratiquement inexistant. Le danger vient plutôt des données sauvegardées sur les serveurs de transactions. Celles-ci deviennent

alors la cible des fraudeurs. Ces derniers, s'ils réussissent à s'introduire dans le système informatique des commerçants, peuvent subitement mettre la main sur des milliers de numéros de carte de crédit. Ces données doivent donc être particulièrement bien protégées pour que les consommateurs acceptent d'y ajouter leurs propres numéros de carte. Il n'en demeure pas moins que cette crainte est souvent largement exagérée. En effet les cas de fraude sont relativement rares et, dans tous les cas, ce sont les commerçants, et non les consommateurs, qui en font les frais.

Finalement, une dernière limite vient restreindre l'utilisation des cartes de crédit dans le cadre du commerce électronique. Celle-ci a trait au coût de transaction élevé qui s'attache à ce moyen de paiement. L'utilisation de la carte de crédit est donc viable uniquement lorsque le prix à payer est supérieur à un certain montant. Par contre, le contexte des environnements électroniques permet d'envisager une multitude de situations où le commerçant aurait avantage à offrir ses services à un prix inférieur. Par exemple, la consultation de pages Web sur le site d'un fournisseur d'information pourrait être facturée sous la forme d'un montant infime pour chaque page consultée. Ces micro-transactions ne sont définitivement pas envisageables dans le contexte du paiement par carte de crédit.

La carte de crédit est néanmoins le mode de paiement le plus utilisé actuellement sur les réseaux électroniques. Ceci s'explique principalement par sa facilité d'utilisation qui permet à la majorité de la population d'y avoir recours. Son important taux de pénétration dans les pays industrialisés assure également les commerçants qu'un grand nombre de consommateurs potentiels disposent des moyens techniques nécessaires pour transiger via Internet. Il est donc essentiel pour le commerçant électronique d'offrir la possibilité au consommateur de payer par carte de crédit.

L’utilisation des moyens traditionnels de paiements augmente dramatiquement les délais de transaction: le paiement pourra prendre plusieurs jours pour parvenir au commerçant, comparativement à quelques secondes pour le paiement en ligne. De plus, cela implique des déplacements de la part du consommateur qui ne sont pas nécessaires lorsque le paiement est effectué électroniquement. En somme, bien que les modes traditionnels de paiement ne puissent être mis de côté, il demeure avantageux d'inciter la clientèle à utiliser l'alternative électronique.

De plus, les moyens traditionnels de paiement commencent à s'adapter eux aussi aux nouveaux environnements dématérialisés. Ainsi, sous l'impulsion d'entreprises privées, différentes monnaies électroniques ont vu le jour. Ces

mécanismes remplacent l'utilisation de la monnaie habituelle par de nouvelles valeurs n'ayant pas cours légal.

L'effet libératoire de ces monnaies ne tient donc qu'au cadre contractuel existant entre le commerçant et le consommateur. De plus, elles ne reposent sur aucun support physique.

Elles peuvent donc être conservées dans des portes-monnaie électroniques qui se trouvent sur des cartes à puce ou sur le disque dur des ordinateurs et que l'on débite au moment de l'achat. Tout comme pour la monnaie classique, ces pièces électroniques ne sont pas la propriété de la personne qui les possède. La valeur monétaire de ces monnaies est habituellement basée sur la valeur de devises traditionnelles, bien que certaines établissent leur propre unité. Celles-ci sont légales dans la mesure où elles s'insèrent dans un accord contractuel entre les parties. Par contre, elles ne bénéficient pas des avantages accordés par la loi à la monnaie ayant cours légal, tel que la protection de l'État contre la destruction ou la contrefaçon.

De la même façon, il est aujourd'hui possible de remplir des chèques électroniques.

Toutefois, il n'est pas certain que ceux-ci constituent véritablement des chèques au sens entendu par les différentes législations. La première difficulté pouvant surgir a trait au caractère écrit des chèques traditionnels. En fonction de l'interprétation des diverses législations sur le sujet, il n'est pas certain que les chèques informatisés, qui sont des documents sur support informatique, soit considérés comme l'équivalent d'un écrit. La seconde difficulté concerne la signature. Bien que certaines juridictions reconnaissent maintenant la validité de la signature électronique, il ne s'agit encore que de quelques exceptions. Dans la majorité des États, les chèques électroniques seront invalides parce qu'ils seront considérés non signés. Finalement, une troisième difficulté peut être envisagée du fait que le tireur d'un chèque électronique perd sa possibilité de le contremander. En effet, un chèque traditionnel est révocable jusqu'à sa présentation alors que la vitesse des communications électroniques confère un caractère instantané à cette étape. Il est donc possible que, dans certaines juridictions, cette perte de droit pour le tireur empêche le chèque électronique d'être considéré comme un véritable chèque. Dans ces circonstances, il serait difficile de prétendre que le commerçant à l'obligation d'accepter le chèque électronique, même dans les juridictions où le chèque certifié par une institution financière possède un effet libératoire. Malgré cela, tout comme pour la monnaie électronique, rien n'empêche les parties de s'entendre sur l'utilisation de ce moyen de paiement.

La charge de la preuve pèse toujours sur celui qui invoque l'extinction d'un droit. Aussi, celui qui se prétend libéré doit justifier le paiement ou tout autre fait qui a éteint son obligation envers son co-contractant. Cependant, pour le consommateur, ce fardeau de preuve peut parfois s'avérer difficile à remplir dans le cadre d'une transaction électronique. En effet, celui-ci dispose rarement des moyens techniques lui permettant de conserver les éléments de preuve qui lui sont utiles. Il n'a souvent pas d'autre choix que de se fier aux enregistrements informatiques fournis par le commerçant, et sur lesquels il n'a aucun contrôle.

De plus, dans les pays de conception civiliste, le droit privilégie fortement l'utilisation de la preuve écrite. En effet, la preuve d'un acte juridique nécessite généralement l'existence d'un écrit. Comme le fait juridique peut, à l'opposé, être prouvé par tous les moyens, certains juristes se sont questionnés sur la nature même du paiement. Aujourd'hui, il semble incontestable que le paiement constitue un acte juridique, puisque celui-ci possède les deux caractéristiques nécessaires : il s'agit de la manifestation d'une volonté individuelle et celle-ci s'exerce avec l'objectif de produire des effets juridiques. Ainsi, en l'absence d'un écrit, le consommateur sera dans l'impossibilité de prouver le paiement.

Puisqu'il n'est pas certain que les documents sur support informatique pourront correspondre à des écrits au sens entendu par toutes les législations, beaucoup de consommateurs risquent de se retrouver sans moyen de preuve. Par contre, certaines juridictions accordent déjà des régimes particuliers de preuve pour les inscriptions informatiques. Par exemple, au Québec, celles-ci font preuve de l'acte juridique si elles sont intelligibles et si elles présentent des garanties suffisamment sérieuses pour qu'on puisse s'y fier.

Cette règle exigeant l'écrit fait toutefois l'objet de plusieurs exceptions, sous réserve des législations nationales. Premièrement, le paiement des petites créances peut habituellement être prouvé par tous les moyens de droit : présomptions, témoignages, aveu... Ceci se comprend dans la mesure ou les parties ne se donnent pas toujours la peine de dresser un écrit pour une transaction de faible valeur. Deuxièmement, les matières commerciales peuvent aussi faire exception. C'est, entre autres, le cas en droit français dont le Code de commerce établit la liberté de la preuve entre les commerçants.

Troisièmement, il est probable que la preuve par l'écrit ne sera pas obligatoire lorsqu'il n'aura pas été possible au consommateur de se la procurer, malgré sa bonne foi et sa diligence. Cette exception est

particulièrement pertinente dans le cadre du commerce électronique dont le contexte ne permet pas la rédaction d'un écrit traditionnel.

Quatrièmement, l'existence d'un commencement de preuve peut parfois permettre au consommateur d'invoquer d'autres moyens de preuve par la suite. Par exemple, l'aveu ou l'écrit émanant de la partie adverse, son témoignage ou la présentation d'un élément matériel constitue des commencements de preuve. De là l'importance pour le consommateur d'obtenir une quittance. Cinquièmement, comme certains auteurs prétendent que cette exigence de l'écrit n'est pas impérative, il serait peut-être possible pour les parties d'y déroger par une convention précisant que les opérations juridiques effectuées sur le réseau peuvent être prouvées par tous les moyens. Si ces prétentions s'avèrent fondées, les commerçants ayant recours à de telles conventions pourront éventuellement se voir opposer des inscriptions électroniques rassemblées par les consommateurs.

3. Coûts de transaction et rapidité d'exécution

Pour que l'utilisation d'un mécanisme de paiement soit avantageuse, les frais relatifs à son utilisation doivent être peu élevés. Parmi les facteurs contribuant à faire augmenter les coûts de transaction, le principal consiste à recourir à un tiers afin de compléter le processus de paiement. Il n'est pas difficile de comprendre que les frais augmentent rapidement lorsque les parties doivent rémunérer une personne supplémentaire pour prendre le paiement en charge. Le degré d'automatisation influence également les coûts de transaction. Lorsque la supervision de personnes physiques est nécessaire au bon déroulement du processus, les coûts augmentent inévitablement. De la même façon, les systèmes basés sur l'utilisation de matériel (carte, lecteur, puces électroniques, etc.) engendrent des coûts plus élevés que les systèmes reposant sur l'utilisation de logiciels.

Toutefois, il est possible qu'une solution matérielle soit avantageuse dans la mesure où celle-ci est largement utilisée.

Dans tous les cas, le coût d'utilisation d'un mécanisme de paiement électronique doit être proportionnel à la valeur de la transaction. Ainsi, les commerçants misant sur des transactions de faibles valeurs ont souvent avantage à opter pour des systèmes dont les coûts sont calculés au pourcentage. D'un autre côté, les commerçants dont les transactions atteignent des sommes importantes recherchent plutôt les mécanismes de paiement établissant un coût fixe pour toutes les transactions.

Le temps passé par le consommateur à effectuer le paiement est un autre type de coût pour l'utilisateur d'un mécanisme de paiement électronique. L'exécution du paiement doit être rapide sinon ce dernier risque d'abandonner l'opération ou chercher un autre commerçant pour ses futurs achats. Comme la partie la plus longue du processus de paiement en ligne concerne la saisie des données par le consommateur, le commerçant devrait lui faciliter cette tâche. Pour y arriver, le commerçant doit être en mesure de conserver les données du consommateur, lui évitant ainsi d'avoir à remplir un nouveau formulaire pour chaque achat. L'utilisation de fichiers témoins peut également être envisagée afin de permettre au consommateur de personnaliser le processus de paiement en fonction de ses propres besoins, dans la mesure où les considérations ayant trait au respect de la vie privée sont prisent en compte.

Encadré 25 : L'échec de First Virtual

La compagnie First Virtual avait lancé le premier mécanisme de paiement sur Internet en 1994. L'utilisation de ce système nécessitait que le consommateur et le commerçant soit préalablement enregistrés auprès de First Virtual. Le consommateur, avant de pouvoir effectuer des achats, devait communiquer les informations relatives à sa carte de crédit par téléphone. Il recevait alors un numéro d'identification personnel (NIP).

Lorsque le consommateur désirait payer un commerçant, il lui divulguait simplement son NIP. Ce dernier le transmettait alors à First

Virtual, accompagné du montant à payer et de son propre NIP. La compagnie s'assurait alors de la validité de la transaction en demandant une confirmation au consommateur par courrier électronique. Une fois la confirmation obtenue, First Virtual utilisait le réseau bancaire traditionnel pour débiter le consommateur et payer le commerçant.

Ce système était l'un des plus simples puisqu'il n'utilisait aucun logiciel particulier. De plus, le recours aux technologies de cryptage n'était pas nécessaire dans la mesure où aucune information confidentielle ne transitait via Internet. Grâce à cette méthode de fonctionnement, First

Virtual était totalement sécuritaire. Enfin, ce système avait également l'avantage de permettre le règlement de petites sommes d'argent en assurant une avance financière de 10$ avant de facturer la carte du consommateur.

Néanmoins, le mécanisme de paiement de First Virtual avait aussi des inconvénients. Premièrement, la présence d'un intermédiaire entraînait des coûts importants pour les parties. Deuxièmement, l'interface entre Internet et le réseau bancaire fermé causait des délais. La confirmation de la transaction prenait beaucoup de temps avant de parvenir au commerçant. Troisièmement, First Virtual ne répondait pas au critère de l'universalité en exigeant l'ouverture d'un compte auprès d'une banque américaine. Quatrièmement, la confidentialité des transactions n'était pas respectée car la compagnie tenait un registre détaillé des opérations effectuées par le biais de son service. Ces inconvénients eurent finalement raison du système. First Virtual délaissa le milieu du paiement électronique en 1998.

Pour que les consommateurs acceptent d'utiliser un mécanisme de paiement électronique, celui-ci doit avant tout être simple. Actuellement, une majorité d'Internautes estiment que les méthodes proposées sont difficiles à utiliser. Le commerçant doit donc porter une attention particulière aux systèmes qui ne requièrent aucune expertise particulière de la part des consommateurs.

Les mécanismes de paiement les plus simples sont évidemment ceux qui ne nécessitent pas d'installation de logiciels clients. Malheureusement ceux-ci sont plutôt rares. Lorsque l'installation de logiciels est inévitable, le recours à des plugiciels (plug-in) est souhaitable puisqu'elle permet au consommateur de continuer à utiliser un logiciel dont il connaît déjà les fonctionnalités. De plus, une fois le processus d'installation complété, le logiciel de paiement électronique doit nécessiter le moins d'interventions possibles de la part de l'utilisateur. Le mécanisme de la transaction devrait être transparent pour lui dans la mesure où il en comprend les implications. Enfin, il est très important que l'entreprise qui met de l'avant le mécanisme de paiement offre un support technique efficace au consommateur.

Tout moyen de paiement doit être en mesure de garantir au créancier la valeur de ce qui lui est remis en guise de paiement. Les mécanismes de paiement électronique doivent donc être capables d'authentifier l'argent transmis afin d'obtenir la confiance des différents acteurs. Cette exigence est particulièrement pertinente pour les systèmes reposant sur l'utilisation de monnaies électroniques. Puisque celle-ci est composée de données informatiques, elle est théoriquement facile à reproduire. Comme la copie informatique est impossible à distinguer de l'originale, la contrefaçon serait

alors impossible à détecter. S'il en était ainsi, toute personne disposant d'une pièce de monnaie électronique pourrait devenir millionnaire en quelques minutes. Pour être viable, les mécanismes de paiement électronique doivent donc éliminer ce problème de la double utilisation (double-spending).

Pour les systèmes en ligne, la solution consiste à communiquer avec la banque émettrice à chaque fois qu'une transaction a lieu. Cette dernière, en maintenant une base de données des pièces utilisées, indique au commerçant si la monnaie qui lui est proposée a déjà été dépensée. Si la réponse est positive, la transaction est annulée, alors que si la réponse est négative, la transaction peut être complétée. Cette façon de faire ressemble en partie à la méthode actuellement utilisée pour vérifier les cartes de crédit.

Pour ce qui est des systèmes hors ligne, il existe principalement deux méthodes pour régler le problème de la double utilisation. La première consiste à doter les cartes d'une puce qui tient un compte exact des pièces de monnaie dépensées. Si le propriétaire de cette carte tente d'utiliser une pièce déjà dépensée, la puce n'autorise pas la transaction.

Ces puces sont conçues de façon à ce que la carte devienne inutilisable après toute tentative de modification des données qui s'y trouvent. La seconde méthode repose sur la cryptographie. En structurant le protocole cryptographique, il est possible de s'assurer que l'identité du double utilisateur soit révélée lorsqu'une pièce de monnaie retourne à la banque. En principe les utilisateurs ne devraient pas dépenser deux fois leurs pièces s'ils sont certains d'être pris en peu de temps. L'avantage de cette deuxième solution est qu'elle ne nécessite pas l'utilisation de puces spéciales et qu'elle peut donc reposer entièrement sur des logiciels.

Pour qu'un mécanisme de paiement gagne la confiance des acteurs du commerce électronique, il doit aussi assurer l'intégrité des communications ayant lieu lors de la transaction. Il s'agit du principal élément de sécurité en matière de commerce sur Internet.

Cela signifie premièrement que les tiers ne doivent pas être en mesure de modifier les messages transmis. Deuxièmement, il faut que l'intégrité du paiement soit aussi protégée contre la fraude de l'une ou l'autre des parties. De plus, dans le cas de la monnaie électronique, l'hypothèse de la collusion entre le consommateur et le commerçant dans le but de tromper la banque émettrice doit être envisagée. Lorsque ces exigences ne sont pas respectées, un grand nombre de transactions courent le risque d'être répudiées, ce qui affecterait la stabilité du commerce électronique en général.

Pratiquement, l'intégrité du paiement est assurée par le recours à la cryptographie. Les procédés utilisés pour une transaction d'une faible valeur sont les mêmes que ceux qui servent pour les transferts importants entre banque ou pour la défense nationale.

Cependant, comme aucun procédé cryptographique n'est totalement inviolable, le commerçant doit tout de même être vigilant en ce qui a trait à la sécurité de son système.

Finalement, le niveau de confidentialité offert par un mécanisme de paiement électronique est un autre élément dont le commerçant doit tenir compte. En effet, le paiement suppose la communication de nombreux renseignements de la part du consommateur. Ce sont justement ces renseignements, récoltés lors de l'utilisation d'un service, qui sont les plus prisés par les entreprises. Il s'agit, entre autres, de l'adresse physique du consommateur, de ses renseignements bancaires, du mode de paiement utilisé, du contexte du paiement (date, heure, provenance …), etc. Ces données ont une valeur économique élevée et permettent un contrôle social important. Il n'est donc pas étonnant que plusieurs entreprises les accumulent afin de dresser des portraits extrêmement détaillés des consommateurs. C'est, entre autres, le cas de certains mécanismes de paiement électronique.

Les commerçants doivent toutefois apprendre à se méfier de ces systèmes. Premièrement, il est fort possible que les pratiques de ceux-ci soient illégales dans plusieurs juridictions.

Comme beaucoup d'États se sont dotés de législations sur la protection des renseignements personnels au cours des dernières années, la collecte en est souvent limitée. Deuxièmement, les entreprises accumulant ces données tentent généralement de les vendre par la suite. Il peut être extrêmement nuisible pour un commerçant d'être associé à ce type de comportement. Sa réputation peut être définitivement entachée.

Troisièmement, les consommateurs n'accorderont pas leur confiance à un système qui permet de récolter des renseignements à outrance. Peu importe la méthode utilisée (base de donnée centrale ou carte à puce), s'il existe un doute quant au contenu des données accumulées lors du paiement, cela peut être suffisant pour freiner l'utilisation d'un système.

D'un autre côté, les mécanismes de paiement électronique totalement anonymes ne représentent pas une meilleure solution. En effet, plusieurs États envisagent de les interdirent à cause du risque qu'ils représentent pour le blanchiment d'argent, l'évasion fiscale et l'achat de produits et services illégaux. Il faut comprendre que le contexte des environnements

dématérialisés permet d'atteindre un niveau d'anonymat encore inégalé dans le monde physique. Si la monnaie classique ne laisse aucune trace, le commerçant traditionnel peut toujours identifier le consommateur visuellement. Le commerce électronique élimine ce dernier élément d'identification. À cela s'ajoute le fait que plusieurs législations exigent des institutions financières qu'elles suivent le déroulement de certaines transactions électroniques et en conservent des traces.

Le mécanisme de paiement idéal doit donc constituer une solution intermédiaire à ces deux extrêmes. Sans accorder l'anonymat complet, il doit assurer au consommateur que seuls les renseignements nécessaires au paiement seront emmagasinés et que ceux-ci seront utilisés à cette unique fin. De plus, le recours à des procédés cryptographiques est essentiel afin de s'assurer que ces renseignements ne peuvent pas être obtenus par des tiers. Évidemment, ces limitations visent autant le commerçant que les intermédiaires ayant un rôle à jouer dans le processus du paiement.

Les technologies disponibles

Compte tenu du grand nombre de moyens de paiement actuellement destinés au commerce électronique, il est impossible de dresser une liste exhaustive des technologies disponibles. Par contre, il est possible de classer la multitude des mécanismes disponibles en quelques catégories. Parmi celles-ci, les technologies basées sur l'utilisation d'une carte de crédit sont définitivement les plus populaires. Toutefois, il en existe plusieurs autres qui méritent d'obtenir l'attention des commerçants. Il s'agit des chèques électroniques, des monnaies électroniques, des micro-paiements ainsi que de l'intégration du prix dans le coût de communication.

Jusqu'à ce jour, la presque totalité des transactions effectuées sur Internet a été réglées par carte de crédit. Il est donc essentiel pour le commerçant d'offrir à sa clientèle la possibilité de payer de cette façon, même si cela implique l'utilisation de plusieurs mécanismes de paiement électronique à la fois. Pour y arriver, de nombreuses technologies de chiffrement sont disponibles. Certains systèmes reposent sur la communication du numéro de carte en ligne alors que d'autres prévoient une communication hors ligne. Ces derniers se font d'ailleurs de plus en plus rares et devraient être évités. L'expérience démontre que ces systèmes, trop complexes ou trop lents, découragent les consommateurs. Dans le même ordre d'idée, certains systèmes permettent aux parties de transiger directement ensemble alors que

d'autres sont fondés sur l'utilisation d'intermédiaires. Les premiers devraient évidemment être privilégiés car ils sont beaucoup moins coûteux.

Pour ces mêmes raisons, la méthode la plus simple est également la plus utilisée. En effet, beaucoup de commerçants se contentent de demander le numéro de carte du consommateur en protégeant la communication à l'aide du protocole SSL (Secure Sockets Layer). Cette façon de faire est idéale pour les transactions ponctuelles puisqu'il n'y a aucune formalité à effectuer avant le paiement. Malheureusement ce mécanisme de paiement électronique est imparfait puisqu'il ne permet pas au commerçant de s'assurer que la personne utilisant la carte en est la détentrice. Il est donc importance pour le commerçant d'y joindre un système de vérification d'adresse. Malgré tout, les petites et moyennes entreprises ont avantages à utiliser SSL qui leur offre un mécanisme de paiement efficace pour un investissement minimal.

Toutefois, SSL n'est pas le seul protocole de chiffrement disponible sur le marché. En fait, selon plusieurs, SET (Secure Electronic Transaction) (http://www.setco.org/) est le dispositif le plus complet et le plus sécuritaire. Celui-ci a été lancé en 1996 par Visa et

MasterCard et déposé dans le domaine public afin de permettre le développement de logiciels compatibles. Tout comme SSL, SET a recours à la cryptographie asymétrique pour répondre aux impératifs de confidentialité et d'intégrité du paiement. SET va toutefois beaucoup plus loin que SSL car il utilise des certificats et des signatures électroniques afin de garantir l'identité du consommateur et du commerçant. Grâce à ce fonctionnement, le commerçant reçoit une autorisation avant de procéder au paiement et il est assuré d'être payé, même en cas de fraude. Le consommateur, quant à lui, est assuré que le commerçant est effectivement enregistré auprès des organismes de carte de crédit.

D'un autre côté, SET est plus lent que SSL à cause des multiples opérations effectuées au moment de la transaction et plus coûteux parce que des logiciels serveurs et clients supplémentaires doivent être installés. Finalement, le client doit posséder un certificat, ce qui complique l'opération. Cependant, son adoption par CyberCash, IMB, Microsoft et

Netscape laissait entrevoir un avenir très prometteur pour le dispositif. Pourtant, SET tarde à se déployer. La principale cause de cet échec semble être le manque d'interopérabilité entre les différents logiciels offerts. Pour résoudre ce problème, les entreprises tentent maintenant de rapprocher SET et SSL afin d'offrir des logiciels permettant de transiger avec l'un ou l'autre des protocoles. C'est le cas, entre autres, de CyberCash et d'IBM. Lorsque

ces logiciels seront disponibles, ils seront sans aucun doute les plus performant sur le marché.

SET est également à l'origine du mécanisme de paiement électronique C-SET (Chip- Secure Electronic Transaction). C-SET permet d'ajouter au modèle de SET un élément physique reposant sur l'utilisation de carte à puce. Selon ce protocole, les procédures sécuritaires s'effectuent sur la carte, éliminant ainsi la nécessité d'envoyer des informations confidentielles sur le réseau. Toutefois, le consommateur doit se procurer un lecteur de carte, essentiel à l'accomplissement des fonctions hors réseau. Jusqu'à maintenant, l'avenir de C-SET reste incertain même s'il a été adopté en France par l'important groupement Carte Bancaire.

Pour sa part, CyberCash (http://www.cybercash.com/) propose un mécanisme de paiement qui, tout en étant conforme aux normes établies par SET, ajoute un intermédiaire à la transaction. Selon ce modèle, CyberCash sert d'interface avec le réseau bancaire après s'être assuré du consentement des parties. Pour y arriver, le consommateur doit d'abord installer un logiciel client. Le consommateur utilise ensuite ce logiciel pour inscrire les informations nécessaires au paiement et signer la commande. Celle-ci est ensuite envoyée au commerçant qui signe lui aussi la commande. Il la redirige ensuite vers CyberCash. À ce moment, l'entreprise valide la transaction avec la banque et retourne la confirmation aux parties. L'avantage principal de ce système est que le numéro de carte de crédit du consommateur reste inconnu du commerçant grâce à un procédé cryptographique. Ainsi, le niveau de sécurité et de confidentialité est très élevé.

Inversement, la nécessité d'acquérir un logiciel spécifique et l'ajout d'un intermédiaire constituent des inconvénients majeurs.

Finalement, de nombreux mécanismes de paiement électronique basés sur l'utilisation de cartes de crédit sont proposés par diverses entreprises dans le cadre de solutions globales de commerce électronique. Le plus souvent, ceux-ci sont fondés sur l'utilisation de SSL.

L'avantage de ces systèmes est qu'ils sont parfaitement intégrés à l'intérieur d'un ensemble logiciel et matériel destiné aux nouveaux cyber-commerçants. Par exemple, le serveur

OpenLinux de Caldera (http://www.calderasystems.com) permet la mise en place rapide d'une solution de commerce électronique sous Linux, y compris un mécanisme de paiement. Le recours à ce type de propositions clef en main peut parfois sauver beaucoup de temps et d'argent.

4. Chèques électroniques

Jusqu'à maintenant, les chèques électroniques ne remportent pas un vif succès auprès des acteurs du commerce électronique. Pourtant, ils constituent des mécanismes de paiement efficace, simple à utiliser et peu coûteux. Il est vrai que la responsabilité du consommateur en cas de fraude peut s'avérer beaucoup plus importante que pour d'autres modes de paiement, tels que les cartes de crédit. Pour l'instant, il existe donc très peu d'initiatives en la matière et seul deux systèmes se distinguent de la concurrence. Il s'agit des projets eCheck du FSTC (Financial Services Technology Consortium) et de NetChex.

Le chèque proposé par eCheck (http://www.echeck.org/) est tout bonnement l'équivalent électronique d'un chèque papier. Le consommateur dispose d'un livret de chèque qu'il peut visualiser et remplir. La seule différence à trait à la signature manuelle qui est remplacée par une signature électronique. On peut donc prétendre que ce mécanisme de paiement est plus sécuritaire que son homologue papier si l'on considère la signature électronique plus fiable que la signature traditionnelle. C'est peut-être ce qui explique l'appui donné à ce système par de nombreux intervenants du milieu financier et par le ministère du trésor américain qui l'utilise déjà pour de nombreux paiements. Par contre, ce mécanisme possède le désavantage de ne pas garantir au commerçant la disponibilité des fonds du consommateur immédiatement. Aussi, la technologie eCheck semble mieux adaptée au contexte des transactions régulières entre deux partenaires commerciaux.

De son côté, le chèque proposé par Netchex (http://www.netchex.com/) constitue plutôt une adaptation du modèle traditionnel au contexte des environnements dématérialisés.

Selon ce système, consommateur et commerçant doivent enregistrer leurs informations bancaires auprès de Netchex. Ainsi, lorsque le chèque est transmis à Netchex via Internet, il ne contient pas ces renseignements. Au moment de la réception, Netchex se charge de vérifier l'authenticité du document et de le compléter avec les informations de sa base de données. La transaction est ensuite transférée sur le réseau fermé du système bancaire, comme pour un chèque papier. Enfin, Netchex confirme le bon déroulement

du processus aux parties. Cette façon de procéder, bien que plus sécuritaire, possède les inconvénients de nécessiter un enregistrement antérieur et d'ajouter la participation d'un tiers à toutes les transactions.

La première distinction pouvant être effectuée afin de classifier les différentes monnaies électroniques concerne leur fonctionnement. Premièrement, certaines prennent la désignation "en ligne" car elles interagissent avec la banque émettrice au moment du paiement. Ces systèmes prennent la forme de porte-feuilles électroniques installés sur les disques durs des ordinateurs. Par exemple, un système de ce type est mis de l'avant par DigiCash (http://www.digicash.com/). Deuxièmement, certaines monnaies électroniques, appelées "hors ligne", permettent aux parties d'échanger des pièces sans que l'intervention de la banque émettrice ne soit nécessaire. Le mécanisme de paiement électronique

InternetCash (http://www.internetcash.com/) fonctionne de cette façon. Le plus souvent, ce type de monnaies électroniques est emmagasiné sur une carte à puce. Celle-ci est parfois jetable, parfois rechargeable. L'inconvénient du mécanisme est qu'un lecteur de carte est souvent nécessaire pour procéder au paiement. Toutefois, cela permet d'étendre l'utilisation de ces monnaies aux commerces physiques. Ceci explique pourquoi la plupart des entreprises optent pour les monnaies électroniques hors ligne, au détriment des systèmes en ligne.

La seconde distinction a trait au niveau de confidentialité offert par la monnaie électronique. Les monnaies identifiées (basic digital coin) permettent de recueillir de l'information concernant l'identité des personnes qui acquiert les pièces. La banque émettrice est alors capable de suivre le parcours de ses pièces, ce qui contrevient aux impératifs de confidentialité. Inversement, les monnaies anonymes (blinded coin) fonctionnent comme la monnaie en papier et ne laissent aucune trace des transactions ayant eu lieu. Pour arriver à ce résultat, la technologie de la signature aveugle est utilisée.

Cela signifie que la banque émettrice, lorsqu'elle signe la pièce de monnaie pour autoriser sa circulation, ne connaît pas son numéro unique. Elle ne connaît que le nom de l'acheteur et la valeur de la pièce. Cette approche devrait donc être privilégiée à la première puisqu'elle assure un excellent niveau de confidentialité.

Compte tenu de ces deux critères, le mécanisme de paiement électronique proposés par Mondex (http://www.mondex.com/) semble être destiné à un avenir prometteur. Il est vrai que Mondex est toujours en développement après de nombreuses années d'expérimentation, mais les importantes

institutions financières qui appuient ce projet ne semblent pas lâcher prise. Ce système de cartes à puce dont les unités peuvent être basées sur cinq devises différentes prétend offrir l'équivalent électronique de la monnaie papier.

Les valeurs chargées sur la carte peuvent ainsi passer de main en main jusqu'au moment où elles retournent à la banque émettrice qui les reconvertit alors en fonction de la devise demandée. La sécurité des transactions est assurée, entre autre, par l'utilisation de signature électronique et le recours à des puces dont la modification entraîne la perte des données y figurant. En ce qui concerne la confidentialité, l'entreprise affirme qu'au moment de la commercialisation de son système, celui-ci sera complètement anonyme.

Toutefois, les cartes Mondex permettent actuellement de recueillir de nombreuses informations relatives aux transactions, ce que l'entreprise considère essentiel pendant sa période d'essais. Évidemment, le principal inconvénient de ce système concerne le lecteur de carte que le consommateur doit se procurer.

5. Coût de communication

Une autre possibilité technique s'offrant au commerçant en matière de paiement électronique est d'intégrer le montant dû par le consommateur à la facture que ce dernier reçoit du prestataire de services qui lui fournit l'accès au réseau. Ce type de prestation est actuellement offert par le service Wanadoo de France Télécom (http://www.wanadoo.fr/).

Ceci permet au consommateur de payer de façon traditionnelle des produits et des services qui n'auraient pas pu l'être autrement. Pour y arriver, le commerçant doit nécessairement avoir conclu une entente avec le prestataire de services en question. Le désavantage majeur de ce procédé est que son utilisation est limitée à la clientèle du fournisseur d'accès. Il peut tout de même être avantageux pour le commerçant d'offrir cette possibilité de paiement parmi d'autres, particulièrement si les consommateurs qu'il désire rejoindre font affaire avec ce prestataire de services en grands nombres.

Conclusion

Somme toute, les possibilités qui s'offrent au commerçant en matière de paiement électronique sont énormes. En fait, l'existence de ce vaste éventail de mécanismes est rendue possible grâce à la nature essentiellement consensuelle du paiement. Ceci permet aux parties d'adopter la technologie de leur choix, qu'il s'agisse d'un système basé sur les cartes de crédit, d'un

chèque ou de monnaies électroniques. Néanmoins, certaines règles juridiques minimales doivent être respectées par ces nouveaux moyens de paiement.

Aussi, avant de choisir celui ou ceux qu'il désire adopter, le commerçant devra tenir compte des considérations relatives au moment et au lieu du paiement, à l'obligation de fournir une quittance ainsi qu'aux règles pertinentes de la preuve.

Le commerçant électronique doit aussi tenir compte de sa clientèle. Les mécanismes ayant recours aux cartes de crédit peuvent difficilement être ignorés puisque ces cartes sont actuellement utilisées par une majorité d'internautes. Toutefois, selon les circonstances, d'autres technologies peuvent être mieux adaptées aux besoins du commerçant. C'est, entre autres, le cas des mécanismes de micro-paiement lorsque la valeur des transactions effectuées est infime. Le commerçant doit alors s'assurer qu'aucune transaction ne sera perdue à cause de l'impossibilité de procéder au paiement.

D'ailleurs, rien n'empêche ce dernier d'offrir plusieurs méthodes de paiement au consommateur.

Dans tous les cas, le commerçant se doit d'être prudent lors de son choix. Les entreprises proposant des mécanismes de paiement électronique étaient jusqu'à maintenant nombreuses et variées. Cependant, depuis quelques temps, leur nombre tend à diminuer.

Plusieurs d'entre elles ferment aujourd'hui leur porte suite à l'échec de leurs systèmes.

Aussi, d'ici à ce qu'un système efficace et sécuritaire s'affirme comme solution universelle du paiement en ligne, les commerçants ont avantage à recourir d'abord et avant tout aux mécanismes ayant déjà fait leurs preuves.

Bibliographie :

1. BRUN, Bernard, "Les mécanismes de paiement sur Internet", Juriscom.net, 20 octobre 1999, Source: http://www.juriscom.net/universite/doctrine/ article5.htm.

2. FROOMKIN, Micheal, "Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases", 1996, 15 U. Pittsburgh Journal of Law and Commerce 395, http://www.law.miami.edu/~froomkin/articles/oceanno.htm

3. GOSHTIGIAN, Patrick G., E-Cash, 1996, Source: http://www.anderson.ucla. edu/faculty/jason.frand/teacher/technologies/goshtigian/index.htm

4. INTERNET.COM, Payment Solutions Reviews, Source: http://ecommerce.internet.com/reviews/glance/0,,3691_5,00.html

5. ISHMAN, Mark, MAQUET, Quincy, "A Consumer's Analysis Of The Electronic Currency System And The Legal Ramifications For A Transaction Gone Awry", Murdoch University Electronic Journal of Law, Volume 6, number 3 (September, 1999), Source: http://www.murdoch.edu.au/elaw/issues/v6n3/ishman63nf.html

6. MILLER, Jim, E-money mini-FAQ, Source: http://www.ex.ac.uk/~RDavies/arian/emoneyfaq.html

7. PLAMONDON, Alain, Le paiement électronique sur Internet : recensement et analyse, 1997, Source : http://rambit.qc.ca/plamondon/ecashind.htm

8. THOUMYRE, Lionel, "Mise en scène des nouveaux moyens de paiement sur Internet", Multimédium, 10 novembre 1998, Source: http://www.mmedium.com/ dossiers/juriscom/paiement.html

9. VAN HOVE, Leo, "Electronic Purses: (Which) Way to go?", First Monday, volume 5, number 7 (July, 2000) , Source:http://www.firstmonday.dk/issues/issue5_7/hove/index.html