Le cadre juridique en droit civil québécois des transactions sur l'inforoute

David G. Masse*

L'avènement d'Internet a suscité un intérêt marqué au sein de la communauté commerciale. En effet, plusieurs y voient une manière idéale d'augmenter l'efficacité des transactions commerciales. Avant que le commerce électronique ne devienne une réalité de tous les jours, il convient toutefois de s'assurer que le risque posé par ce nouveau type de commerce soit suffisamment bas.

Le commerce électronique existait déjà avant l'essor d'Internet. Certaines entreprises pratiquaient l'échange de documents informatisés (ÉDI) en réseau fermé depuis le début des années soixante-dix. Cette solution n'est toutefois accessible qu'aux entreprises importantes, qui ont les moyens d'implanter l'ÉDI en réseau fermé. De plus, les transactions entre entreprises seront habituellement gérées par un contrat-maître, qui permet d'éviter les imprévus juridiques. Lorsqu'il s'agit de transactions en réseau ouvert, comme sur Internet, il est souvent irréaliste de penser encadrer chaque relation par un contrat-maître ; il faut alors se tourner vers la législation existante. Or la législation en place au Québec ne favorise pas à l'heure actuelle le développement du commerce électronique.

Le cadre juridique actuel ne pose pas de problème majeur quant aux éléments essentiels du contrat ; il en va toutefois autrement quant à la preuve du contrat formé sur Internet. En effet, il importe de savoir si un document informatisé constitue un «écrit» au sens de l'article 2863 C.c.Q. De cette question découle le régime de preuve applicable aux documents informatisés. La doctrine est partagée à ce sujet, certains auteurs affirmant que le document informatisé n'est pas un «écrit». Selon cette analyse, les articles 2837-2839 C.c.Q. forment une suite étanche, et le régime traditionnel de preuve des écrits ne s'applique pas aux actes juridiques inscrits sur support informatique. Cette conclusion, bien qu'elle soit la plus susceptible d'être retenue, constitue une entrave importante au développement du commerce électronique au Québec.

L'auteur propose plutôt de considérer l'acte juridique inscrit sur support informatique comme un écrit à part entière, en conformité avec les recommandations de la Commission des Nations Unies pour le Droit Commercial International (C.N.U.D.C.I.) Cela permettrait de créer un régime neutre, qui accorde aux documents informatisés un statut équivalent à celui des documents sur support papier. Pour ce faire, il serait toutefois nécessaire de remédier à la rédaction des articles 2837-2839 C.c.Q., afin de séparer les questions d'admissibilité des questions de valeur probante.

The advent of the Internet has attracted great interest from the commercial community. Many see the Internet as an ideal opportunity to increase the efficiency of business transactions. Before electronic business becomes a daily reality, however, it makes sense to ensure that the inherent risks of this new type of trade are sufficiently low.

Electronic trade existed before the expansion of the Internet. Some businesses have been using electronic data interchange (EDI) on closed networks since the early 1970s. This solution, however, is only available to large businesses, which have the means to set up EDI on a closed network. Moreover, transactions between businesses are usually governed by a framework contract, thereby avoiding legal surprises. In the case of open-network transactions, such as those on the Internet, it would be unrealistic to think that a framework contract could govern each transaction; we must therefore turn to existing legislation. But the legislation in Quebec does not currently further the development of electronic trade.

The current legal framework does not pose any major problems for the essential elements of a contract made on the Internet; that is not the case, however, for questions of evidence. More specifically, it is important to determine if a computerized document is a "writing" in the sense intended by 2863 C.c.Q. This in turn determines which regime of evidence applies to computerized documents. Doctrine is divided on this question, some authors concluding that a computerized document is not a "writing". According to this view, articles 2837-2839 C.c.Q. form a watertight compartment and the traditional regime of written evidence does not apply to juridieal acts made and recorded on computer. This position, although the one most likely to be adopted, represents a significant barrier to the development of electronic trade in Quebec.

The author suggests treating the juridical act made and recorded on computer as a full-fledged "writing", conforming with the recommendations of the United Nations Commission on International Trade Law (U.N.C.I.T.R.A.L.). This would permit the creation of a neutral regime, in which computerized documents are on an equal footing with paper documents. To achieve this goal, it would be necessary to redraft articles 2837-2839 C.c.Q. in order to distinguish questions of admissibility from questions of probative value.

* Secrétaire adjoint de la Société, BCE Inc. et Bell Canada. La présente étude a été rédigée alors que l'auteur était avocat et associé chez Chait Amyot à Montréal.

McGill Law Journal 1997
Mode de référence : (1997) 42 R.D. McGill 403
To be cited as: (1997) 42 McGill L.J. 403

Introduction

Bienvenue à la nouvelle frontière du «cyberespace»[1], où nous sommes tous des pionniers en puissance. Mot innovateur, cyberespace convient à merveille pour décrire un endroit inexistant, mais qui est vraisemblablement plus peuplé d'aventuriers, d'explorateurs, d'éclaireurs et de pionniers que ne l'était le Nouveau Monde à l'ère de Paul Chomedey de Maisonneuve, fondateur de Montréal, il y a plus de 350 ans. Cette nouvelle technologie présente des défis qui changeront notre manière de penser et de faire les choses, en plus de nous amener vers un monde où les messages complexes, les actes juridiques et les devises voyagent à la vitesse de la lumière.

Nous devons nous conformer à cette nouvelle réalité et adapter nos institutions juridiques pour nous permettre d'être à la hauteur de la concurrence mondiale à laquelle nous devrons faire face. Conscient des défis à l'horizon, le gouvernement fédéral a mis sur pied le Comité consultatif sur l'autoroute de l'information, en lui donnant le mandat de conseiller le gouvernement quant aux mesures qui devraient être prises pour que la société canadienne s'adapte à la nouvelle réalité. En effet, selon le rapport du Comité :

> [l]'autoroute de l'information porte les germes d'une transformation sociale. Les Canadiens doivent se demander s'ils accepteront passivement le changement ou s'ils en deviendront plutôt les agents. Pour le Comité, le choix est évident : la technologie de l'information doit permettre aux Canadiens, à titre individuel et collectif, d'utiliser la technologie à leur avantage personnel et social. L'avenir leur appartient[2].

L'ajustement requis n'est nulle part plus important et lourd de conséquences que dans l'arène du commerce. Le Comité recommande en termes très clairs aux Canadiens de réagir sans tarder :

> [a]u secteur privé, le Comité adresse le vu [sic] qu'il se mette en marche sans plus tarder. La course mondiale est engagée pour mettre au point l'autoroute de l'information. Les entreprises canadiennes ne peuvent présumer de rien. La concurrence a une incidence sur presque tous les aspects de la politique gouvernementale. Dans le contexte de l'économie mondiale, les gouvernements ne peuvent agir comme ils l'ont déjà fait pour protéger les entreprises ou les secteurs économiques contre la concurrence étrangère, et ne le feront pas. Tout comme le public canadien, le gouvernement s'attendra à ce que le secteur privé tire le plus d'avantages possible d'un contexte économique libéralisé. Les investissements des secteurs public et privé dans l'apprentissage et la formation auront une incidence cruciale sur la réussite de la main-d'oeuvre canadienne dans un contexte concurrentiel. Les entreprises qui investissent dans la technologie et les ressources humaines connaîtront la prospérité. Celles qui ne le font pas échoueront.

---

[1] Traduction du mot anglais *cyberspace* inventé par William Gibson, auteur américain. Voir W. Gibson, *Neuromancer*, New York, Ace Books, 1984.

[2] Comité consultatif sur l'autoroute de l'information, *Le défi de l'autoroute de l'information* (Rapport final) (septembre 1995) http://xinfo.ic.gc.ca/info-highway/final.report/fra/ch7.html (16 juin 1997) [ci-après *Le défi*].

> Le Comité invite aussi *tous les Canadiens*, individuellement, à faire usage de la technologie de l'information. Ils doivent prendre en charge leur propre éducation et ne pas considérer l'autoroute de l'information comme une menace, mais plutôt comme une chance d'accéder à une meilleure qualité de vie et d'acquérir une plus grande autonomie[3].

Sur le plan juridique québécois, nous avons un nouveau *Code civil*, fruit d'un long travail de réflexion et destiné à servir de toile de fond pour l'épanouissement du Québec dans un nouveau millénaire. Bien avant l'adoption de ce Code, le voeu a été exprimé au législateur qu'il prenne soin d'adapter le Code aux nouveaux défis présentés par la technologie de l'information :

> Que le législateur soit vigilant en s'assurant de ne pas bloquer le droit et le rendre imperméable aux développements technologiques : sa définition de la signature ainsi que celle de l'écrit doit être assez libérale pour donner ouverture à de nouvelles techniques de matérialisation de l'entente[4].

La question qui se pose donc est la suivante : est-ce que notre nouveau *Code Civil* est à la hauteur du défi d'un monde virtuel dématérialisé et ce, notamment dans le domaine commercial ? Afin de fournir une réponse à cette question, la présente étude analyse l'infrastructure en place au sein du *Code civil du Québec*, en vue de déterminer si elle répond de manière adéquate aux défis de la société de demain.

I. Le commerce

Pour bien saisir les incidences du monde électronique et de l'inforoute sur le commerce, il importe de comprendre ce qu'est le commerce. Les méthodes de communication, le droit des affaires et les règles juridiques qui gouvernent l'environnement dans lequel le commerce évolue ne constituent que quelques-unes des variables de l'environnement commercial contribuant au succès d'une entreprise.

Le bénéfice économique

L'essence même du commerce est la recherche du bénéfice ; celui-ci s'obtient par l'échange de biens et de services entre personnes. L'environnement qui permet ces échanges n'est jamais exempt de risques : qu'il s'agisse de l'environnement hostile de l'âge de pierre, des brigands de la route du Moyen Âge ou des pirates de la haute mer à l'époque de la Renaissance, le risque a toujours fait partie intégrante de l'entreprise commerciale.

Les aléas du commerce et la gestion du risque

Les principaux outils disponibles pour la gestion du risque commercial sont les limites qui peuvent être imposées à la responsabilité personnelle des participants, la

---

[3] *Ibid.* [italiques de l'original].

[4] P. Patenaude, «Commentaires sur l'avant-projet de réforme au Code civil chapitre de la preuve : de l'importance de ne pas imposer législativement une fin de non-recevoir aux moyens techniques modernes de matérialisation de l'accord des volontés» (1988) 19 R.D.U.S. 31 à la p. 35.

mesure dans laquelle des tiers peuvent être appelés à indemniser les parties en cas de perte et l'encadrement juridique de l'entreprise par l'entremise de contrats, de coutumes ou d'usages commerciaux appropriés.

L'environnement du commerce électronique

L'expérience du libre-échange nord-américain nous enseigne que le commerce s'épanouit dans un environnement de libre-échange de biens, de services et de renseignements[5]. C'est dans un tel élan qu'une nouvelle forme de technologie tente aujourd'hui de percer. En effet, nous sommes à l'aube d'une révolution dans l'échange de renseignements commerciaux : le commerce électronique.

Le commerce électronique en réseau ÉDI fermé

L'ÉDI peut être défini comme suit : «[...] l'échange de documents informatisés, [qui] remplace la transmission de formules commerciales courantes (bons de commande, factures, formules d'expédition, etc.) par un système informatisé de communication et de consignation de données»[6].

L'échange de documents informatisés a connu ses débuts vers les années soixante, alors que l'informatisation des grandes entreprises était déjà assez avancée. Les premiers échanges se faisaient à l'intérieur d'une seule et même entreprise entre ses divers établissements situés un peu partout dans le monde. Les avantages importants que sont la rapidité, la qualité, l'économie et l'efficacité de la transmission de données informatisées ont bientôt poussé ces grandes entreprises à vouloir utiliser l'ÉDI avec leurs partenaires commerciaux et leurs fournisseurs.

Jusqu'à présent, l'ÉDI s'est pratiqué en réseau informatique fermé, c'est-à-dire que les intervenants échangent leurs documents informatisés sur des réseaux privés. Plusieurs raisons justifient cette approche : contrairement aux réseaux ouverts, les réseaux fermés présentent un médium d'échange normalisé où la sécurité, l'identification des intervenants et l'intégrité des communications sont assurées, puisqu'il existe entre les parties une relation commerciale antérieure, accompagnée souvent d'un contrat écrit régissant les modalités des échanges électroniques. Cette normalisation et ce contrôle sont nécessaires afin de permettre des échanges commerciaux, comme nous le verrons lorsque nous discuterons des enjeux dans un environnement de réseaux ouverts. L'implantation d'une solution ÉDI en réseau fermé est cependant très coûteuse, ce qui en limite dans une certaine mesure l'efficacité.

Le commerce électronique offre des avantages considérables. À l'heure actuelle, les seuls à pouvoir bénéficier de ces avantages sont les entreprises commerciales importantes, dont l'ampleur justifie le coût élevé de l'implantation de l'ÉDI en réseau fermé. Ces entreprises, quoique puissantes sur le plan économique, sont relativement peu nombreuses. En 1993, leur nombre était estimé à seulement 30,000 en Amérique

---

[5] Voir A. Coyne, «The 21st Century Belongs to Canada» *Saturday Night* (octobre 1995) 72.

[6] G. Jenkins et R. Lancashire, *Échange de documents informatisés : l'ÉDI à la portée de tous*, éd. rév., Etobicoke (Ontario), MacTop, 1993 à la p. 5.

du Nord[7]. Le nombre limité d'entreprises ayant recours à l'ÉDI restreint naturellement l'efficacité des marchés. En effet, dans la mesure où le nombre d'intervenants est limité, la concurrence se trouve par le fait même réduite. Il s'ensuit que le marché comme mode efficace de répartition de biens et de services est amoindri et par le fait même, les prix des biens et des services ne sont pas aussi concurrentiels qu'ils pourraient l'être.

Les normes ÉDI

Cette volonté grandissante d'échanger des données commerciales informatisées a mené à l'établissement de réseaux informatiques et de normes de transmission de données. Ces normes et réseaux régionaux ont donné naissance, dans le cours normal de leur évolution, à des réseaux et à des normes plus généralisés, devenus sectoriels, puis multi-sectoriels et finalement mondiaux. Malgré le développement des normes internationales qui encadrent aujourd'hui l'ÉDI, il n'en demeure pas moins que l'échange de documents informatisés ne se fait encore qu'entre partenaires commerciaux ayant une relation précédant l'avènement de l'ÉDI dans le domaine commercial. De plus, ces commerçants sont en général reliés par un réseau informatique fermé.

Le commerce électronique en réseau ouvert

Contrairement aux réseaux fermés ÉDI existants, l'Internet est un réseau ouvert, c'est-à-dire un réseau de réseaux recouvrant le globe. Il s'agit d'un réseau ouvert en ce sens qu'il n'est soumis à aucun contrôle qui en limite l'accès. La structure d'Internet se rapproche de celle d'une toile d'araignée où chaque filament correspond à un réseau distinct. Les communications sur Internet circulent au moyen d'un protocole de transmission : le protocole TCP/IP[8].

Sur Internet, les messages voyagent de réseau en réseau de façon largement aléatoire. Il est impossible de tracer à l'avance le chemin que suivra le message. En fait, il est possible qu'un seul et même message emprunte plusieurs chemins pour se rendre à destination. Une moitié du message prendra un chemin, tandis que l'autre moitié en empruntera un autre. C'est cette caractéristique d'Internet qui constitue sa force. À l'origine, il s'agissait d'un réseau militaire, conçu pour résister aux attaques nucléaires pouvant à tout moment anéantir une grande partie du réseau[9]. Tout comme la toile d'araignée, Internet résiste aux attaques ; si une partie de la toile est détruite, l'araignée empruntera le reste de la toile pour circuler.

---

[7] *Ibid.* à la p. 78.

[8] Le protocole TCP/IP (*Transport Control Protocol/Internet Protocol*) subdivise les messages en segments numériques et dote chaque segment de renseignements lui permettant de naviguer seul de réseau en réseau, séparé de ses segments soeurs et frères, pour enfin se réunir avec eux à destination et reformer le message original.

[9] D. Johnston et S. Handa, *Getting Canada OnLine : Understanding the Information Highway*, Toronto, Stoddart, 1995 aux pp. 17-19.

Pendant qu'ils se déplacent de réseau en réseau, les messages peuvent être lus par quiconque a accès aux réseaux empruntés. Cette parfaite insécurité et cette transparence d'Internet n'affectent cependant pas sa mission principale, qui jusqu'à récemment consistait à servir de messagerie pour les centres universitaires. C'est tout autre chose que d'y faire circuler des renseignements commerciaux confidentiels ou encore des données destinées à permettre la circulation de devises, telles que des numéros de cartes de crédit ou de débit. Pourtant, c'est exactement ce que de nombreux intervenants désirent accomplir afin d'ouvrir tout grand les portails du commerce électronique mondial.

Afin d'augmenter son efficacité et de répartir les bénéfices qui en découlent, il est nécessaire d'augmenter l'accessibilité au commerce électronique. Pour y parvenir, il est essentiel de créer un environnement de commerce électronique permettant aux commerçants d'y accéder en grand nombre et en toute quiétude. Le *sine qua non* pour réaliser cet objectif est de permettre un commerce aisé sur un modèle de réseau ouvert, fondé sur le respect de normes généralement connues et appliquées. Comment peut-on concrètement rendre Internet propice à ce rôle ?

Afin d'être propice au commerce, une forme de communication doit fournir un moyen, jugé acceptable par la communauté commerciale, d'assurer une certitude de résultat suffisante pour justifier le risque d'y transiger. Au minimum, le commerçant doit savoir avec qui il fait affaires, s'il existe un engagement juridique entre les parties eu égard à l'objet de la transaction et si la contrepartie qu'il compte toucher sera versée (normalement un paiement en devises ayant cours légal dans le pays du commerçant). Il s'agit là des éléments classiques du contrat.

Le risque de perte est présent dans toute entreprise commerciale. Or, le risque est, de par son essence même, un élément relatif. L'appréciation du seuil de risque «acceptable» pour justifier l'épanouissement du commerce varie donc selon les circonstances. Quoi qu'il en soit, le commerçant attend rarement que la certitude du résultat soit parfaite avant de s'aventurer dans un nouveau milieu commercial. En effet,

> [t]he advantages of electronic commerce are perceived as so great that companies have implemented electronic communications technologies despite the difficulty of determining the legal efficacy and effect of electronic transactions. In the United States prior to the enactment of Article 4A of the Uniform Commercial Code, over one trillion dollars a day was sent electronically[10].

Tous semblent d'avis que, pour le moment, l'insécurité d'Internet ne le rend pas propre au développement efficace de l'ÉDI. Un bon nombre de questions juridiques restent en suspens, malgré le fait que les transactions ÉDI se poursuivent depuis environ dix ans, à plus ou moins grande envergure, en réseau fermé. En effet, de nombreuses questions persistent quant au fondement juridique des transactions électroniques :

> [l]'ÉDI connaît un tel essor dans les secteurs des affaires et de l'administration publique que le système juridique a peine à suivre. Plusieurs questions se po-

[10] A.H. Boss, «The Emerging Law of International Electronic Commerce» (1992) 6 Temple Int'l & Comp. L. J. 293 à la p. 302.

> sent auxquelles il faudra bien répondre, tôt ou tard. Quel est le caractère juridique des communications effectuées par le biais de l'ÉDI ? Ont-elles une valeur contractuelle ? Les tribunaux voudront-ils reconnaître les documents commerciaux informatisés (factures, bons de commande) ?
>
> Certains types d'accords commerciaux ne sont exécutoires que s'ils sont attestés par un écrit signé par les parties. Les tribunaux accepteront-ils en tant «qu'écrits signés», les documents et authentifications transmis par des moyens électroniques ? Si les termes d'un accord ainsi conclu devaient donner lieu à un litige entre les parties, les documents informatisés seront-ils admissibles comme preuve ? Comment les parties peuvent-elles incorporer, dans leurs accords, les mêmes protections que celles qui sont assurées par les clauses actuellement inscrites sur les formulaires traditionnels (en petits caractères au verso)[11] ?

Ces questions subsistent principalement parce que les lois présentement en vigueur dans le monde n'ont pas été conçues pour s'appliquer au contexte de l'informatique avec son «écriture» numérique. D'autre part, le fait que l'ÉDI ne s'est développé jusqu'à présent qu'en réseaux fermés est peut-être la raison fondamentale ayant retardé l'adaptation du droit aux transactions électroniques.

Afin de développer le commerce électronique en réseau ouvert, comme ce serait le cas sur Internet, il est primordial de combler les lacunes subsistantes et donc de répondre aux questions juridiques soulevées par les transactions électroniques.

II. La gestion du risque dans les transactions commerciales électroniques

Le risque dans les transactions commerciales se gère principalement entre cocontractants et le contrat est l'instrument juridique par excellence pour la gestion du risque. En fait, c'est la force exécutoire du contrat que les parties recherchent. Le conseiller juridique est donc appelé à jouer un rôle important dans l'implantation de l'ÉDI, que se soit en réseau fermé ou en réseau ouvert[12].

Le contrat est défini à l'article 1378 C.c.Q. comme «un accord de volonté, par lequel une ou plusieurs personnes s'obligent envers une ou plusieurs autres à exécuter une prestation.» L'article 1385 C.c.Q. présente les éléments essentiels à la formation du contrat :

- la présence de personnes capables de contracter ;
- l'échange de consentement ;
- une cause ; et
- un objet.

Les questions problématiques dans le cadre de contrats négociés dans un environnement électronique concernent (1) l'identification des personnes capables de

---

[11] Jenkins et Lancashire, *supra* note 6 à la p. 71.

[12] *Ibid.* à la p. 28.

contracter, (2) l'échange de consentement et, une fois le contrat conclu, (3) la façon d'en faire la preuve. Quoique le commerce électronique soulève une multitude de questions intéressantes dans bien des domaines juridiques (songeons notamment aux modes de paiement[13], aux méthodes d'exécution forcée, aux problèmes de conflits de lois, au droit de contrôler les renseignements générés par le commerce électronique et passant entre les mains de tiers[14], à l'applicabilité des règles sur le transport aux réseaux intermédiaires[15], etc.), nous restreindrons notre analyse aux principes de base du commerce électronique, c'est-à-dire à la seule question de la formation des contrats. Afin de mieux cerner la problématique, nous aborderons séparément chacun des éléments essentiels à la formation du contrat, entre autres dans le contexte des transactions commerciales en réseau ouvert. Cet enjeu est important, puisque tout contrat non conforme à ces conditions peut être frappé de nullité[16].

A. L'échange de consentement

Les questions reliées à l'échange de consentement sont les mêmes, que la transaction électronique soit envisagée dans le cadre actuel de l'ÉDI en réseau fermé ou dans le contexte éventuel du commerce électronique sur un réseau ouvert comme Internet. Il convient donc de déterminer dans quelle mesure les solutions déjà fournies par l'ÉDI en réseau fermé peuvent être transposées à un système en réseau ouvert.

Dans le cadre des transactions ÉDI, les commerçants sont liés par une relation commerciale préexistante. En effet, ils se connaissent et peuvent encadrer leurs échanges dématérialisés par le biais d'un contrat-maître. C'est ce contrat qui fait dès lors la loi entre les parties et qui régit leurs futures transactions électroniques. Au fil de l'évolution de l'ÉDI, plusieurs organisations ont eu l'occasion de développer des contrats-types pour encadrer l'échange de documents informatisés[17]. Contentons-nous d'examiner un seul de ces contrats, soit le contrat-type commenté publié par le gouvernement du Québec[18]. Or, avant de nous attarder à celui-ci, il convient de saisir les enjeux sous-jacents.

L'article 1386 C.c.Q. prévoit que «[l]'échange de consentement se réalise par la manifestation, expresse ou tacite, de la volonté d'une personne d'accepter l'offre de contracter que lui fait une autre personne.» La loi n'impose pas de formalisme quant à la conclusion de contrats commerciaux tel que le contrat de vente de marchandises. Rien n'empêche donc la négociation de contrats par l'entremise de communications

---

[13] Voir art. 1564 C.c.Q. qui est rédigé en termes suffisamment larges pour permettre le virement électronique de fonds, le paiement par transmission de numéros de cartes de crédit, etc.

[14] Voir Boss, *supra* note 10 à la p. 299 ; Johnston et Handa, *supra* note 9 à la p. 190 et s.

[15] Voir art. 2030 C.c.Q. et s. ; Boss, *ibid.* à la p. 297 ; voir aussi *Thomas* c. *United States*, 117 S. Ct. 74 (1996).

[16] Voir art. 1416 C.c.Q.

[17] Voir A.H. Boss et J.B. Ritter, *Electronic Data Interchange Agreements : A Guide and Sourcebook*, Paris, I.C.C., 1993.

[18] K. Benyekhlef, *Échange de documents informatisés : contrat-type commenté*, Québec, Publications du Québec,1991.

informatiques, pourvu, bien sûr, que les parties prennent connaissance de l'échange de consentement.

Les communications informatiques sont complexes sur le plan matériel. Pourtant, ceux qui communiquent par courrier électronique savent que ce n'est pas tellement différent d'une correspondance postale. On doit tout de même apprécier la façon dont s'effectue une telle correspondance afin d'être en mesure, à titre de juristes, d'encadrer convenablement les échanges sur le plan juridique, de façon à faciliter l'usage des communications informatiques pour la négociation fiable des contrats.

Les ordinateurs communiquent entre eux par le biais de renseignements encodés en langage numérique binaire. Il s'agit d'un langage écrit constitué de deux caractères seulement : «0» et «1». Quoique très simple en fait de langage, l'alternance de «0» et de «1» suffit pour former l'alphabet[19] et les chiffres[20]. Il est évident qu'il s'agit d'un langage écrit très primitif et inefficace. Cependant, lorsque ces unités binaires sont utilisées des millions et même des milliards de fois pour établir des configurations complexes dans la mémoire matricielle d'un ordinateur, elles peuvent constituer des textes, des images, des sons et même des sons et images juxtaposés dans des bandes animées comparables aux vidéos que nous connaissons tous.

Afin de permettre à l'être humain de lire une correspondance numérique informatisée, l'initiateur et le destinataire doivent obligatoirement utiliser des logiciels compatibles. La question primordiale devient donc le choix des moyens technologiques. Ainsi, on doit déterminer les normes de traduction du langage binaire qui s'appliqueront aux échanges de documents informatisés.

On constate que les contrats-types ÉDI conçus pour les transactions commerciales sur réseaux fermés consacrent une grande partie de leurs dispositions à la normalisation des échanges informatiques[21]. En effet, le choix des normes de communication est une question fondamentale puisqu'il rend les communications informatiques intelligibles et donc la formation de contrats possible. Il en résulte, au chapitre élémentaire de l'échange de consentement, qu'aucune modification ou adaptation des lois existantes n'est vraiment nécessaire pour permettre la conclusion de contrats ÉDI en réseau fermé. Un contrat-maître, déterminant les normes de communication applicables, permet l'échange valide des consentements, lequel est primordial à la formation de contrats.

Nous pouvons maintenant apprécier, dans le contexte approprié, les dispositions du contrat-type québécois pour l'échange des documents informatisés[22]. Le contrat-type est constitué de neuf articles. Les dispositions de l'article 1 sont consacrées aux inévitables définitions de mots-clés, tels que «chiffrement», «destinataire», «document», «ÉDI», «expéditeur», «message», etc. Le premier sujet abordé par le

---

[19] En langage binaire, la lettre «a» s'écrit «1100001».

[20] En langage binaire, le chiffre «1» s'écrit «110001».

[21] Il existe des contrats-types ÉDI rédigés entre autres pour le Québec, le Canada, les États-Unis, les Royaume-Uni, France, Italie et autres pays européens, l'Australie et la Nouvelle-Zélande (voir Boss et Ritter, *supra* note 17).

[22] Voir Benyekhlef, *supra* note 18.

contrat-type est la notion de la normalisation des communications informatiques et de l'échange de documents informatisés. Ce sont les dispositions des articles 2, 3 et 4 qui traitent de cette question primordiale. Ces articles, de nature relativement technique, réfèrent à des annexes encore plus techniques ayant pour mission d'incorporer les normes ÉDI appropriées au secteur des activités industrielles des parties[23].

En ce qui concerne les transactions commerciales sur réseaux ouverts, il suffit donc de permettre aux commerçants qui désirent s'y aventurer d'utiliser une norme de communication informatique convenable. Ceci ne présente pas un obstacle à l'heure actuelle dans les réseaux ouverts. Contrairement aux réseaux privés, les réseaux ouverts, dont Internet, se trouvent dotés de toute la normalisation voulue pour permettre l'échange de documents numériques entre intervenants sans qu'ils aient à convenir à l'avance d'une norme de communication. Dans les faits, il existe déjà plusieurs normes qui permettent des communications informatiques efficaces à l'échelle mondiale par Internet[24]. Ainsi, en établissant un site convenable sur le World Wide Web d'Internet, un commerçant québécois peut offrir des biens et des services sur le marché mondial. Il peut faire une offre correspondant aux attentes du *Code civil* et recueillir l'acceptation d'un client qui «visite» son site. En ce qui a trait à l'échange des consentements, un contrat tout à fait valable en droit québécois s'en trouvera formé et ce, sans même avoir nécessité un contrat-cadre sur la normalisation des communications[25]. Un seul obstacle demeure : celui de l'identification des intervenants.

B. L'identification des personnes capables de contracter

Pour qu'il y ait acceptation d'une offre de contracter sur un réseau informatique ouvert, il doit y avoir un degré de certitude élevé dans l'identification des parties en présence et dans l'acheminement des messages. Nous avons vu que la certitude dans l'acheminement des messages et dans leur traduction en langage humain ne pose pas de problèmes importants. L'identification des intervenants est une tout autre question.

La nécessité d'identifier avec certitude les parties impliquées dans la négociation d'un contrat est, à toutes fins pratiques, absolue. En effet, l'établissement de l'identité du cocontractant est indéniablement requis par nombre de dispositions du *Code civil* :

---

[23] Voir la discussion sur les normes ÉDI dans la partie I ci-dessus.

[24] Songeons à la norme ASCII pour les caractères alphanumériques de base, la norme MIME pour les caractères accentués et les autres caractères non compris dans les caractères ASCII de base, les normes TCP/IP, SMTP et HTTP pour les transferts de données et le langage de balisage de documents numériques SGML qui comprend la norme HTML utilisée pour la normalisation et le balisage de documents numériques aux fins de présentation sur le World Wide Web. Dans le mesure où une norme ÉDI s'avérerait nécessaire ou souhaitable, une norme multi-sectorielle internationale comme la norme EDIFACT est disponible.

[25] L'intérêt du contrat-cadre est de permettre non seulement la communication compréhensible de messages numériques, mais également l'intégration de ces communications avec les systèmes comptables et de contrôle d'inventaire des participants, réalité au coeur même de l'ÉDI. Dans la mesure où une telle intégration n'est pas souhaitable ou nécessaire, le recours à un contrat-cadre peut être évité.

> **1388.** Est une offre de contracter, la proposition qui comporte tous les éléments essentiels du contrat envisagé et qui indique la volonté de son *auteur* d'être lié en cas d'acceptation [nos italiques].
>
> **1389.** L'offre de contracter émane de *la personne qui prend l'initiative* du contrat ou qui en détermine le contenu, ou même, en certains cas, qui présente le dernier élément essentiel du contrat projeté [nos italiques].
>
> **1398.** Le consentement *doit être donné par une personne qui, au temps où elle le manifeste, de façon expresse ou tacite, est apte à s'obliger* [nos italiques].

Dans les rapports contractuels traditionnels, l'identité des parties est établie par un ensemble de facteurs. La connaissance physique que les parties ont l'une de l'autre, composée du sexe, de la physionomie et des caractéristiques de la voix de la personne ainsi que de sa renommée sont les éléments sur lesquels nous nous fions pour identifier le cocontractant éventuel. Une fois satisfaits de son identité, nous négocions le contrat et exigeons, comme étape ultime de confirmation, que le cocontractant appose sa signature au contrat.

L'exigence d'identification et d'authentification est problématique dans un environnement numérique, mais pose moins de problèmes dans le cadre d'une transaction ÉDI en réseau fermé qu'en réseau ouvert. En effet, l'ÉDI en réseau fermé suppose que les parties à la transaction ont été en mesure de négocier une entente-cadre. Le seul but des dispositions du contrat d'interchange en ce qui concerne l'identité des parties et l'authentification des messages est de fournir le moyen technologique normalisé de distinguer les messages électroniques qui parviennent du cocontractant. Les parties utilisent ainsi des mots de passe ou autres codes secrets, de même que des techniques de chiffrement, afin de générer une signature numérique susceptible d'identifier l'origine et l'authenticité d'un message informatisé.

Contrairement au *Code civil du Bas Canada*, le *Code civil du Québec*, en vigueur depuis le 1er janvier 1994, définit la signature en termes suffisamment larges pour permettre de reconnaître juridiquement, en sus de la signature manuscrite classique que nous connaissons depuis le XVIe siècle, d'autres signes qui manifestent notre consentement[26]. Ainsi, l'article 2827 C.c.Q. déclare :

> La signature consiste dans l'apposition qu'une personne fait sur un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement.

Rien, dans le droit civil québécois, ne s'oppose donc à ce que la signature d'un acte se fasse par l'apposition, dans un document numérique, d'une série de codes identifiant le signataire avec suffisamment de certitude[27]. C'est en analysant les mécanismes de la signature numérique que nous pourrons déterminer si elle constitue une alternative convenable à la signature manuelle.

---

[26] Voir P. Trudel, G. Lefebvre et S. Parisien, *La preuve et la signature dans l'échange de documents informatisés au Québec*, Québec, Publications du Québec, 1993 à la p. 65.

[27] Voir *ibid.* aux pp. 87-88.

C. La signature numérique

L'article 2827 C.c.Q. nous offre un moyen adéquat pour implanter au Québec un régime d'identification et d'authentification électronique hors pair, susceptible de permettre d'identifier de façon convenable les intervenants dans le commerce électronique, même dans un environnement de réseau ouvert comme Internet.

La signature numérique fait appel à une technique de chiffrement, désignée sous le nom de «cryptographie par clés publiques», laquelle modifie un message numérique d'une façon toute particulière pour permettre d'en identifier le signataire. Il importe de comprendre comment cette méthodologie résout les problèmes reliés à l'identification des intervenants dans le cyberespace.

La cryptographie par clés publiques est susceptible de déploiement à grande échelle afin de faciliter à la fois la sécurité des données et l'identification des intervenants dans un environnement en réseau ouvert. Ce genre de déploiement à grande échelle est désigné par le vocable «infrastructure de clés publiques». Le système de cryptographie par clés publiques a été inventé en 1977 par trois professeurs du célèbre Massachusetts Institute of Technology, soit les professeurs Ron Rivest, Adi Shamir et Len Adleman. En 1982, ils fondèrent la société américaine RSA Data Security Inc. dans le but de commercialiser la méthode cryptographique qu'ils ont nommée *RSA public key cryptosystem*. Cette méthode est, pour le moment, si étroitement liée à cette société, qu'il convient d'y faire référence comme la méthode RSA.

La méthode RSA consiste en la détermination de deux clés d'encryption reliées entre elles. Un message encrypté avec l'une des deux clés ne peut être décrypté que par l'autre et vice versa. Le lien entre les deux clés est tel qu'il est, à toutes fins pratiques, impossible de deviner l'une des clés à partir de l'autre. Au coeur de la méthode RSA se trouve la prémisse mathématique qui reconnaît comme étant extrêmement difficile, sinon pratiquement impossible, de décomposer un nombre donné en des nombres primaires ayant été multipliés ensemble pour l'obtenir. La société RSA Data Security Inc. l'explique ainsi dans sa propre documentation commerciale :

> RSA public and private keys are actually each made up of two numbers — an *exponent* and a *modulus*. The modulus is common to both the public and the private key, and is the product of two very large prime numbers. Since the public key is, of course, made public, the best course for a potential attacker to take is to attempt to factor the modulus back into its component primes, thereby gaining the information required to derive the private key.
>
> But factoring is one of the most fundamentally difficult mathematical tasks — there are precious few "shortcuts." For example, using the best available techniques, factoring a single typical 200-digit RSA modulus would keep a network of one thousand high-powered (70 MIPS) workstations busy for over *one thousand years*. Even a Cray YMP® supercomputer would take tens of thousands of years just to crack *one user's* key[28].

[28] Cahier pub. de RSA Data Security Inc., 100 Marine Parkway, Redwood City, CA 94065 [italiques de l'original].

Grâce à la méthode RSA, il devient possible de concevoir ce qu'on appelle généralement la signature numérique. Supposons que tous les juristes du Québec soient dotés de courrier électronique sur Internet. Chaque juriste dispose également d'un logiciel d'encryption RSA et possède deux clés : une clé privée secrète, connue uniquement du juriste, et une clé reliée à la clé privée, mais qui est connue par sa corporation professionnelle qui la certifie et la rend publique.

Prenons l'exemple simplifié de deux juristes québécois : l'avocat André et le notaire Bernard. L'avocat André dispose d'un jeu de clés RSA : sa clé privée «alphasecrète» et sa clé publique correspondante «alphapublique», cette dernière étant certifiée (après vérification) par le Barreau du Québec comme étant la sienne. Parallèlement, le notaire Bernard dispose aussi de deux clés RSA : sa clé privée «betasecrète» et sa clé publique correspondante «betapublique», laquelle est, dans son cas, certifiée par la Chambre des Notaires du Québec comme étant la sienne.

Lorsque l'avocat André désire transmettre le message confidentiel «envoie-moi une copie de mon testament» au notaire Bernard, il utilise son logiciel de courrier électronique. Ce logiciel chiffre le texte du message à l'aide de la clé publique «betapublique» du notaire Bernard qu'André prend soin d'obtenir de la Chambre des Notaires du Québec. En même temps qu'il chiffre le message, le logiciel se sert du texte même du message («envoie-moi une copie de mon testament») pour distiller une empreinte numérique («100498») qui est également chiffrée, mais cette fois à l'aide de la clé privée «alphasecrète» d'André. Le message («envoie-moi une copie de mon testament») et son empreinte numérique («100498»), tous deux ainsi chiffrés, sont alors transmis par Internet à Bernard.

Le texte chiffré du message («envoie-moi une copie de mon testament») peut être inspecté à loisir lorsqu'il est en transit, mais le message lui-même ne peut pas être lu, car, ayant été chiffré avec la clé publique «betapublique» de Bernard, seule la clé «betasecrète» de ce dernier en permet le déchiffrement. Par contre, l'empreinte numérique du message («100498») peut être déchiffrée pendant le transit, car, ayant été chiffrée avec la clé privée «alphasecrète» d'André, elle peut être déchiffrée avec la clé publique «alphapublique» d'André, laquelle est généralement connue puisque publiée par le Barreau du Québec. Cependant, la technique de l'empreinte numérique est telle qu'il est pratiquement impossible de reconstituer le message lui-même («envoie-moi une copie de mon testament») à partir de son empreinte numérique («100498»)[29]. Le message est donc parfaitement sécurisé pendant qu'il est en transit sur Internet.

---

[29] *Ibid.* :

> The RSA Digital Signature employs a cryptographic "hashing" algorithm to create a message digest that is unique to each document, much like a fingerprint. If even a single bit of the document is changed, roughly 50% of the bits in the corresponding message digest will change. Furthermore, the hashing algorithm is a one-way function: the document content cannot be reconstructed from the bits of the message digest. With RSA's MD family of message digest algorithms — featuring 128-bit message digests — the probability that different documents will have the same digest by coincidence is

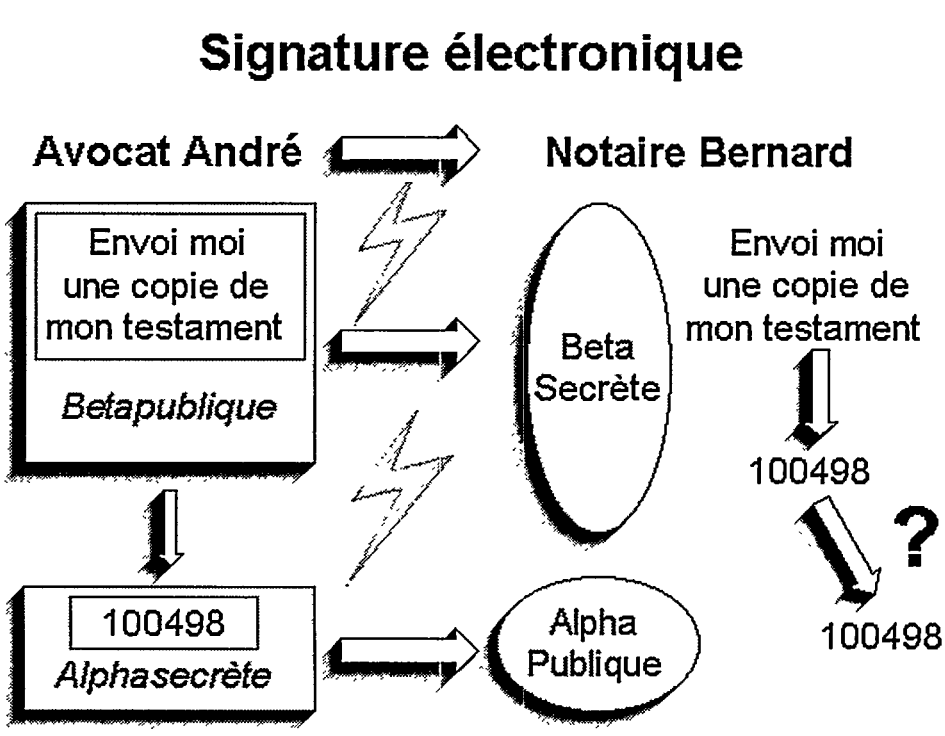
Bernard reçoit éventuellement le message chiffré et, voyant que le message provient d'André, obtient du Barreau du Québec la clé publique «alphapublique» d'André s'il ne l'a pas fait antérieurement. À l'aide de sa propre clé privée «betasecrète», il déchiffre le message («envoie-moi une copie de mon testament»). Ce déchiffrement se fait de façon transparente par son logiciel de courrier électronique. Ce logiciel se sert ensuite du texte du message pour distiller le même genre d'empreinte numérique que celle générée par l'ordinateur d'André et qui a accompagné le texte chiffré du message. En même temps que le logiciel de Bernard déchiffre le message, il tente de déchiffrer cette première empreinte numérique du texte du message en se servant de la clé publique d'André «alphapublique». Ensuite, le logiciel de Bernard compare les deux empreintes numériques : celle qui était chiffrée et qui a été reçue avec le message et celle que le logiciel vient de créer. Si les deux empreintes sont identiques, le logiciel peut en conclure avec quasi-certitude que :

- d'une part, l'expéditeur est l'avocat André. Cette conclusion s'impose puisque c'est la clé publique «alphapublique» d'André, certifiée par le Barreau du Québec, qui a permis de déchiffrer l'empreinte numérique du texte du message. Seul André aurait pu en être l'expéditeur, car un document chiffré par une clé de la paire de clés (en l'occurrence la clé «alphasecrète») ne peut-être déchiffré qu'avec l'autre clé du jeu (en l'occurrence la clé «alphapublique») ;
- d'autre part, le message n'a pas subi d'altération en transit. S'il en était autrement, les deux empreintes numériques du texte du message ne correspondraient pas.

Le diagramme ci-dessous démontre la complexité des opérations précédemment décrites. Mais comme c'est souvent le cas, ce qui est très difficile d'exécution et de compréhension pour l'homme devient très facile une fois soumis au traitement informatique.

---

less than 1 in a trillion *trillion*, effectively ensuring that two message digests will only match if their source documents are bit-for-bit identical (*ibid.* [italiques de l'original]).



Là où il existe des autorités de certification reconnues (comme le Barreau du Québec et la Chambre des Notaires) la méthodologie de la signature numérique administrée dans une infrastructure de clés publiques répond amplement au besoin juridique d'identification des parties en cause dans les transactions dématérialisées, que ce soit en réseau fermé ÉDI ou en réseau ouvert.

Cette méthodologie n'est toutefois pas parfaite. Elle demeure assujettie aux mêmes risques d'imperfection que toutes les autres institutions de l'Homme. Gardons à l'esprit notre point de départ : le risque ne s'élimine jamais, il ne peut qu'être géré. Il est évident que le risque le plus important survient lorsqu'une personne non autorisée s'empare de la clé privée et s'en sert à des fins illicites.

D'autre part, même si la clé privée demeure secrète, la méthode peut être compromise. La société RSA Data Security Inc. ainsi que certaines des sociétés se servant de la méthode RSA dans la conception de logiciels[30] voient leurs systèmes cryptographiques constamment soumis à des tentatives de compromission par des experts en cryptographie. Par exemple, grâce à son programme intitulé «Hack Netscape!», le groupe californien Community ConneXion incite les «hackers» partout dans le monde à compromettre la sécurité du logiciel Netscape conçu afin de faciliter les transactions commerciales sur le World Wide Web d'Internet.

[30] Soit par exemple les sociétés Microsoft, Novell, Sun Microsystems, Lotus Development Corporation, WordPerfect, AT&T, Netscape et Motorola.

Les premiers à compromettre la méthode RSA ont été, d'une part, un étudiant de l'École Polytechnique de Paris, Damien Doliguez[31] et, d'autre part, presque simultanément en Angleterre, David Byers et Éric Young[32]. Quelques semaines à peine après ce premier succès double d'août 1995, deux étudiants en cryptographie de l'Université de Californie à Berkeley, Ian Goldberg et David Wagner, ont réussi à déjouer ce même logiciel le 17 septembre 1995[33].

Or, ces brèches de sécurité ne semblent pas suffisamment importantes pour mettre en doute l'utilisation de la méthode RSA comme fondement de transactions sur réseaux ouverts. La brèche orchestrée par M. Doliguez a été réalisée grâce à l'utilisation simultanée de 111 postes de travail très puissants Unix et d'un super ordinateur pendant huit jours consécutifs à l'encontre d'une clé de 40 bits seulement. Le coût d'une telle concertation de pouvoir informatique est évalué à environ $10,000 US. La société Netscape soutient que des clés de 40 bits conviennent aux transactions dont les montants sont assez modestes, comme pour la plupart des achats de consommation ; dans le cas de transactions où les enjeux sont plus importants, la société Netscape recommande l'utilisation d'une clé de 128 bits. Le coût pour compromettre une telle clé serait d'environ $5,600,000,000,000,000,000,000,000,000,000 U.S.[34].

Somme toute, la signature numérique répond largement, nonobstant ses quelques failles, aux besoins d'identification et d'authentification existant présentement dans le cadre des communications sur réseaux ouverts. Manifestement, la signature numérique présente une certitude de résultat dans l'identification des intervenants ainsi qu'une sécurité face au maintien de la confidentialité des communications qui dépassent très largement ce qu'offrent les méthodes de communication traditionnelles. Personne ne peut prétendre qu'une communication par courrier électronique protégée par la méthode RSA est moins sécuritaire que l'envoi d'une lettre dans une enveloppe scellée. La même conclusion s'impose pour ce qui est des communications téléphoniques sur lignes terrestres et encore plus dans le cas des communications par téléphone cellulaire. Pourtant, les juristes québécois emploient ces méthodes couramment pour communiquer des renseignements protégés par le secret professionnel.

Il semble que les entreprises commerciales américaines soient de l'avis que la méthode RSA, telle qu'utilisée dans le logiciel Netscape™, donne ouverture à une certitude de résultat suffisante pour justifier son utilisation dans les transactions commerciales sur Internet[35]. Au Canada, la société de fiducie Bayshore Trust a annoncé qu'elle entendait entamer un service de prêts personnels sur le World Wide Web fondé

---

[31] Voir la déclaration publiée à http://Pauillac.inria.fr/~doliguez/ssl/announce.txt.

[32] Voir la déclaration publiée à http://www.dcs.ex.ac.uk/~aba/ssl/ (août 1995).

[33] Pour un récit assez complet voir M.J. Markoff, «Security Flaw is Discovered in Software Used in Shopping» *The New York Times* (19 septembre 1995) première page.

[34] Voir http://www.netscape.com/newsref/std/key_security.html.

[35] Voir Markoff, *supra* note 33 à la p. D21 : les sociétés américaines Wells Fargo Bank, MCI Communications, Internet Shopping Network et Virtual Vineyards se servent déjà de Netscape avec la méthode RSA pour conclure des transactions commerciales sur Internet.

sur la version de Netscape™ qui intègre la méthode RSA[36]. Dans le même reportage, la Banque de Montréal indiquait son intention d'offrir éventuellement des services financiers sur Internet[37].

D'ailleurs, le Comité consultatif sur l'autoroute de l'information recommande l'adoption d'un régime de cryptographie par clés publiques afin de faciliter le commerce électronique et de permettre l'échange sécuritaire de documents confidentiels (tels les communications entre avocats, notaires, médecins et leurs clients ou patients) :

> Le fait que les échanges commerciaux électroniques puissent créer un secteur économique entièrement nouveau souligne la nécessité de prévoir des mesures de sécurité électronique pour le commerce et la protection de la vie privée (rec. 10.11[38]). La libre circulation des renseignements et les échanges d'information sur l'autoroute favorisent le commerce électronique. Mais, il faut que les entreprises soient en mesure de vérifier l'identité des clients ou des entreprises avec lesquelles elles font des affaires. Cette vérification pourrait s'effectuer par l'entremise d'un mécanisme indépendant qui aurait la capacité de certifier l'identité des personnes concernées. Ce mécanisme, qui pourrait correspondre à un réseau d'authentification appelé *infrastructure de sécurité ; [sic] à clé publique*, se composerait d'un ou de plusieurs réseaux interfonctionnels qui relieraient des services d'authentification. Le Comité encourage le gouvernement, qui utilise lui-même une infrastructure de sécurité à clé publique, à prendre la tête du mouvement pour instaurer un mécanisme canadien commun et indépendant, doté de la capacité d'authentification (rec. 10.14). Il l'encourage aussi à favoriser la création de services de protection dans les domaines du secteur privé qui en ont besoin[39].
>
> [...]
>
> Pour assurer une base juridique valable à la sécurité des communications électroniques et des transactions commerciales, le Comité recommande au gouver-

---

[36] Voir «Trust Company Offers Loans via Internet» *The [Montreal] Gazette* (6 octobre 1995) C1. Ceux et celles désirant un prêt personnel doivent consulter http://www.bayshoretrust.com.

[37] *Ibid.*

[38] «Rec. 10.11» dans *Le défi, supra* note 2 à http://xinfo.ic.gc.ca/info-highway/final.report/fra/rec10.html :

> L'utilisation généralisée du commerce électronique offrira de nombreuses possibilités pour la croissance et la création d'emplois au Canada. Par conséquent, les gouvernements fédéral, provinciaux et territoriaux devraient travailler de concert pour tenter de résoudre les aspects juridiques, ainsi que ceux qui relèvent du contrôle commercial et d'autres questions touchant à la sécurité, qui pourraient entraver l'utilisation du commerce électronique au sein du gouvernement et du secteur privé, ainsi qu'au niveau international. Cette démarche devrait comprendre une mise à jour de diverses dispositions législatives fédérales, telles que la *Loi sur la preuve au Canada* et la *Loi d'interprétation*, pour refléter le rôle déterminant que joueront les transactions électroniques et les signatures numériques dans la conduite du commerce électronique sur l'autoroute de l'information. Il faudrait aussi déployer des efforts continus pour arriver à une plus grande uniformité en matière législative dans toutes les compétences canadiennes et avec nos principaux partenaires commerciaux.

[39] «Accès et incidences sociales : La dimension humaine» dans *Le défi, ibid.* à http://xinfo.ic.gc.ca/info-highway/final.report/fra/ch4.html#SECURITY [nos italiques].

> nement d'instaurer une infrastructure de sécurité à clé publique, c'est-à-dire un réseau de certification qui serve à encadrer le commerce électronique. Ceci fait partie de l'infrastructure juridique et pratique dont le Canada a absolument besoin pour participer à l'univers numérique et à l'économie mondiale[40].

L'implantation d'une telle infrastructure nécessitera un travail assez important puisqu'il s'agira de normaliser sur le plan juridique les règles qui s'appliqueront aux personnes qui désirent utiliser les réseaux ouverts comme moyen de communication sécuritaire. Cette normalisation nécessitera, dans une certaine mesure, le recours à une législation destinée à encadrer l'institution de la signature numérique. Ceci s'impose puisque le but recherché est de permettre le recours à la signature numérique dans un environnement de réseau ouvert par des intervenants n'ayant aucune relation antérieure à leur premier échange dématérialisé. Nous devons donc, dans cette hypothèse, exclure à toutes fins pratiques le recours au contrat comme outil de normalisation juridique.

Presque tous les auteurs s'entendent pour dire que la normalisation par voie de lois spéciales est une question délicate, puisque le législateur doit développer des règles qui s'harmonisent avec les développements commerciaux et qui interviennent avec le minimum de réglementation nécessaire pour permettre l'épanouissement des forces du marché[41]. Le législateur a donc intérêt à consulter le projet de loi type réalisé par le groupe de travail des Nations Unies sur la normalisation des transactions commerciales informatisées[42]. À l'heure actuelle, plusieurs juridictions américaines ont déjà adopté des lois pour reconnaître la signature électronique ou sont en train d'élaborer de telles lois. Mentionnons à titre d'exemple les États de l'Utah, de la Californie, de la Floride, de l'Oregon et de Washington[43]. Tous ces projets sont inspirés des travaux du Information Security Committee of the American Bar Association[44].

III. La preuve du contrat

Nous avons vu jusqu'ici que la conclusion d'un contrat par communication informatisée est possible en droit civil québécois et qu'il n'y a pas d'obstacles majeurs quant au fond juridique. Nous devons maintenant passer du fond à la forme, afin

---

[40] «Sommaire» dans *Le défi*, *ibid.* à http://xinfo.ic.gc.ca/info-highway/final.report/fra/exsum.html#ACCESS.

[41] Voir par ex. P. Trudel, «Interuet et commerce électronique : réglementation et autoréglementation», Conférence de l'Institut mondial ÉDI, Montréal, 30 et 31 août 1995 [non-publié] ; A.H. Boss, «Security: It Ain't Just a Matter of Encryption: The Development of Legal Infrastructures to Support the Growth of Electronic Commerce», Conférence de l'Institut mondial ÉDI, Montréal, 30 et 31 août 1995 [non-publié] ; B.M. Cremades et S.L. Plehn, «The New Lex Mercatoria and the Harmonization of the Laws of International Commercial Transactions» (1984) 2 Boston U. Int'l L. J. 317 ; M.J. Bonell, «Unification of Law by Non-Legislative Means: The UNIDROIT Draft Principles for Interuational Commercial Contracts» (1992) 40 Am. J. Comp. L. 617.

[42] Voir Benyekhlef, *supra* note 18.

[43] Voir A. Asay, «Introduction to the Law and Technology of Digital Signatures», Conférence de l'Institut mondial ÉDI, Montréal, 30 et 31 août 1995 à la p. 13 [non-publié].

[44] Voir Information Security Committee of the American Bar Association, *Digital Signature Guidelines : Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*, Chicago, Publication Policies & Contracting, 1996.

d'affronter le plus délicat des aspects juridiques relatifs aux contrats dématérialisés, soit la preuve.

La principale raison d'être du contrat est de nous permettre éventuellement de contraindre notre cocontractant à respecter ses engagements. C'est sur cet élément de contrainte que nous fondons notre appréciation du degré de certitude du résultat justifiant le risque commercial que nous courons dans la recherche du bénéfice. La manifestation la plus importante de cette contrainte est l'intervention des tribunaux pour ordonner l'exécution de l'engagement contractuel. En vue d'obtenir cette ordonnance, nous devons pouvoir faire la preuve devant le tribunal que le contrat existe bel et bien. Comment pouvons-nous faire cette preuve ? L'article 2811 C.c.Q. déclare :

> La preuve d'un acte juridique ou d'un fait peut être établie par écrit, par témoignage, par présomption, par aveu ou par la présentation d'un élément matériel, conformément aux règles énoncées dans le présent livre et de la manière indiquée par le Code de procédure civile ou par quelque autre loi.

Les principaux moyens auxquels nous avons généralement recours pour faire la preuve du contrat sont l'écrit et le témoignage. Ce sont, après tout, les deux procédés que nous utilisons pour exprimer notre volonté, volonté dont le contrat est l'expression juridique.

La preuve du contrat par témoignage fait toutefois l'objet d'importantes limitations. En effet, en vertu de l'article 2862 C.c.Q., elle n'est pas recevable lorsque la valeur en litige excède $1,500. Ce même article prévoit que, lorsque le contrat est passé dans le cours des activités d'une entreprise, la preuve testimoniale est recevable sans égard au montant, mais seulement à l'encontre du commerçant, jamais en sa faveur. Puisque ce que nous cherchons est d'assurer la force exécutoire du contrat en faveur du commerçant, pour le rassurer quant à la certitude du résultat recherché, nous ne pouvons nous fier au témoignage comme moyen de preuve du contrat dématérialisé.

Ceci nous ramène donc à l'écrit comme instrument privilégié pour faire la preuve du contrat. Lorsque nous négocions un contrat, nous prenons généralement soin de le rédiger par écrit et de le faire signer par les parties. Le but de cet exercice est de pouvoir remettre à chacune des parties un écrit susceptible de faire la preuve du contenu obligationnel du contrat et d'écarter la possibilité d'un éventuel témoignage visant à contredire les termes du contrat écrit.

Examinons les dispositions du *Code civil* suivant lesquelles le contenu obligationnel du contrat se prouve par un écrit sur support papier et ne peut être contredit par témoignage :

> **2826.** L'acte sous seing privé est celui qui constate un acte juridique et qui porte la signature des parties ; il n'est soumis à aucune autre formalité.
>
> **2827.** La signature consiste dans l'apposition qu'une personne fait sur un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement.

> **2829.** L'acte sous seing privé fait preuve, à l'égard de ceux contre qui il est prouvé, de l'acte juridique qu'il renferme et des déclarations des parties qui s'y rapportent directement.
>
> **2863.** Les parties à un acte juridique constaté par un écrit ne peuvent, par témoignage, le contredire ou en changer les termes, à moins qu'il n'y ait un commencement de preuve.

De prime abord, les dispositions du *Code civil* ne semblent pas poser d'entrave à la transposition de nos pratiques actuelles dans un monde dématérialisé. En effet, nous avons de bonnes raisons de croire que la signature numérique correspond à la notion de signature exigée par l'article 2826 C.c.Q.[45]. Nous savons également que cet article dispense l'acte sous seing privé de toute autre formalité. Ce que l'article 2826 C.c.Q. passe sous silence est de savoir si un document numérique binaire informatisé est un «écrit» au sens de l'article 2863 C.c.Q. Ceci est le noeud du problème pour le commerce électronique en ce qui concerne la preuve d'un contrat dématérialisé.

Le *Code civil* manque de rigueur dans la rédaction des articles 2826, 2827, 2829 et 2863 C.c.Q. ainsi que des autres articles du Livre septième *De la preuve*. À titre d'illustration, l'ensemble des 31 articles (2812-2842 C.c.Q.) du Chapitre premier du Titre deuxième de ce Livre, chapitre intitulé «De l'écrit», se servent tour à tour des expressions «acte», «document» et «écrit» sans pour autant définir ces termes importants. Dans le *Code civil,* le mot «document» revient 73 fois, le mot «écrit», 102 fois et le mot «acte», 359 fois. Autant de références à ces mots, mais aucune définition pour nous guider.

Afin d'éclaircir la situation, nous devons nous attarder tout particulièrement à l'étude d'une série de trois articles insérés au Chapitre premier et manifestement conçus afin de traiter de la question de la preuve des documents informatisés :

> SECTION VI : Des inscriptions informatisées.
>
> **2837.** Lorsque les données d'un acte juridique sont inscrites sur support informatique, le document reproduisant ces données fait preuve du contenu de l'acte, s'il est intelligible et s'il présente des garanties suffisamment sérieuses pour qu'on puisse s'y fier.
>
> Pour apprécier la qualité du document, le tribunal doit tenir compte des circonstances dans lesquelles les données ont été inscrites et le document reproduit.
>
> **2838.** L'inscription des données d'un acte juridique sur support informatique est présumée présenter des garanties suffisamment sérieuses pour qu'on puisse s'y fier lorsqu'elle est effectuée de façon systématique et sans lacunes, et que les données inscrites sont protégées contre les altérations. Une telle présomption existe en faveur des tiers du seul fait que l'inscription a été effectuée par une entreprise.
>
> **2839.** Le document reproduisant les données d'un acte juridique inscrites sur support informatique peut être contredit par tous moyens.

---

[45] Voir la partie II.C, ci-dessus.

C'est sur l'interprétation de ces trois articles que l'épanouissement du commerce sur l'autoroute de l'information au Québec dépend largement. Malheureusement, il existe déjà beaucoup de controverse quant à leur portée. Afin d'assurer un tel épanouissement, il nous faudrait conclure que ces articles sont en eux-mêmes convenables à cette fin. Si tel n'est pas le cas, il faudra adopter sans tarder les amendements qui s'imposent.

Les commentaires du ministre de la Justice nous renseignent quant à la source de ces trois articles de droit nouveau :

> Cet article [2837 C.c.Q.] relatif aux inscriptions informatisées constitue du droit nouveau. Il couvre, entre autres, les contrats conclus à distance et les contrats verbaux, dont les données sont directement inscrites sur support informatique ; il vise donc à réglementer des contrats d'entreprise ou certains contrats de consommation qui interviennent par l'utilisation de guichets automatiques et il permet de viser également certains paiements électroniques.
>
> L'article n'a toutefois pas la même utilité pour les actes juridiques constatés d'abord dans un écrit avant d'être inscrit [sic] sur support informatique, compte tenu de la règle de la meilleure preuve et du fait que les documents reproduisant des données informatisées peuvent être contredits par tous moyens. Ces documents ne seront recevables que dans les cas où une preuve secondaire peut être admise, ou encore dans le cas où des dispositions législatives, tels les articles 2840 à 2842, établissent qu'ils font preuve au même titre que l'original s'ils respectent les conditions par la loi.
>
> Le premier alinéa, qui s'inspire d'une recommandation du Conseil de l'Europe, pose deux conditions essentielles à la preuve de l'acte juridique : que le document reproduisant les données soit intelligible et qu'il présente des garanties suffisantes pour pouvoir s'y fier.[46]

Les recommandations du Conseil de l'Europe[47], auxquelles font allusion les commentaires du ministre de la Justice, ont été étudiées par la Commission des Nations Unies pour le Droit Commercial International («C.N.U.D.C.I.»)[48] et les principes de base sur lesquels ces recommandations sont fondées ont éventuellement inspiré le projet de loi type du C.N.U.D.C.I. publié par le gouvernement du Québec[49]. Contrairement aux recommandations du Conseil de l'Europe, qui ne visaient que la question de l'archivage par micrographie ou sur support informatique, le projet de loi type est censé servir de guide d'implantation pour le législateur qui entend adopter une loi ou modifier ses lois existantes pour faciliter les transactions commerciales dématérialisées. L'objet de ce projet de loi type est de voir à ce qu'une transaction dématérialisée,

---

[46] *Code civil du praticien : Loi sur l'application de la réforme du Code civil et commentaires du ministre de la justice*, Montréal, DacFo, 1995 aux pp. 929-30, art. 2837.

[47] Conseil de l'Europe, Comité des Ministres aux États membres, 341e réunion des Délégués des Ministres, Textes adoptés, Rec. N° R (81) 20, Recommandation relative à l'harmonisation des législations en matière d'exigence d'un écrit et en matière d'admissibilité des reproductions de documents et des enregistrements informatiques (1981).

[48] Voir A.H. Boss, «The International Commercial Use of Electronic Data Interchange and Electronic Communications Technologies» (1991) 46 Bus. Lwyr. 1787 à la p. 1790.

[49] Benyekhlef, *supra* note 18.

constatée par l'échange de données sur support informatique, ne soit pas entravée par les exigences traditionnelles nécessitant une signature manuscrite et une écriture sur support papier. En voici les principales dispositions :

> **Article 4 — RECONNAISSANCE JURIDIQUE DES MESSAGES DE DONNÉES**
>
> La valeur légale, la validité ou la force exécutoire d'une information ne sont pas refusées au seul motif qu'elle est présentée sous la forme d'un message de données.
>
> **Article 5 — ÉCRIT**
>
> 1- Lorsqu'une règle de droit exige qu'une information soit par écrit ou soit présentée par écrit, ou prévoit certaines conséquences si elle ne l'est pas, un message de données est conforme à cette exigence si cette information est accessible de manière à pouvoir être consultée ultérieurement.
>
> 2- [...]
>
> **Article 6 — SIGNATURE**
>
> 1- Lorsqu'une règle de droit exige une signature ou prévoit certaines conséquences en l'absence d'une signature, cette exigence est satisfaite dans le cas d'un message de données :
>
> a) Si une méthode est utilisée pour identifier l'initiateur du message de données et pour indiquer que cette personne approuve l'information qu'il contient ; et
>
> b) Si cette méthode est aussi fiable que cela était approprié au vu de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris tout accord entre l'initiateur et le destinataire du message de données.
>
> 2- [...]
>
> **Article 7 — ORIGINAL**
>
> 1- Lorsqu'une règle de droit exige qu'une information soit présentée sous sa forme originale, ou prévoit certaines conséquences si elle ne l'est pas, un message de données est conforme à cette exigence :
>
> a) Si l'information est exposée à la personne à laquelle elle doit être présentée ; et
>
> b) S'il existe une garantie fiable quant à l'intégrité de l'information entre le moment où elle a été composée pour la première fois sous sa forme définitive en tant que message de données ou autre, et le moment où elle est exposée.
>
> [...]
>
> **Article 8 — ADMISSIBILITÉ ET VALEUR PROBANTE D'UN MESSAGE DE DONNÉES**
>
> 1- Dans toute procédure légale, aucune disposition relative aux règles de preuve ne sera appliquée afin d'empêcher l'admission en preuve d'un message de données :
>
> a) Au motif qu'il s'agit d'un message de données ; ou,

> b) S'il s'agit de la meilleure preuve que la personne qui la présente peut raisonnablement escompter obtenir, au motif qu'il n'est pas sous sa forme originale.
>
> 2- Une information présentée sous la forme d'un message de données se voit accorder la force probante voulue. Lors de l'évaluation de la force probante d'un message de données, il est tenu compte de la fiabilité du mode de création, de conservation ou de communication du message de données, de la fiabilité du mode de préservation de l'intégrité de l'information, de la manière dont l'initiateur a été identifié et de tout autre facteur pertinent.
>
> 3- Sous réserve de toute autre règle de droit, lorsque l'information sous la forme d'un message de données est conforme aux exigences de l'alinéa b) du paragraphe 1 de l'article 8, cette information ne se voit accorder une force probante moindre au motif qu'elle n'a pas été présentée sous sa forme originale[50].

L'objectif essentiel recherché par les dispositions de la loi modèle C.N.U.D.C.I. est de donner lieu à un régime juridique essentiellement neutre, qui ne favorise ni ne défavorise une transaction pour le seul motif qu'elle est présentée sous forme de message de données informatiques plutôt que sous forme d'écrit signé. Dans les commentaires du ministre de la Justice, le législateur québécois ne fait pas référence à la loi modèle C.N.U.D.C.I., se contentant de renvoyer à la recommandation du Conseil de l'Europe que l'on peut considérer comme surannée, particulièrement si l'on tient compte de la rapidité des développements dans tout ce qui a trait à l'informatique et aux communications informatisées. Le législateur québécois a-t-il, par l'adoption des articles 2837 à 2839 C.c.Q., instauré un régime juridique neutre ne distinguant pas outre mesure entre le support papier et le support informatique comme moyen de conclusion des contrats ?

À cette question de grande importance s'ajoutent les questions suivantes qui en découlent ou servent à la compléter :

- Est-ce qu'une inscription en langage numérique binaire inscrite sur support informatique est un écrit ?

- Quel est le sens de l'article 2837 C.c.Q. lorsqu'il parle du «document» qui reproduit les données inscrites sur support informatique ? Cette notion de document serait-elle limitée à l'inscription des données informatiques sur support papier ?

- Est-ce que l'article 2837 C.c.Q. s'applique seulement à l'acte juridique concrétisé sur support informatique ou s'applique-t-il également à un contrat négocié antérieurement dont les données sont ensuite inscrites sur support informatique ?

- Quelle est la valeur probante de l'acte dématérialisé compte tenu de l'article 2839 C.c.Q. ?

Voilà autant de questions sur lesquelles l'unanimité fait défaut dans la doctrine. Voyons si on peut répondre à ces diverses interrogations d'une façon qui pose le moins d'obstacles possible aux transactions dématérialisées inscrites sur support informatique.

---

[50] *Ibid.*, art. 4-8, *passim*.

A. Est-ce qu'une inscription sur support informatique est un écrit ?

Il n'y a rien de tellement révolutionnaire à considérer l'inscription de données sur médium informatique comme de l'écriture. Le fait de se servir d'un stylo pour tracer les caractères de l'alphabet sur un papier ne se distingue pas vraiment du fait de se servir de la tête d'écriture d'un disque informatique pour polariser l'oxyde de métal sur la platine plastique d'une disquette : dans les deux cas, il y a écriture. Les seules différences sont au plan du langage utilisé (les langues occidentales se servent d'un langage écrit de 26 caractères, tandis que le langage informatique écrit se sert de deux caractères) et du moyen technologique de laisser des traces sur les médias d'écriture (stylo et papier versus tête d'écriture et platine). Dans les deux cas, des traces physiques sont laissées sur les médias. Dirions-nous que des inscriptions latines sur des tablettes de pierre ne sont pas des écrits ? Dans notre société moderne, il y a peut-être autant de gens capables de lire le latin que de gens capables de lire le langage bimaire informatique.

La réponse à la question dépend-t-elle de notre degré de familiarité avec le moyen d'écriture et le langage choisi ? Sommes-nous plus disposés à reconnaître comme écriture le latin gravé sur la pierre que le texte ASCII binaire inscrit sur la disquette ? Nous devrions être plus rigoureux dans notre analyse et nous fonder sur une appréciation de la nature même de ce qu'est l'écriture, plutôt que sur nos préjugés fondés uniquement sur la technologie avec laquelle nous sommes déjà familiers. Une telle vision des choses nous permettrait d'arriver à la conclusion que, même en l'absence de textes de loi, l'inscription de données sur support informatique est de l'écriture et constitue un écrit au sens du *Code civil.*

L'analyse des article pertinents du *Code civil* vient corroborer cette hypothèse. En effet, les articles 2837 à 2839 C.c.Q., qui forment la section intitulée «des inscriptions informatisées», se trouvent au chapitre premier, intitulé «de l'écrit», du deuxième titre du Livre septième, portant sur la preuve. Le chapitre «de l'écrit» répertorie tout d'abord les copies de loi (art. 2812 C.c.Q.), puis les actes authentiques (2813-2821 C.c.Q.) et semi-authentiques (2822-2825 C.c.Q.). Il traite ensuite des actes sous seign privé (2826-2830 C.c.Q.), puis des «autres écrits» (2831-2836 C.c.Q.). Ces derniers comprennent les papiers domestiques et autres écrits non-signées. Le chapitre «des écrits» se continue par la section traitant «des inscriptiuons informatisées», pour finalement se clore par les articles portant sur «la reproduction de certains documents» (2840-2842 C.c.Q.). Il apparait donc, selon la géographie interne du *Code civil*, que les inscriptions électroniques constituent bel et bien des écrits, au même titre que les documents sur papier. Cette conclusion est appuyée davantage par l'utilisation que fait le législateur du verbe «inscrire» et du mot «inscription», de même racine que le mot «écrit», aux articles 2837 et 2838 C.c.Q.

Un argument contraire peut être présenté, à l'effet que l'énumération des écrits est close par la section V (2831-2836 C.c.Q.), intitulée «des autres écrits». Cette énumération serait dès lors exhaustive, ce qui exclurait les inscriptions informatiques du domaine des écrits. Celles-ci s'apparenteraient dès lors à la «reproduction de certains documents», et n'auraient de rôle à jouer que dans la détermination du *contenu* de

certains écrits. Selon nous, cet argument ne saurait s'avérer concluant, face à la structure claire du chapitre de la preuve.

Le *Code civil* semble donc ouvrir la porte à la reconnaissance des inscriptions électroniques en tant qu'écrits. Une telle conclusion serait par ailleurs propice au développement du commerce électronique au Québec. Comme nous pourrons le constater plus loin, l'infrastructure mise en place au *Code civil* ne reconnait toutefois pas aux inscriptions électroniques le même statut qu'aux écrits sur papiers, ce qui risque de causer des problèmes dans le future[51].

B. *Quel est alors le sens de l'article 2837 C.c.Q. lorsqu'il parle du «document» qui reproduit les données inscrites sur support informatique ?*

Le fait demeure que l'inscription de données sur support informatique est un écrit d'un genre très particulier qui mérite un traitement particulier. Même s'il était humainement possible de parvenir à lire un disque informatique sans support informatique en déchiffrant la polarisation des oxydes de métal, cette lecture serait pénible. Elle serait par contre un peu moins ardue que de lire un texte écrit en hiéroglyphes égyptiens. En ce sens, l'écriture informatique, même si elle est lisible, n'est pas raisonnablement intelligible pour le commun des mortels.

En vertu de l'article 2837, le *Code* nous dispense de cette tâche épineuse en permettant exceptionnellement la production d'un «[...] document reproduisant ces données [...] s'il est intelligible et s'il présente des garanties suffisamment sérieuses pour qu'on puisse s'y fier». En ceci, le *Code* fait une concession particulière, permettant la production non pas de l'original, mais d'une copie de l'original. La production de l'original imposerait la présentation de la disquette ou fort probablement du disque fixe, ce qui serait très peu pratique. Par contre, la partie sur laquelle repose le fardeau de la preuve devra démontrer que le document est une reproduction fiable de l'acte juridique constaté sur le support informatique. Ceci ne revient peut-être pas à présenter une expertise pour faire le lien entre les particules d'oxyde de métal polarisées et le texte de l'acte juridique, mais cela requiert néanmoins une expertise quant aux systèmes informatiques impliqués et à la fiabilité du processus de traduction des données.

Le terme «document» ne fait pas l'objet d'une définition dans le *Code civil.* Toutefois, si nous faisons référence aux articles du *Code* qui utilisent ce mot, nous sommes en mesure de constater que le seul support satisfaisant à tous les emplois de ce terme est l'écriture sur support papier. Il n'y a toutefois rien qui exclut expressément le recours à une interprétation plus libérale, qui permettrait d'admettre d'autres supports à titre de «documents» tel que suggéré par les articles 2837 et s. C.c.Q. Pour leur part, Pierre Trudel, Guy Lefebvre et Serge Parisien soumettent que la présentation des informations sur un écran cathodique serait satisfaisante pour les fins de ces articles[52]. Étant donnée l'absence d'une définition, nous devrons malheureusement demeurer

[51] Voir la partie III.C, ci-dessous.

[52] *Supra* note 26 à la p. 24.

dans l'incertitude en attendant soit une intervention législative, soit une interprétation jurisprudentielle du terme «document».

Puisque nous savons à tout le moins que le «document» dont parle l'article 2837 C.c.Q. est certainement un écrit, sommes-nous en mesure de conclure, tel que suggéré plus haut, que l'acte juridique lui-même inscrit sur support informatique est un écrit ? Un argument peut certainement être reçu à l'effet que ce n'est que le document reproduisant les données de l'acte informatisé qui constitue un écrit au sens de la loi. Dans cette optique, le seul intérêt des articles 2837 et s. C.c.Q. serait d'écarter la règle de la meilleure preuve en matière d'imprimés provenant d'inscriptions informatisées.

Ceci est d'ailleurs la voie emprunté par certains auteurs, dont Jean-Claude Royer et Léo Ducharme. Selon eux, l'acte juridique inscrit sur support informatique n'est pas tout à fait un écrit :

> [d]ans ces cas [où le contrat est inscrit sur support informatique au moment même de sa formation], le document reproduisant l'inscription informatisée est recevable. Les articles 2860 et 2863 du *Code civil du Québec* ne s'appliquent pas, puisque l'acte juridique n'est pas constaté par écrit. Par ailleurs, les articles 2862 et 2843 du même Code ne limitent que la recevabilité d'une preuve par témoignage ou par déclaration extrajudiciaire[53].

Cette interprétation engendre d'autres conclusions créant à leur tour des nouvelles difficultés d'interprétation. Il suffit de citer l'extrait suivant de *La preuve civile* pour en constater la complexité :

> 415 — *Preuve contraire* — Comme les autres écrits prévus aux articles 2831 à 2834 du *Code civil du Québec*, le document reproduisant les données d'un acte juridique sur support informatique peut être contredit par tous les moyens [2839 C.c.Q.]. Cette règle s'applique, même si l'inscription informatisée a été effectuée au moyen d'une carte magnétique permettant d'identifier son auteur. Il est vrai que la signature électronique peut être comprise dans la définition de la signature énoncée à l'article 2827 C.c.Q. Cependant, le document qui reproduit l'inscription informatisée n'est pas un acte sous seing privé. Il est exclusivement réglementé par les articles 2837 à 2839 du *Code civil du Québec*[54].

Si, malgré la présence d'une signature, l'inscription informatique d'un acte juridique n'était pas un acte sous seing privé, ce ne pourrait être que pour la raison que cet acte n'est pas en lui-même équivalent à un écrit : car nous savons qu'un acte juridique constaté dans un écrit et comportant une signature est un acte sous seing privé au sens de la loi.

Ducharme prend une position moins restrictive quant à la nature de l'acte juridique inscrit sur support informatique, mais il explore la question avec un regard moins intense que Royer. Tout comme ce dernier, Ducharme tente de déterminer si l'article 2837 C.c.Q. s'applique à tous les actes dont les données sont inscrites sur support informatique ou seulement à ceux de ces actes pour lesquels le médium du support in-

---

[53] J.-C. Royer, *La preuve civile*, 7e éd., Cowansville, Yvon Blais, 1995 à la p. 229 ; voir également L. Ducharme, *Précis de la preuve*, 4e éd., Montréal, Wilson & Lafleur, 1993 à la p. 156.

[54] Royer, *ibid.* à la p. 231.

formatique a servi à la conclusion de l'acte. Cette discussion mène à la fois Ducharme et Royer à affirmer que l'article 2837 C.c.Q. ne vise que ces derniers actes. Selon eux, conclure autrement bouleverserait bien d'autres règles du *Code civil*. Le passage suivant du *Précis de la preuve* est indicatif des problèmes que ces auteurs craignent si l'interprétation contraire était retenue :

> 463. [...] Cette interprétation s'appuie tout d'abord sur un argument de texte. En effet, la portée de l'article 2837 C.c.Q. est limitée aux cas dans lesquels les données d'un acte juridique sont inscrites sur support informatique. Cette expression laisse entendre qu'il doit y avoir simultanéité entre l'expression de la volonté et son inscription sur support informatique. Lorsque c'est oralement ou par un écrit que la volonté des parties s'est d'abord exprimée et que l'inscription sur support informatique n'est intervenue qu'après coup, il est difficile de prétendre que ce sont alors les données de l'acte juridique qui ont été inscrites. Si l'acte s'est accompli par écrit, l'inscription portera sur les données de cet écrit et s'il a lieu oralement, sur les données du témoignage de celui qui en est l'auteur.
>
> 464. [...] En effet, tant la règle de la meilleure preuve énoncée à l'article 2860 C.c.Q., que la règle de la prohibition du ouï-dire énoncée à l'article 2853 C.c.Q. s'opposent à ce que de simples informations conservées sur support informatique soient traitées différemment des mêmes informations consignées par écrit. Peut-on concevoir, par exemple, que si les données d'un acte notarié sont transcrites sur support informatique, le document reproduisant ces données fasse preuve du contenu de l'acte ? L'article 2846 C.c.Q., en exigeant que l'acte juridique constaté dans un écrit soit prouvé par la production de l'original ou d'une copie qui légalement en tient lieu, s'oppose évidemment à ce qu'on puisse prouver un acte notarié par le moyen d'un document reproduisant les données de cet acte transcrites sur support informatique. De même, la prohibition de la preuve par ouï-dire exprimée à l'article 2853 C.c.Q. s'oppose à ce que des déclarations concernant l'accomplissement d'un acte juridique servent à établir l'existence de cet acte, du seul fait qu'elles ont été enregistrées sur support informatique au lieu d'être simplement mises par écrit.
>
> 465. Pour les deux raisons que nous venons d'invoquer, il appert donc que la portée des articles 2837 à 2839 C.c.Q. doit être limitée au seul cas dans lequel le support informatique a été substitué au support papier pour l'expression d'un acte juridique[55].

Par contre, l'interprétation de Royer et Ducharme est contestée par Claude Fabien[56] ainsi que par Trudel, Lefebvre et Parisien, lesquels écrivent :

> Que penser de ces deux thèses qui s'affrontent ? Malgré l'opinion du professeur Ducharme, il paraît plus raisonnable de soutenir, tout comme le professeur Fabien, que l'article 2837 doit être interprété largement. [...] En créant une section spécifique concernant les inscriptions informatisées, le législateur québécois n'a probablement pas voulu en réduire la portée au simple cas des transactions qui sont conclues directement au moyen d'un ordinateur. Cela serait mé-

---

[55] Ducharme, *supra* note 53 à la p. 156.

[56] Voir C. Fabien, «La communicatique et le droit civil de la preuve» dans *Le droit de la communicatique : actes du colloque conjoint des facultés de droit de l'université de Poitiers et de l'université de Montréal*, Montréal, Thémis, 1992.

> connaître la plupart des transactions conclues dans la vie quotidienne. En effet, même si de plus en plus de transactions sont conclues directement par ÉDI, il n'en demeure pas moins que bon nombre de celles-ci sont toujours arrêtées selon un moyen traditionnel, pour ensuite être enregistrées sur support informatique. On a qu'à penser à la réservation d'un billet d'avion. [...]
>
> Doit-on conclure que le législateur ne voulait pas régir ce type de transactions lorsqu'il a édicté les règles applicables aux inscriptions informatisées ? Nous en doutons fortement. Ces exemples sont, selon nous, plus convaincants que celui du contrat notarié utilisé par le professeur Ducharme pour nier l'applicabilité du *Code civil du Québec* aux transactions conclues oralement ou par écrit et, subséquemment, inscrites sur support informatique[57].

C. *Vers une solution appropriée à cette problématique*

Si l'on part de la prémisse selon laquelle l'acte inscrit sur support informatique est lui-même un écrit, presque toutes les difficultés soulevées par ces auteurs ont tendance à se dissiper. En effet, si l'inscription sur support informatique est (sous réserve des conditions imposées par les articles 2837 et 2838 C.c.Q.) elle-même un écrit, les autres règles du *Code civil* peuvent simplement recevoir application et aucun problème n'est posé. Inutile alors de distinguer entre le traitement des actes juridiques et des faits juridiques sur support informatique, sujet qui a lui-même fait couler beaucoup d'encre[58], ni de savoir si l'acte a été directement conclu sur support informatique et ensuite transcrit. Dans le cas du support papier, si nous sommes en présence d'un contrat signé, nous ne nous posons pas la question de savoir si le contrat était à ses débuts une entente orale ou s'il a été précédé d'un avant-contrat. L'inscription informatisée, reconnue comme un écrit, peut dès lors revêtir toutes les formes et prendre toutes les nuances de l'écrit sur support papier que nous connaissons de longne date. Rien ne s'opposerait alors à la notion d'actes sous seing privé (voir les propos de Royer ci-dessus) ou même d'actes notariés sur support informatique (contrairement aux inquiétudes de Ducharme précédemment mentionnées)[59].

Peut-on conclure, dans l'état actuel du droit au Québec, que l'acte juridique inscrit sur support informatique est un écrit ? Nous croyons que la réponse ne peut être que non. Nous pensons, malheureusement, et avec beaucoup de respect pour l'opinion contraire, que Royer a raison quand il écrit que cet acte «est exclusivement réglementé par les articles 2837 à 2839 du *Code civil du Québec*»[60] qui forment en-

---

[57] *Supra* note 26 à la p. 23.

[58] Voir *ibid.* à la p. 27 et s.

[59] D'ailleurs, la Chambre des Notaires du Québec propose justement, par son projet très ambitieux *cybernotariat*, de conclure des actes notariés sur les inforoutes. Voir à cet effet le mémoire intitulé «Le projet d'infrastructure de certification notariale» déposé le 12 septembre 1996 par la Chambre des Notaires auprès de la Commission Parlementaire de la Culture de l'Assemblée Nationale dans le cadre des audiences sur les enjeux du développement de l'inforoute québécoise ; voir également les témoignages en date du 30 octobre 1996 devant ladite Commission par les M[es] Cloutier et Perreault à http://www.assnat.qc.ca/fra/Publications/debats/JOURNAL/CC/961030/1650.HTM#961030007 (16 juin 1997).

[60] *Supra* note 53 à la p. 231.

semble une suite étanche d'articles et qui donnent lieu à un régime de preuve spécial et à part pour les actes juridiques inscrits sur support informatique. Ce régime n'a, somme toute, que peu de rapport avec les règles de preuve, par ailleurs très complètes et nuancées, qui se rapportent aux actes juridiques traditionnels inscrits sur support papier.

Qu'est-ce qui nous empêche, dans l'état actuel du droit, de retenir la thèse de l'inscription sur support informatique en tant qu'écrit ?

Selon nous, le problème réside dans la rédaction fautive des articles 2837 et 2839 C.c.Q.. Ceux-ci auraient dû être rédigés de façon à faire de l'inscription de l'acte juridique ou du fait juridique sur support informatique un écrit comme tous les autres écrits, avec la seule réserve que cet écrit puisse se prouver par une reproduction intelligible jugée fiable et conforme. Ceci constitue d'ailleurs l'essentiel de la recommandation du projet de loi type du C.N.U.D.C.I. que nous avons précédemment étudié.

Voici précisément où la rédaction de ces articles laisse à désirer. Souvenons-nous qu'ils se lisent ainsi :

> **2837.** Lorsque les données d'un *acte juridique* sont inscrites sur support informatique, le document reproduisant ces données *fait preuve du contenu de l'acte*, s'il est intelligible et s'il présente des garanties suffisamment sérieuses pour qu'on puisse s'y fier [italiques de l'auteur].
>
> Pour apprécier la qualité du document, le tribunal doit tenir compte des circonstances dans lesquelles les données ont été inscrites et le document reproduit.
>
> **2839.** Le document reproduisant les données d'un acte juridique inscrites sur support informatique peut être contredit par tous moyens.

Selon nous, ces articles auraient dû être rédigés de la façon suivante :

> **2837.** Lorsque les données d'un acte juridique *ou d'un fait juridique* sont inscrites sur support informatique, *cette inscription est réputée à toutes fins un écrit si le document reproduisant ces données* est intelligible et s'il présente des garanties suffisamment sérieuses pour qu'on puisse s'y fier.
>
> Pour apprécier la qualité du document, le tribunal doit tenir compte des circonstances dans lesquelles les données ont été inscrites et le document reproduit.
>
> **2839.** *La conformité du* document reproduisant les données d'un acte juridique *ou d'un fait juridique* inscrites sur support informatique *à l'inscription de ces données sur le support informatique* peut être *contredite* par tous moyens.

Le fait d'avoir tenté de traiter à la fois la question de l'admissibilité et la question de la valeur probante de l'inscription d'un acte juridique sur support informatique est la source du problème. Dans l'état actuel du droit, en se remettant à ces articles tels que présentement rédigés, si l'on accepte de considérer cette inscription comme un écrit, on vient immédiatement se heurter au dilemme de réconcilier la situation de l'inscription informatique qui serait signée versus l'inscription électronique non signée et la valeur probante divergente qui résulte alors entre l'inscription informatisée et le même acte sur support papier. Car un écrit traditionnel signé ne peut se contredire par témoignage (art. 2863 C.c.Q.), tandis que ce genre de témoignage demeure

admissible dans le cas de l'inscription informatisée. Au fond, la rédaction fautive de ces articles prend sa source dans un certain manque d'appréciation par le législateur de la nature des rapports existant dans un environnement de communication informatique. Les procédés informatiques permettent désormais d'avoir recours à la signature dématérialisée. Notre droit devrait donc reconnaître l'équivalence entre l'inscription informatisée et l'inscription sur support papier. Les articles 2837 et 2839 C.c.Q. ont été adoptés sur la foi d'une recommandation du Conseil de l'Europe datant de 1981[61], sans tenir compte de l'évolution de la technologie et du droit de l'informatique depuis plus de 13 ans. Même à l'époque où le *Code civil* était en voie d'adoption en juin 1991, le travail des Nations Unies sur le projet de loi modèle C.N.U.D.C.I., qui propose de donner lieu à nne équivalence juridique entre le numérique et le papier, était très avancé et les notions de la signature numérique et des infrastructures de clés publiques étaient déjà connues[62].

Les problèmes d'interprétation soulevés ci-dessus par les auteurs risquent de poser un obstacle sérieux au développement du commerce électronique. Le régime de preuve résultant équivaut à considérer le document comme n'ayant pas la valeur d'un acte sous seing privé. Ceci est désolant, surtout si l'on considère que les experts du domaine informatique s'entendent pour dire que la méthode de la signature numérique donne lieu à un degré de certitude dans les transactions commerciales qui dépasse de loin tout ce que l'on obtient aujourd'hui en utilisant un support papier[63].

Le problème ne se pose pas de façon tout aussi aiguë dans le cas de transactions ÉDI en réseau fermé puisque, comme nous l'avons vu, ces transactions peuvent généralement être encadrées par un contrat préalable d'interchange de données qui peut suppléer aux lacunes du *Code civil* au chapitre de la preuve des transactions dématérialisées. Quoique certains doutes aient été exprimés quant au caractère licite de telles conventions, la majorité des auteurs s'accordent pour affirmer leur légalité[64]. Cependant, le problème demeure entier dans le cas des transactions sur réseaux ouverts, puisque le recours au contrat préalable s'avère une solution irréaliste dans un grand pourcentage des cas[65].

Conclusion

Quels apports juridiques et technologiques sont donc nécessaires afin de rendre l'inforoute propice aux transactions commerciales ?

Il est évident qu'une adaptation s'impose si nous désirons tirer pleinement profit des nouvelles opportunités que nous offrent les technologies de communication in-

---

[61] *Supra* note 47.

[62] U.N.C.I.T.R.A.L., «Legal Issues of Electronic Data Interchange» (1991) 22 *Yearbook of the United Nations Commission on International Trade Law* 381 ; voir aussi National Institute of Standards and Technology, «A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)» (1991) 56:169 U.S. Fed. Reg. 42980 à la p.42981.

[63] Voir Asay, *supra* note 43 à la p. 5.

[64] Voir Trudel, Lefebvre et Parisien, *supra* note 26 aux pp. 98-100.

[65] Voir Boss, *supra* note 10 à la p. 304.

formatique. Plusieurs chemins s'offrent à nous. Or, l'histoire nous enseigne que les chemins naturels sont les plus efficaces.

Songeons pour un moment, à titre d'exemple, aux sentiers que nous empruntons naturellement par opposition à ceux qui nous sont imposés de façon arbitraire. Des sentiers très naturels se dessinent de façon inévitable dans le gazon de nos parcs et endroits publics très fréquentés. Ces sentiers tracent le plus souvent une série de belles courbes, mais suivent rarement la voie pavée dessinée par l'architecte ou l'urbaniste. Il apparaîtrait plus efficace pour les architectes et urbanistes de tenter de déceler ces sentiers naturels et ensuite de leur fournir une chaussée convenable plutôt que de choisir un trajet arbitraire, pour ensuite ériger des clôtures afin de barrer l'accès aux pelouses.

Ce parallèle illustre bien la théorie de réglementation fondée sur le libre marché. Les solutions qui correspondent aux attentes naturelles des gens sont généralement les meilleures. Nous avons vu que le cadre juridique québécois laisse à désirer en fait d'infrastructure pour l'épanouissement du commerce électronique. D'une part, nous nous devons d'innover pour mettre en place une infrastructure de clés publiques ou un autre moyen qui nous permettra d'etablir de façon certaine l'identité des parties. D'autre part, le régime de la preuve des transactions dématérialisées ne donne pas lieu à une certitude de résultat similaire à celle que l'on obtient en utilisant le support papier.

Nous suggérons donc que le gouvernement du Québec et ses organismes de réglementation adoptent, dans un avenir rapproché, des règles qui favorisent l'épanouissement de l'économie québécoise sur l'autoroute de l'information, tout en ayant le moins d'impact possible sur l'environnement et les institutions juridiques que nous connaissons et maîtrisons déjà. À cet effet l'auteur propose :

- l'établissement, de concert avec l'industrie de l'informatique québécoise et l'Office des professions, d'une infrastructure de clés publiques pour desservir les professionnels du Québec, laquelle serait administrée par les corporations professionnelles et subventionnée entièrement par les utilisateurs. Ces corporations professionnelles certifient déjà la qualité professionnelle de leurs membres envers le public et il est naturel qu'elles jouent ce rôle à l'avenir dans un contexte de rapports dématérialisés ; et
- l'amendement des articles 2837 à 2839 du *Code civil* tel que suggéré ci-dessus, pour faire de l'inscription informatisée un écrit, conformément aux recommandations de l'Organisation des Nations Unies.

Le Québec a déjà une réputation mondiale enviable dans le domaine de l'informatique. Il se doit d'aller de l'avant et de servir de modèle au monde entier.

Dans l'économie axée sur le savoir, le rapport de la croissance économique a changé. Tandis que la théorie économique classique voulait que la croissance économique soit le résultat du cumul des capitaux et du travail, la croissance économique à l'ère de l'économie axée sur le savoir requiert le cumul des capitaux, du travail et de

l'innovation[66]. Si le Québec innove en établissant un environnement juridique et une infrastructure technologique propices à l'épanouissement du commerce électronique, les industries québécoises qui auront participé à l'implantation de cette infrastructure jouiront d'un marché mondial pour leurs produits.

---

[66] Voir Johnston et Handa, *supra* note 9 aux pp. 212-13.