Université de Montréal

LA CONVENTION RELATIVE À LA PREUVE ET À LA CONSERVATION DE DOCUMENTS ÉLECTRONIQUES D'ENTREPRISE : PERSPECTIVES JURIDIQUES

Par

Éric Dunberry

Faculté de droit

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître en droit (LL.M.)

Avril 2000

Page d'identification du jury

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé

LA CONVENTION RELATIVE À LA PREUVE ET À LA CONSERVATION DE DOCUMENTS ÉLECTRONIQUES D'ENTREPRISE : PERSPECTIVES JURIDIQUES

Présenté par

Éric Dunberry

a été évalué par un jury composé des personnes suivantes :

Claude Fabien	président du jury
Jacques Frémont	directeur de recherche
Pierre Trudel	membre du jury

Mémoire accepté le 5 juillet 2000

SOMMAIRE

Ce mémoire pose l'hypothèse et tente de démontrer que la mise en œuvre d'une convention relative à la preuve et à la conservation de documents électroniques (la « Convention ») constitue un outil efficace de gestion de risques juridiques liés à l'utilisation de documents électroniques. Il prend comme toile de fond les échanges commerciaux réalisés sur Internet entre partenaires intégrés œuvrant en amont des consommateurs et, dans ce cadre spécifique, traite de l'environnement juridique, de l'architecture, du contenu et de la mise en œuvre d'une Convention adaptée.

En première partie du mémoire, l'auteur discute de la raison d'être de la Convention. Il traite du commerce électronique et ses risques propres, du document électronique et ses attributs distinctifs et de la finalité de l'archivage. Il aborde l'origine et les manifestations des risques juridiques liés à l'utilisation de documents électroniques et examine le bien-fondé de la Convention comme outil de gestion efficace de ces risques.

L'analyse révèle que le commerce électronique intervient par l'échange de données numériques inintelligibles, dénuées de substrat matériel et de structure permanente. Ces échanges ont lieu dans un environnement décentralisé, dématérialisé et transnational, qui connaît la pluralité des règles de droit et la concurrence de régimes normatifs et de forums compétents. Il en résulte pour l'entreprise de nouveaux risques juridiques liés à la reconnaissance des documents électroniques et à la fiabilité des données qu'ils contiennent aux fins probatoires, statutaires ou administratives pour lesquels ils ont été créés et conservés. Ces risques découlent de l'incertitude du droit dans le cyberespace et des difficultés d'application aux documents dématérialisés de notions juridiques traditionnelles tels la signature, l'écrit et l'original.

L'auteur démontre que la Convention constitue un outil efficace de gestion de ces risques juridiques. Elle est licite et en phase avec la réalité du cyberespace où l'autoréglementation et le consensualisme régissent utilement les échanges. Elle est négociée pour s'adapter aux situations juridiques prévalant entre partenaires commerciaux, tenant compte de leur spécificité et de l'évolution prévisible du droit et des technologies.

En seconde partie, l'auteur discute de l'élaboration de la Convention. Il identifie des principes directeurs et les balises contenues dans des régimes normatifs canadiens et

internationaux en matière de commerce électronique pour guider des parties contractantes. Il conclut que l'architecture de la Convention doit se fonder sur l'établissement d'équivalences fonctionnelles entre un monde papier, et son droit positif, et un monde virtuel, et ses incertitudes juridiques. Ce processus exige la création et le maintien, aux plans technologique, contractuel et opérationnel, d'un environnement garantissant la fiabilité des documents électroniques tout au long de leur cycle de vie. Enfin, l'auteur livre aux entreprises ses réflexions concrètes en vue de la négociation du contenu obligationnel et de la mise en œuvre de la Convention.

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

LISTE DES SIGLES ET ABRÉVIATIONS

AAA	American Arbitration Association
ABA	Association du Barreau Américain
B.R.	Cour du Banc de la Reine
C. de D.	Cahiers de droit
C.A.	Cour d'appel
C.c.B.C.	Code civil du Bas-Canada
C.C.C.	Canadian Criminal Cases
C.c.Q.	Code civil du Québec
C.P.	Cour provinciale
C.p.c.	Code de procédure civile
CCI	Chambre de commerce internationale
C.Q.	Cour du Québec
C.S.	Cour supérieure
CAI	Commission d'accès à l'information
CDROM	Compact Disk – Read Only Memory
CHLC	Conférence pour l'harmonisation des lois du Canada
CIREDIT	Centre International de Recherche et d'Étude de Droit de l'Informatique et des Télécommunications
CNUDCI	Commission des Nations-Unies pour le droit commercial international
CRDP	Centre de recherche en droit public de l'Université de Montréal
EDI	Échange de données informatisées
EDIA	Standard Data Interchange Agreement

LISTE DES SIGLES ET ABRÉVIATIONS

EDICA	Model Electronic Data Interchange Agreement de l'EDI Counsel of Australia
EDIFACT	Electronic Data Interchange Registration Authorities
F.	Federal Reporter
F. Supp.	Federal Supplement (U.S.)
G-7	Groupe des sept pays industrialisés
HTTP	Hypertext Transmission Protocol
ICP	Infrastructure à clé publique
ISO	Organisation internationale de normalisation ou International Standards Organization
J.E.	Jurisprudence Express
J.O.	Journal officiel de la République française
L.C.	Lois du Canada
L.Q.	Lois du Québec
L.R.Q.	Lois refondues du Québec
LCIA	London Court of International Arbitration
LUCE	Loi uniforme sur le commerce électronique
LUPE	Loi uniforme sur la preuve électronique
NZEDIA	New-Zealand Electronic Data Interchange Association
OCDE	Organisation de coopération et de développement économiques
P3P	Plateform for Privacy Preferences
PICS	Plateform for Internet Content Selection
PIIC	Comité de la Politique de l'Information, de l'Informatique et des Communications
Q.B .	Queen's Bench

LISTE DES SIGLES ET ABRÉVIATIONS

R. du B.	Revue du Barreau
R.C.S.	Recueil des arrêts de la Cour suprême
R.D.J.	Revue de droit judiciaire
R.D.U.S.	Revue de droit de l'Université de Sherbrooke
R.G.D.	Revue générale de droit
R.I.D.C.	Revue internationale de droit comparé
R.J.Q.	Recueil de jurisprudence du Québec
R.L.	Revue légale
R.R.Q.	Règlements refondus du Québec
TCP/IP	Transmission Control Protocol/Internet Protocol
UETA	Uniform Electronic Transactions Act
UNCID	Uniform Code of Conduct for Interchange of Data by Teletransmission
WORM	Write Once Read Memory

REMERCIEMENTS

Nous tenons à remercier notre directeur de recherche, Jacques Frémont, pour ses précieux commentaires et suggestions.

Ce mémoire n'aurait pu être complété sans le soutien continu de mon épouse, Nathalie Lévesque, et les sourires de notre fille Julia.

INTRODUCTION

Ce mémoire pose l'hypothèse et tente de démontrer que la mise en œuvre d'une convention relative à la preuve et à la conservation de documents électroniques (la « Convention[1] ») constitue un outil efficace de gestion de risques juridiques liés à l'utilisation de documents électroniques[2]. Il prend comme toile de fond les échanges commerciaux réalisés sur Internet entre partenaires intégrés œuvrant en amont des consommateurs et, dans ce cadre spécifique, traite de l'environnement juridique, de l'architecture, du contenu et de la mise en œuvre d'une Convention adaptée.

Le bien-fondé du recours proposé à une telle Convention ne s'établit pas dans l'abstrait. Il procède plutôt (1) du développement fulgurant du commerce électronique sur Internet, (2) des risques particuliers qui y sont associés et (3), des besoins de l'entreprise moderne pour des outils efficaces de gestion de ces risques. Il nous paraît donc utile de rappeler brièvement ces trois réalités du cyberespace en guise d'introduction.

Le développement du commerce électronique

Internet est un réseau décentralisé de réseaux d'ordinateurs regroupant des dizaines de millions d'ordinateurs et d'usagers répartis dans plus de 100 pays[3]. Conçu dans les années '60 à des fins militaires par le Département américain de la Défense, Internet s'est développé durant les années '80 grâce à l'implication de chercheurs universitaires friands d'échanges scientifiques outre-frontières, pour progressivement

---

1 Le mot « Convention » réfère à la fois à la convention relative à la preuve et à la conservation de documents électroniques discutée, de façon générale, dans ce mémoire, et à la Convention dont le contenu est abordé, de façon plus spécifique, à la section 2.3. Les recherches au soutien du bien fondé de cette hypothèse relative à la Convention ont été complétées en date du 1er avril 2000.

2 Le document électronique et ses attributs distinctifs sont définis à la section 1.1.2.

3 Pour une étude de la croissance passée et projetée d'Internet et du commerce électronique, consulter le Résumé de synthèse du Comité de la Politique de l'Information, de l'Informatique et des Communications (PIIC) de l'Organisation de Coopération et de Développement Économique (OCDE) intitulé *The Economic and Social Impacts of Electronic Commerce: Preliminary Findings and Research Agenda*, disponible au site http://www.oecd.org//subject/e_commerce/summary.htm préparé en vue de la Conférence ministérielle d'Ottawa des 7 au 9 octobre 1998 ainsi que les autres documents de consultation et de référence de l'OCDE concernant le commerce électronique disponibles au site http://www.oecd.org.//dist/sti/it/ec/news/ottawa.htm.

devenir ces dernières années une source de documentation, un moyen de communication et bientôt, un lieu de commerce incontournable[4].

Ce déploiement rapide de places d'affaires virtuelles affranchies des contraintes de distance et de frontières n'est pas fortuit ou aléatoire; il témoigne plutôt de la recherche et de l'importance des gains de productivité associés aux échanges numérisés, du maintien de coûts d'exploitation considérablement inférieurs à ceux d'autres moyens de communication et de l'avènement de solutions informatiques et cryptographiques assurant davantage la sécurité et la confidentialité des transactions électroniques[5]. Les observateurs de ce Nouveau Monde s'entendent pour dire que la valeur des échanges auxquels des dizaines de millions d'usagers seront partie d'ici l'an 2003 dépassera le trillion de dollars américains pour représenter plus de 50 % des ventes effectuées aux États-Unis par voie de cartes de crédit, et près de 15 % des ventes au détail réalisées dans sept pays de l'OCDE[6]. Ces projections, jugées conservatrices par l'OCDE[7], annoncent une croissance exponentielle du commerce électronique, du stade embryonnaire qui le caractérise encore[8] à un niveau d'activités planétaire susceptible d'affecter globalement les règles du commerce, les structures de l'économie, les marchés du travail et le comportement des consommateurs.

Cette croissance précède des réformes économiques prévisibles, parce qu'inévitables en matière de technologie, de commerce, de concurrence, de politique sociale et de droit. Déjà, ce besoin de réformes fait l'objet d'abondantes discussions[9] essentiellement centrées sur les transactions électroniques conclues directement entre entreprises, en amont des consommateurs. Ces échanges commerciaux représentent aujourd'hui plus de 80 % de tout le commerce électronique[10]. C'est d'ailleurs ce secteur

---

4 OCDE, *The Economic and Social Impacts of Electronic Commerce: Preliminary Findings and Research Agenda, op. cit.*, note 3, pp. 27 et ss.

5 *Id.*, pp. 9 à 25.

6 *Id.*, p. 9, Tableau 1. Les pays visés sont le Canada, la Finlande, la France, l'Allemagne, le Japon, les États-Unis et le Royaume-Uni.

7 *Id.*, p. 15.

8 *Id.*, Tableau 1. L'OCDE évalue les échanges commerciaux effectués sur Internet pour l'année 1996-1997 à quelque 26 milliards de dollars américains, soit 3 % des achats par cartes de crédit aux États-Unis et moins de 0,5 % du commerce de détail dans sept pays de l'OCDE. Dans le même sens, au Québec, voir les conclusions du rapport des sondeurs ScienceTech Communications, *Perspectives sur le commerce électronique et les Politiques publiques,* MIQ-98, réalisé en octobre 1998.

9 *Id.*, pp. 20 et ss.

10 *Id.*, p. 12.

commercial qui dictera véritablement, à court et à moyen terme, les paramètres de développement du commerce électronique[11], d'où l'intérêt de nous consacrer spécifiquement à ce secteur aux fins de notre mémoire.

L'importance de ce secteur commercial s'explique d'abord en termes économiques, puis à la lumière des attributs d'Internet qui en font encore un lieu virtuel à risques réels ou perçus pour le consommateur d'aujourd'hui. Au plan économique, nous savons qu'Internet s'impose naturellement comme un lieu d'échanges permettant de transiger rapidement et efficacement avec des partenaires commerciaux, particulièrement pour l'entreprise œuvrant dans la fourniture de biens intangibles[12] ou d'informations. Ces économies et gains d'efficacité se manifestent déjà de multiples façons[13]. Ils s'annoncent substantiels[14] et seront pleinement réalisés si l'entreprise œuvrant dans un environnement concurrentiel établit un lien de confiance suffisant avec ses partenaires pour s'intégrer avec eux par la voie de réseaux informatiques. Or, on constate déjà d'importants maillages et, dans certains cas, l'existence d'extranets dans le tissu industriel actuel, en dépit des risques d'élimination d'intermédiaires au commerce, des risques de comportements anticoncurrentiels liés à l'intégration recherchée ou encore, de rareté des ressources humaines qualifiées[15], autant de facteurs pourtant susceptibles de freiner l'adhésion des commerçants au nouveau paradigme du cyberespace.

---

11 L. HELM, « Business-to-business trade set to dominate Internet », *Financial Post*, 18 février 1999.

12 À titre illustratif, mentionnons les logiciels, les œuvres multimédia, les compilations sous forme de banques de données, le courtage de biens mobiliers, la fourniture de services de voyage ou de services financiers, ou encore les télécommunications radiophoniques et télévisuelles.

13 Pensons, notamment, au remplacement de places d'affaires multiples par un site virtuel unique, à la réduction des inventaires par l'adoption de systèmes de contrôle des inventaires dits « juste à temps », à l'augmentation du volume d'affaires, au placement et à la vérification informatisés des commandes, à la simplification du service à la clientèle ou après-vente à l'aide de systèmes intelligents, à la diminution des erreurs de traitement, à la réduction des coûts de distribution et de transport ou encore, à l'accessibilité à de nouveaux marchés.

14 OCDE, *The Economic and Social Impacts of Electronic Commerce: Preliminary Findings and Research Agenda, op. cit.*, note 3, p. 14, Tableau 2. Au seul titre des coûts de distribution, de récentes analyses économiques prévoient des économies cumulatives de 89 % dans les services bancaires, de 87 % dans les services aériens de réservation, de 97 % à 99 % dans la distribution des logiciels, de 67 % à 71 % dans les opérations de paiements commerciaux et de 50 % dans le traitement de produits d'assurance vie.

15 OCDE, *The Economic and Social Impacts of Electronic Commerce: Preliminary Findings and Research Agenda, op. cit.*, note 3. Au titre des risques d'élimination d'intermédiaires, le courtier en valeurs mobilières ou immobilières, l'agent de voyage et le courtier d'assurance sont à risque, compte tenu du développement actuel du commerce électronique et des produits communs qu'ils offrent. Les revendeurs traditionnels de livres seraient également menacés.

Par contre, pour le consommateur, la dématérialisation des échanges dans un environnement transactionnel ouvert et peu réglementé pour sa protection présente des risques suffisants pour tempérer son enthousiasme devant la nouveauté et retarder, sinon interdire sa participation au commerce électronique. Des questions d'intégrité des échanges, de sécurité des paiements, de fraude, d'atteinte à la vie privée ou encore d'applicabilité de régimes étatiques de protection sont abondamment traitées par les auteurs pour expliquer les réticences d'une majorité de consommateurs[16]. D'importants efforts sont déployés à cette enseigne et la presse spécialisée fait continuellement état du développement de solutions informatiques conçues pour réduire ces risques. Malgré tout, l'appréhension du consommateur demeure et est aussi réelle que le sont les gains recherchés par l'entreprise. Aussi, dans l'attente d'initiatives législatives ou technologiques susceptibles d'assurer aux consommateurs le niveau de confiance requis, le développement prédominant des échanges entre commerçants devrait se poursuivre et dominer le commerce électronique.

Les risques réels et anticipés

S'il ne peut y avoir de doute quant au développement du commerce électronique, sa pérennité ne sera assurée que par l'adhésion continue d'un nombre croissant d'entreprises responsables. Ces entreprises voudront nécessairement gérer adéquatement les risques nouveaux que pose ce commerce électronique sur Internet. Parmi ceux-ci figure en bonne place l'utilisation inévitable de documents électroniques[17]. Ces écrits[18] dénués de tout substrat matériel permanent constituent le fondement de ce commerce, s'agissant de la formation en ligne d'un contrat de valeur pour l'entreprise, de son

---

16 Consulter à ce sujet les conclusions de la Conférence ministérielle d'Ottawa du 7 au 9 octobre 1998, *Un Monde sans frontières : Concrétiser le potentiel du commerce électronique mondial*, OCDE, SG/EC (98) 14/Rev6, p. 4 et les Annexes 1 et 2, ainsi que les documents de référence qui sont identifiés au site http://www.oecd.org./dist/sti/it/ec/ news/ottawa.htm.

17 J.D. GREGORY, *Electronic Legal Records: Pretty Good Authentification*, disponible au site http//www.callacbd.ca/summit/. Voir également du même auteur *Solving Legal Issues in Electronic Commerce*, pp. 18 et ss., dont copie est disponible à l'adresse [redacted] et plus généralement, consulter les articles, comptes rendus de réunions et documents de réflexion disponibles au site de la Conférence pour l'harmonisation des lois au Canada en matière de documents électroniques, http://www.law.ualberta.ca/alri/ucl/findex.htm.

18 Le *Code civil du Québec* (« C.c.Q. ») traite de la preuve des inscriptions informatisées au Chapitre I du Titre Deuxième du *Livre de la preuve*, sous la rubrique intitulée « De l'écrit ». Voir à ce sujet la section 2.2.1.

exécution ou de son extinction libératoire par la voie d'un transfert de fonds électroniques[19].

Les risques juridiques liés à l'utilisation de ces documents électroniques sont bien réels dans un environnement dématérialisé et transnational[20]. D'abord, les déficiences inhérentes des infrastructures et des protocoles de communication qui constituent Internet, tout comme le fait fautif de tiers malveillants, peuvent considérablement miner la fiabilité du document numérique, au point d'interdire l'identification de l'expéditeur ou du destinataire, de détruire l'intégrité des données, de violer la confidentialité des échanges ou encore, de mener à la répudiation des messages de données. Le document électronique est alors dénué de toute utilité. À ces risques d'ordre technologique s'ajoutent ceux résultant du fait que le cyberespace demeure une terre en proie à la concurrence entre régimes normatifs de sources multiples[21]. Ce constat et une analyse même sommaire de nombreux textes législatifs font rapidement conclure aux juristes qu'il existe des barrières juridiques significatives à la reconnaissance et à l'utilisation de documents électroniques pour prouver l'existence d'actes ou de faits juridiques devant un tribunal judiciaire compétent[22]. S'ajoutent également d'innombrables zones d'incertitude découlant de l'interprétation de textes de lois non conçus pour connaître le commerce électronique. L'application des concepts traditionnels de signature, d'original et d'écrit[23], qui sont bien ancrés dans une tradition papier millénaire, donnent ouverture à des cas de figure révélateurs des difficultés perçues par l'entreprise comme des risques d'affaires associés à l'utilisation de documents électroniques.

---

19 La définition, la mise en service et la reconnaissance d'une monnaie électronique dans les milieux du commerce électronique nous paraissent indispensables. En effet, la question n'est plus de savoir si l'apparition d'une pareille unité de valeur est souhaitable ou prévisible. Le passage à une monnaie dématérialisée aura lieu, que cette évolution soit encadrée ou non. La technologie le permet et les marchés l'exigent. Le consommateur désire une monnaie sûre et discrète, moins lourde et coûteuse, aussi convertible qu'internationale, qui lui procure une plus grande liberté d'action et une autonomie compatible avec ses besoins spécifiques. Le commerçant recherche l'ouverture de nouveaux marchés ainsi qu'une réduction des coûts d'exploitation et de paiements associés à ces occasions d'affaires électroniques. Le défi véritable est de comprendre cette dynamique commerciale émergente et de produire la monnaie appropriée. L'utilisation de monnaies électroniques implique nécessairement le recours à des documents électroniques.

20 *Infra*, sections 1.1.1 et 1.2.1.

21 *Infra*, sections 1.1.1 et 1.2.1.

22 *Infra*, sections 1.2.1 et 2.2.1.

23 *Infra*, section 1.2. Selon un groupe de travail sur ces questions de droit dont les travaux sont disponibles au site http://www.canada.justice.gc.ca/commerce/ chapitre/chol, le terme « écrit » figurerait plus de 1 600 fois dans les lois du Canada et ne serait défini qu'à cinq reprises. Le terme « document » apparaîtrait plus de 2 000 fois et ne serait défini que dans une douzaine de cas. Les expressions « signature » et « signé » paraîtraient plus de 600 fois sans aucune définition statutaire.

Le besoin d'outils efficaces de gestion

La recherche par l'entreprise moderne d'outils de gestion des risques liés au commerce électronique constitue une troisième réalité du cyberespace. Celle-ci se manifeste de diverses façons. L'apparition d'autorités de certification témoigne éloquemment d'un besoin de sécurisation accrue des échanges électroniques[24]. Certains commerçants du cyberespace livrent bataille pour la libéralisation des exportations et l'utilisation de puissants algorithmes cryptographiques. D'autres prônent la création d'une monnaie électronique codée qui faciliterait des échanges sûrs et discrets dès l'étape transactionnelle. Cette dernière façon d'occulter les dangers d'un réseau ouvert ne fait pas l'unanimité en raison, notamment, des risques de prolifération de crimes économiques qui pourraient en découler[25].

Peu d'intervenants, s'il en est, contestent cependant l'utilité d'outils conçus pour doter l'entreprise d'une mémoire de ses transactions électroniques et de moyens fiables pour prouver leur existence, le moment venu, au moyen de documents électroniques fiables et recevables par le tribunal saisi d'un différend né dans le cyberespace[26]. En effet, l'entreprise doit pouvoir attester ses actes juridiques ainsi qu'établir légalement ses droits et défendre pleinement ses intérêts suivant des règles de preuve préétablies dans le cadre de poursuites judiciaires ou de procédures amiables de résolution de conflits[27]. Elle est également tenue à des obligations d'archivage d'origine statutaire[28] qu'elle se doit de remplir, sous peine de s'exposer à des sanctions civiles ou pénales. Si ce dernier motif d'archivage s'impose à l'entreprise par le seul effet de la loi, le premier motif renvoie au comportement prudent et diligent de la personne raisonnable guidée dans cette voie par des dirigeants mandataires soucieux de préserver la mémoire du temps.

---

24 Ayant pour fonction d'établir un lien entre une personne et une paire de clés asymétriques, l'autorité de certification constitue un véritable tiers de confiance dont les services d'identification, de vérification et de gestion des clés destinées à la signature numérique et au chiffrement créent un environnement plus sûr. Des autorités de certification œuvrent déjà aux États-Unis et ailleurs à la suite de l'adoption de lois-cadres. Voir, sur la certification, S. PARISIEN, P. TRUDEL, V. WATTIEZ-LAROSE, *L'identification et la certification dans le commerce électronique : droit, sécurité, audit et technologies*, Cowansville, Éd. Yvon Blais, 1996, pp. 117 et ss.

25 É. DUNBERRY, « Les monnaies électroniques : un cas d'espèce », (1997) 76 *R. du B.* 332.

26 *Infra*, section 1.2.2.

27 *Infra*, section 1.1.3.2.

28 *Infra*, section 1.1.3.3.

L'archivage électronique, que nous assimilerons aux activités de conservation utile de documents électroniques, est donc un moyen de gestion des risques liés à l'utilisation de documents électroniques, donc au commerce électronique, s'il permet d'atteindre les objectifs d'ordre historique, administratif et probatoire que vise l'entreprise dans le cours normal de ses affaires, tout en lui garantissant de rencontrer les obligations d'archivage d'origine statutaire qui s'imposent à elle. La décision de conserver ses documents sous forme électronique s'impose à l'entreprise aguerrie dans l'art de gérer et d'archiver des volumes sans cesse croissants de documents. Cependant, l'élaboration d'une Convention adaptée aux échanges électroniques entre partenaires commerciaux intégrés soulève cependant de nouvelles questions qui seront vraisemblablement au cœur des réflexions stratégiques d'entreprises maillées.

Au plan technologique, l'entreprise devra s'assurer que les produits informatiques, incluant particulièrement les logiciels utilisés pour la création, la conservation et la reproduction des inscriptions informatisées, présentent des garanties suffisantes de fiabilité. Elle devra opter pour la technologie appropriée en matière d'échanges de données, de signature électronique et de chiffrement, et définir les composantes informatiques du système d'archivage électronique en spécifiant, par devis, leurs caractéristiques technologiques propres. Elle voudra se doter de supports durables pour le stockage de données numériques et tiendra compte, dans ses choix, du développement prévisible des nouvelles technologies. Elle voudra jouir de lieux physiques et d'un environnement propice au fonctionnement de ses systèmes informatiques.

Pour le gestionnaire, il importera de déclarer haut et fort l'intention de l'entreprise de recourir à l'archivage électronique et d'en promouvoir l'utilisation auprès de ses partenaires commerciaux. L'entreprise devra procéder à la définition des rôles et des responsabilités et à la formation de responsables internes de l'archivage, après avoir jugé de l'opportunité de recourir aux services d'impartiteurs ou de certificateurs de confiance. Se poseront aussi les questions du retrait de documents non critiques en vue de leur conservation dans des aires d'entreposage à coûts réduits, de l'élimination de documents papier désuets ou de leurs copies multiples, du lieu d'archivage, ou encore de la destruction de documents au terme de leur vie utile ou de périodes de conservation appropriées. L'élaboration de politiques de conservation qui soient viables et susceptibles de réduire les coûts de l'archivage seront considérées, tout comme la recherche de gains de productivité par la simplification des fonctions de recherche et de communication des

données conservées. En outre, le gestionnaire voudra profiler la fonction d'archivage comme un outil de développement de nouveaux produits ou de pénétration de marchés jusque-là non rentables en permettant la compilation de banques de données à valeur ajoutée, particulièrement dans les cas de maillage entre partenaires commerciaux.

Pour le juriste, le défi que pose la conservation et la preuve du document électronique résulte avant tout de sa dématérialisation en un langage machine inintelligible pour l'humain. Cet état, qui le distingue radicalement du document papier sur lequel l'entreprise, les tribunaux et les autorités publiques s'appuient pour agir depuis des siècles, explique la difficulté d'assurer l'authentification, l'intégrité et la fiabilité du document électronique tout au long de son cycle de vie pour qu'il puisse servir les fins pour lesquelles il a été créé et conservé. Ces fins sont connues, comme le sont les règles de preuve édictées pour la reconnaissance judiciaire de documents originaux, écrits et signés même si, il faut en convenir, l'application de ces règles dans le cyberespace demeure floue, faute d'interprétations judiciaires définitives[29]. Certes, les tribunaux prendront acte du nouveau paradigme qu'impose le commerce électronique et feront preuve d'une volonté d'adaptation aux changements, en dépit d'exigences formalistes, favorisant autant que faire se peut une interprétation évolutive des textes. Ne le faisaient-ils pas déjà au Québec, avant même la réforme de janvier 1994[30]? Ceci dit, l'incertitude juridique est palpable malgré des initiatives législatives récentes[31] et le conseiller juridique d'entreprise vit une difficile période de transition. Dans l'attente d'amendements ponctuels ou d'une réforme plus globale, l'entreprise cherchera réconfort, comme elle le fait déjà par la clause compromissoire en matière de litiges, dans l'établissement d'un régime privé, connu et accepté parce que négocié à l'avance. Cette forme d'autoréglementation contractuelle n'est certes pas étrangère aux internautes qui choisissent fréquemment de se régir par des normes qui s'imposent en raison des

---

29 *Infra*, section 1.2.1.

30 Dans trois arrêts impliquant Hydro-Québec, la Cour du Québec a livré certains éléments utiles attestant de l'ouverture de nos tribunaux dans certaines circonstances et ce, avant même l'entrée en vigueur des dispositions du *Code civil du Québec* en matière de signature numérique. Dans *Hydro-Québec* c. *Malouf,* C.Q. Montréal 500-02-014314-89, 1993-12-17, la Cour jugeait recevables des feuilles informatisées pour faire la preuve de services rendus « sans qu'il soit nécessaire qu'une compagnie de l'envergure d'Hydro-Québec ait à assigner tous les employés qui, au cours de la période facturée, sont allés sur les lieux faire des relevés ». Et le juge de rajouter « de nos jours, les ordinateurs et l'informatique sont d'usage courant dans le commerce ». La Cour a jugé dans le même sens dans les affaires *Hydro-Québec* c. *Mondor*, C.P. Joliette 705-02-000209-841, 1986-02-06 et *Hydro-Québec* c. *Benedek* [1995] R.L. 436 (C.Q.M.).

31 *Infra*, section 2.2.2.

avantages qu'elles procurent, ou encore par nécessité. Internet n'est-il pas d'ailleurs le résultat de normes et de protocoles emportant l'adhésion volontaire des usagers?

Ce mémoire, nous l'avions annoncé d'entrée de jeu, entend démontrer que la mise en œuvre de la Convention relative à la preuve et à la conservation de documents électroniques constitue un outil efficace de gestion de risques liés à l'utilisation de documents électroniques sur Internet. À cette fin, nous traiterons d'abord du commerce électronique et ses risques propres (1.1.1), du document électronique et ses attributs distinctifs (1.1.2) et de la finalité de l'archivage électronique (1.1.3). Preuve sera ensuite faite que la Convention est licite en droit québécois (1.2.2.1), qu'elle constitue un outil conventionnel particulièrement bien adapté à l'environnement a-national du cyberespace (1.2.2.2) et qu'elle peut être négociée pour répondre spécifiquement aux attentes commerciales d'entreprises maillées (1.2.2.3) tout en palliant, par l'établissement d'équivalences fonctionnelles, à l'incertitude et au déphasage qui existe entre, d'une part, les règles de droit et les solutions jurisprudentielles pensées pour un environnement papier et, d'autre part, la réalité et les risques propres au commerce électronique (1.2.1).

Nous procéderons ensuite à la définition de principes directeurs dans l'architecture de la Convention, tenant compte des objectifs stratégiques et des priorités d'affaires de l'entreprise ainsi que des obstacles juridiques que doit franchir la Convention pour atteindre sa finalité (2.1). Afin d'assurer l'arrimage souhaitable entre l'architecture proposée et les règles de droit actuelles ou prévisibles en matière de conservation et de preuve de documents électroniques, nous serons guidés par les dispositions pertinentes du *Code civil du Québec* (2.2.1), de même que par des initiatives législatives phares au Canada et ailleurs en matière d'archivage et de preuve électronique (2.2.2). Nous tiendrons compte également des normes et des pratiques de l'industrie en ces matières (2.2.3). Ce faisant, nous pensons favoriser la reconnaissance et l'adhésion *de facto* à l'architecture proposée.

Nous aborderons enfin de façon concrète certains aspects du contenu et de la mise en œuvre de la Convention (2.3), avant de conclure.

1. LA RAISON D'ÊTRE DE LA CONVENTION RELATIVE À LA PREUVE ET À LA CONSERVATION DE DOCUMENTS ÉLECTRONIQUES D'ENTREPRISE

1.1 LE COMMERCE, LE DOCUMENT ET L'ARCHIVAGE ÉLECTRONIQUES

Il importe de cerner ce qui distingue le commerce, le document et l'archivage électroniques des réalités équivalentes que connaît l'entreprise dans son environnement commercial traditionnel. Ces distinctions sont à l'origine des risques nouveaux que des partenaires commerciaux voudront gérer par Convention.

1.1.1 Le commerce électronique et ses risques d'affaires propres

On ne peut identifier les risques d'affaires propres au commerce électronique sans comprendre ce qu'est Internet et son mode de fonctionnement.

Chaque communication sur Internet implique un site expéditeur, un site destinataire, des ordinateurs serveurs, des routeurs et une infrastructure de communication par fils, par câbles ou par d'autres technologies. L'information circule sous une forme numérisée grâce au développement de protocoles de communication entre ordinateurs, principalement désignés par l'acronyme TCP/IP. Les données transmises sont hachées en millions de datagrammes ou *packets* contenant une fraction du message, son adresse ultime et la séquence d'identification et de réassemblage du message. Ces datagrammes circulent de sites en sites, à l'échelle planétaire, empruntant des chemins défiant toute logique géographique. La gestion optimale de ces datagrammes est assurée par de puissants ordinateurs routeurs constituant de véritables gares de triage électronique opérant à la vitesse de la lumière.

Évidemment, des intermédiaires se situent entre l'expéditeur et le destinataire d'une communication et assurent des fonctions de transit dont la nature varie significativement. Les principaux intermédiaires sont les transporteurs publics[32] et les

---

32 Ces transporteurs sont généralement des sociétés d'envergure nationale ou internationale œuvrant dans les domaines de la transmission de données numériques par fils, radio, procédés visuels ou optiques ou d'autres systèmes électromagnétiques. Référence est ici faite, notamment, aux compagnies de téléphone, de câbles ou de communication par satellite. Consulter également, quant aux principaux intermédiaires, D. JOHNSTON, D. JOHNSTON, S. HANDA, *Undertaking the Information Highway*, Toronto, Stoddart Publishing Co. Ltd., 1995, ch. 3, pp. 93 et ss.

fournisseurs d'accès et de services[33] auxquels se joignent les opérateurs de babillards électroniques ou de groupes de nouvelles *UseNet*[34] et les opérateurs de listes de distribution[35]. Tous ces intermédiaires ont en commun qu'ils facilitent la diffusion de documents électroniques par Internet. Ils se distinguent par leur degré de participation et d'engagement réel dans la diffusion. Ce degré se mesure en première ligne, selon la jurisprudence, suivant le niveau de connaissances et de contrôle dont jouit l'intermédiaire en relation avec le contenu de la communication. Le *World Wide Web* célèbre cette année son huitième anniversaire depuis l'avènement, en 1992, du désormais célèbre protocole HTTP[36]. Le Web connaîtrait son troisième âge, soit celui du maillage entre partenaires commerciaux sous la forme d'extranets. Or, cette créature que constitue Internet demeure jeune, certes, mais en constante progression vers un niveau d'organisation plus élevé. Cette évolution n'altère en rien cependant la dominance depuis l'origine d'une toile ouverte constituée de personnes de tout acabit en relation continue.

L'architecture d'Internet et son mode de fonctionnement constituent donc un environnement décentralisé, dématérialisé et transnational assujetti à des régimes normatifs concurrents. Il en résulte pour l'entreprise des risques d'affaires nouveaux.

La dématérialisation des échanges peut faire naître des problèmes d'intégrité et de fiabilité des données. En effet, tout informaticien confirmera la facilité avec laquelle un document numérisé peut être copié, altéré ou dénaturé, par erreur ou par fraude, au risque de ceux qui se fient à ces données ou qui peuvent être tenus responsables de leur inexactitude.

Certaines manifestations de ces risques sont particulièrement préoccupantes à l'étape de la formation de contrats commerciaux en ligne. Un premier cas concerne

---

33 Ces fournisseurs sont des entreprises commerciales disposant de droits d'accès au réseau Internet. Il existe deux types de fournisseurs : les fournisseurs de « connectivité » qui agissent essentiellement comme point de transit, sans offrir d'autres services que la connexion au réseau Internet. Les fournisseurs d'accès ou de services à valeur ajoutée exploitent généralement d'anciens réseaux commerciaux privés et centralisés désormais liés à Internet et offrent des services de communication, d'information et de recherche à leurs abonnés, suivant une tarification variable.

34 Ces opérateurs sont des sociétés commerciales de gestion d'échanges publics et collectifs articulés en hiérarchie autour de sujets particuliers constituant le point focal des échanges. Ces groupes se comptent par milliers et favorisent la création de communautés virtuelles d'intérêt.

35 Ces intermédiaires permettent aux utilisateurs d'Internet de participer à des discussions, de s'abonner à des systèmes d'échanges d'informations et de former des groupes d'intérêt dotés de moyens d'échanges collectifs. Ces listes sont administrées à l'aide de programmes de gestion de messagerie électronique capables de prendre en charge les abonnements et la circulation des messages.

36 Il s'agit de l'acronyme désigné pour *Hypertext Transmission Protocol.*

l'usurpation d'identité résultant de l'appropriation non autorisée d'une marque personnelle.[37]. L'usurpation de codes d'accès, de clés privées ou d'autres identifiants numériques engendre des problèmes évidents résultant de l'incapacité d'identifier son cocontractant. Cette mascarade[38] est facilitée par Internet en raison d'un culte de l'anonymat qui perdure[39]. De la même manière, le risque de répudiation existe lorsque l'expéditeur nie l'émission d'un message à la suite d'une erreur, d'un acte de piratage ou d'un refus d'endosser la paternité d'un message[40]. Pour le vendeur en ligne, la difficulté sera bien réelle au moment de la livraison d'un bien! Une troisième situation, tout aussi préjudiciable, naît lorsque l'altération accidentelle ou malveillante des données fera conclure à un vice de consentement et à la nullité du contrat électronique. En effet, la modification non autorisée d'un élément déterminant de la transaction électronique fait entrevoir d'innombrables situations juridiques où ce qui aura été accepté différera de ce qui était offert, au détriment des parties contractantes ou à l'instigation de l'une d'elles. Enfin, la dématérialisation accroît le risque de bris de confidentialité et de perte du caractère secret de données commerciales. Dans l'économie du savoir, l'information est un objet de commerce de valeur et procure à l'entreprise un avantage concurrentiel qu'elle doit protéger. Le développement continue de puissants algorithmes cryptographiques et la pénétration de solutions technologiques pour sécuriser les transactions témoignent éloquemment de la valeur de l'information et de risques associés à l'utilisation d'Internet. S'il est vrai que l'entreprise connaît déjà certains de ces risques dans le monde tangible, elle comprend qu'ils sont aggravés dans le cyberespace où toutes les composantes d'une transaction, qu'il s'agisse de l'offre, de l'acceptation, de la

---

37 *Infra*, section 1.2.1. Au Québec, on se référera à l'article 2827 C.c.Q.

38 S. PARISIEN, P. TRUDEL, V. WATTIEZ-LAROSE, *op. cit.*, note 24, p. 61.

39 L'anonymat entourant l'auteur d'une communication s'obtient grâce à l'intervention d'intermédiaires ou *remailers* dont la tâche est de purger le message des données l'associant à l'expéditeur, puis de l'expédier au destinataire choisi. L'identité de l'expéditeur peut cependant être retracée et l'anonymat violé si l'intermédiaire en question conserve l'information acquise et la révèle de plein gré ou lorsque contraint par un tribunal. On parlera alors d'un message anonyme qui peut être retracé ou de *traceable anonymity*. Ce risque d'identification peut être réduit par l'utilisation d'une chaîne d'intermédiaires et de la cryptographie à clé publique. Dans un tel système, aucun des intermédiaires ne peut lire le message parce que codé en série par l'utilisation de la clé de chaque intermédiaire dans la chaîne. Il faut enfin distinguer l'auteur anonyme de celui qui utilise un pseudonyme menant à la création d'une personnalité artificielle, dite digitale, dotée de sa propre signature électronique. Pour une analyse détaillée de l'utilisation de pseudonymes, voir F. FROOMKIN, *Flood Control on the Information Ocean, Living With Anonymity Digital Cash and Disputed Database*, disponible au site http://www.digicash.com.

40 S. PARISIEN, P. TRUDEL, V. WATTIEZ-LAROSE, *op. cit.*, note 24, p. 62.

livraison d'un bien intangible ou du paiement sont réduites à un simple échange d'informations indifférenciées.

La transnationalité d'Internet engendre d'autres risques associés au commerce électronique. Cette transnationalité résulte de ce qui est à l'origine d'Internet, soit l'existence d'interconnexions sans cesse changeantes rendues possibles grâce à l'infrastructure des systèmes de communication actuels. Internet apparaît comme une véritable résultante, une toile virtuelle sans point d'origine qui évolue d'heure en heure à l'échelle de la planète, dans un parfait désintéressement des contraintes géographiques et géopolitiques. Or, dans le cadre d'un litige, l'entreprise évalue les risques d'un jugement défavorable en tenant compte des faits pertinents, du droit substantif et des attributs du forum compétent. Si les faits demeurent, le choix du droit substantif applicable à une situation juridique et du forum compétent pour en disposer, s'ils n'ont pas été stipulés par contrat, obéit à des règles de conflits de lois et de juridictions relevant du droit international privé, lesquelles laissent place à l'interprétation. Ces règles de droit sont applicables aux situations juridiques établies sur Internet[41], même si leur application concrète pose des difficultés, et forcent l'entreprise à considérer l'effet d'un phénomène dit de *forum shopping* par la partie lésée. La question revêt un intérêt véritable lorsque l'entreprise maintient des places d'affaires et des actifs saisissables dans plusieurs juridictions. Ainsi, il est logique de croire qu'une partie lésée dotée de moyens suffisants voudra évaluer les chances de gains pouvant résulter de procédures judiciaires contre l'entreprise dans celle des différentes juridictions pouvant se saisir du différend qui lui procurera les meilleures chances de succès. Il suffit de rappeler les précédents américains en matière d'octroi de dommages pour juger de la pertinence et de la difficulté pour l'entreprise d'évaluer le risque global auquel elle s'expose dans un nouveau territoire d'affaires virtuel.

Ce risque n'est réel que si plusieurs juridictions peuvent se dire compétentes pour connaître d'une affaire litigieuse. L'étude des facteurs de rattachement traditionnels tels le domicile, la résidence, le lieu de la cause d'action, du fait dommageable ou de la conclusion d'un contrat dans le cadre d'un monde virtuel décentralisé, souvent sans point d'ancrage sinon l'arbitraire du lieu choisi pour l'implantation d'un serveur, permet d'envisager une définition élargie des règles d'attribution concernant les litiges nés dans le cyberespace et l'émergence de nouveaux facteurs de rattachement. Le concept de

---

41 *Infra*, note 45.

réseau[42] à l'intérieur duquel un fait dommageable se produit presque instantanément dans plusieurs territoires géographiques, par l'intermédiaire de serveurs interconnectés, illustre bien l'accroissement prévisible du nombre de juridictions compétentes ou qui se diront compétentes pour connaître d'une affaire. De nombreuses décisions de tribunaux civils font déjà présager de débordements juridictionnels[43].

Internet est toujours en proie à la concurrence que se livrent des régimes normatifs de sources multiples, en dépit d'efforts d'harmonisation à l'échelle internationale dans différents secteurs d'activités économiques[44]. Le droit y est incertain[45] et ces incertitudes posent un risque d'affaires pour le gestionnaire peu friand d'imprévision ou d'indétermination dans les règles de droit qui le régissent. L'origine et les manifestations de ces risques juridiques sont abordées en détail plus loin[46], s'agissant d'un point focal dans l'élaboration de la Convention.

Enfin, nous ne pourrions clore cette section sans rappeler qu'Internet est une toile formée d'ordinateurs et de lignes de communication bien tangibles animés par des logiciels. Ce réseau demeure en tout temps vulnérable devant des bris d'équipements, des pannes de logiciels, des erreurs humaines, des catastrophes naturelles et des bogues informatiques comme nous l'a rappelé d'ailleurs à grands frais le passage à l'an 2000.

---

42 L'application des règles du droit international privé nous renvoie à certaines réalités informatiques que les tribunaux devront appréhender. Référence peut être faite à l'antémémorisation, aux signatures électroniques, au codage des informations, à la détermination du lieu de formation d'un contrat, au concept d'adresse électronique aux fins de la détermination du lieu de l'acte juridique ou encore, aux techniques de stockage de données sous forme numérique aux fins de la localisation de biens meubles pouvant constituer un actif saisissable. Nos tribunaux devront comprendre que l'espace cybernétique n'existe pas; seules existent des interconnexions entre ordinateurs et réseaux d'ordinateurs faisant d'Internet la résultante d'interconnexions où toute référence purement spatiale est susceptible d'induire en erreur.

43 *Zippo Mfg* v. *Zippo Dot Com Inc.*, 952 F Supp. 1119, 1124 (W.D. Pa 1997); *CF Heros Inc.* v. *Heroes Found*, 958 F Supp. 1 (D.D.C. 1996); *Hasbro Inc.* v. *Clue Computing Inc.*, 994 F Supp. 34, 38 (D. Mass 1997); *Braintech, Inc.* c. *John C. Kostiuck* [1999] B.C.J. n° 622; au Québec, consulter *Investors Group Inc.* c. *Hudson*, J.E. 99-499 (C.S.). Consulter également A. GAHTAN, M. KRATZ, F. MANN, *Internet Law, a practical guide for legal and business professionals,* Toronto, Carswell, 1998, ch. 10, pp. 319-341.

44 P. TRUDEL, F. ABRAN, K. BENYEKHLEF, S. HEIN, *Le droit du cyberespace*, Faculté de droit de l'Université de Montréal, Centre de recherche en droit public, Montréal, Éd. Thémis, 1997, chapitre 7, Les politiques nationales, pp. 7.1 et ss.

45 Pour une analyse des incertitudes du droit et de leur impact sur l'activité économique en général et le cyberespace en particulier, consulter les textes d'auteurs réunis sur le sujet, sous la direction de E. MACKAAY, dans *Les incertitudes du droit*, Faculté de droit de l'Université de Montréal, Centre de recherche en droit public, Montréal, Éd. Thémis, 1999.

46 *Infra*, section 1.2.1.

Les promoteurs d'Internet minimisent l'importance de tels bris en raison du niveau élevé de redondance intégrée au réseau et du nombre presque illimité de configurations possibles pour acheminer les datagrammes. Ils doivent néanmoins admettre l'existence de bris, d'erreurs et de retards dans les communications et de territoires non accessibles. Ces bris peuvent provoquer des interruptions d'affaires, des pertes de données, des retards de livraison et, plus généralement, des inexécutions contractuelles susceptibles d'engager la responsabilité du commerçant dans le cyberespace. S'agissant d'un risque d'affaires, l'entreprise voudra le gérer au mieux, y compris par la négociation de clauses d'exclusion ou de limitation de responsabilité, de conventions d'indemnité, de clauses de force majeure et par d'autres schémas d'allocation des risques.

1.1.2 Le document électronique et ses attributs distinctifs

Le document électronique est au cœur de la Convention. Il importe donc de le définir et d'identifier ses attributs distinctifs. Le document électronique est d'abord et avant tout un document; il sert donc à instruire[47]. Il constitue un ensemble d'informations structurées fixées sur un support pour témoigner d'une intention de communication et qui possèdent une valeur pour l'entreprise à l'égard de ses processus de travail[48]. Cette valeur peut être d'ordre historique, légal, administratif, informatif ou technique[49]. Le document est qualifié d'électronique en raison du support et des systèmes informatiques dont il dépend. Le Conseil international des archives nous le rappelait dans son guide d'archivage publié en février 1997 :

> « *Un document est de l'information consignée, créée ou reçue au moment d'amorcer, d'effectuer ou de compléter les activités menées par une institution ou une personne et qui présente un contenu, un contexte et une structure permettant de prouver l'existence de ces activités, indépendamment de la forme ou du support.[...]*
>
> *Les documents électroniques ont une caractéristique distincte : étant consigné sur un support informatique et en symboles (chiffres*

---

47 Du latin *documentum, doceo* : enseigner, instruire, faire valoir. Dictionnaire latin Hachette.

48 Glossaire de l'ingénierie documentaire, Rapport synthèse du Chantier en ingénierie documentaire intitulé *La gestion des documents adaptés à l'inforoute gouvernementale,* janvier 1999.

49 *Infra,* section 1.1.3.

> *binaires), leur contenu ne peut être lu et compris qu'au moyen d'un ordinateur ou d'une technologie assimilée.* »[50]

Plus récemment, le législateur fédéral proposait une définition du document électronique dans le *projet de loi C-6* (le « *Projet de loi C-6* ») sur la protection des renseignements personnels et les documents électroniques[51], une définition qui n'est d'ailleurs pas sans rappeler celle déjà offerte par la Conférence pour l'harmonisation des lois au Canada[52] (« CHLC ») dans sa *Loi uniforme sur la preuve électronique*[53]. Ainsi, le document électronique comprend « *l'ensemble de données enregistrées ou mises en mémoire sur quelque support que ce soit par un système informatique ou un dispositif semblable et qui peuvent être lues ou perçues par une personne ou par un tel système ou dispositif. Sont également visés tout affichage et toute sortie imprimée ou autre de ces données* »[54]. Le mot « donnée » est défini largement pour inclure « *toute forme de représentation d'informations ou de notions* »[55].

Ces textes nous sont utiles pour saisir les attributs du document électronique qui le distingue du document sur support papier. Ceux-ci sont au nombre de quatre. Le document électronique se distingue d'abord par le fait que les données qu'il contient sont consignées sur un support informatique sous la forme de symboles binaires qui ne peuvent être lus et compris qu'au moyen d'équipements et de technologies informatiques. À titre d'exemple, lorsqu'un document est numérisé, il passe d'une facture compréhensible par l'homme à un langage machine illisible.

> « *Le passage du document sous forme papier à sa version électronique découle de la technologie du « numériseur » ou du « balayeur optique », lequel permet de transformer un document*

---

50 Conseil international des archives, *Guide for managing electronic records from an archival perspective*, février 1997, p. 11.

51 *Projet de loi C-6* (à l'origine C-54), 1ère session, 36e législature, 46-47 Élizabeth II, 1997-1998, déposé le 1er octobre 1998 et réimprimé le 12 avril 1999.

52 La définition de document électronique proposée par la CHLC dans sa *Loi uniforme sur la preuve électronique* se lit comme suit : *« Electronic record means data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data, other than a printout referred in Sub-section 4(2) ».* Beaucoup d'autres définitions existent ou sont proposées dans le corpus législatif vu à la section 2.2.2. Voir également les documents de consultation et les comptes rendus de réunions annuelles de la CHLC en matière de preuve électronique disponibles au site http://www.law.ualberta.ca/alri/ulc.

53 *Infra*, section 2.2.2.

54 *Projet de loi C-6*, art. 31(1).

55 *Ibid.*

> *imprimé en fichier binaire et de l'introduire ainsi dans l'ordinateur. Le principe est succinctement le suivant : en cours de numérisation, le balayeur émet une lumière qui réfléchit dans le document à être numérisé, cette réflexion étant alors convertie par le balayeur en fichier binaire, c'est à dire en 0 et en 1, selon la brillance obtenue de chacun des pixels captés.*
>
> *Au moment de cette transformation en fichier binaire, l'image est entreposée sur le disque magnétique de l'ordinateur tout en faisant l'objet d'une indexation automatique par le logiciel de gestion électronique intégré à l'appareil de numérisation, lequel générera des références essentielles au document permettant son repérage immédiat dans l'avenir.* » [56]

Le document numérisé constitue ainsi un fichier électronique à l'image du document original, stocké sur un support magnétique à densité et à durée de vie variables[57]. L'accès au document, son retrait et sa lecture commandent la « traduction » inverse, d'un langage machine à un langage intelligible, d'où l'importance de préserver la fiabilité du document reproduit sous forme numérique tout au long de son cycle de vie. Le maintien de la fiabilité du document créé dès l'origine sous forme numérique pose le même défi[58].

Deuxièmement, les données informatisées sont dissociées de tout substrat matériel permanent. Contrairement au document sur support papier, dans lequel l'information et le papier se fusionnent de façon permanente lors de l'impression, les inscriptions informatisées migrent à la vitesse de la lumière d'un support à l'autre. Cette existence indépendante dont jouit l'information dématérialisée accroît les risques d'altérations involontaires ou malveillantes et force la mise en œuvre de mécanismes spécifiques pour garantir la fiabilité du contenu du document électronique.

Troisièmement, les structures logiques d'un document sur support papier sont apparentes et font partie intégrante de celui-ci, au point de contribuer à son authentification. Le document électronique veut s'affranchir d'une structure permanente. Il se définit plutôt en fonction de champs, de conventions de programmation et de

---

56 B. TROTTIER, « L'archivage des documents sous forme électronique : aspects pratiques et légaux », *Congrès annuel du Barreau du Québec*, 1997, p. 181.

57 On pense ici, notamment, au CDROM (*Compact Disk – Read Only Memory*) et, de façon plus temporaire à l'utilisation de WORM (*Write Once Read Many*) utilisés selon certaines normes précises, dont la norme ISO concernant l'inscription et le formatage des fichiers.

58 On peut imaginer d'autres catégories de documents électroniques, dont ceux faisant l'objet d'EDI suivant une grammaire définie ou encore les images numérisées de documents sur support papier.

langages évolués suivant des structures conçues pour extraire des données organisées à l'intérieur d'un environnement codé. Pour préserver le document numérisé, il faut nécessairement préserver les éléments informationnels requis pour recréer la structure d'origine, qu'il s'agisse du balisage ou de marquage, par exemple[59].

Le quatrième élément distinctif concerne l'existence de données secondaires connues sous le vocable de métadonnées du fait qu'elles sont nécessaires à la définition du contexte ou de la structure du document électronique, au-delà de son contenu. Elles procurent des renseignements relatifs aux données d'un document électronique qui permettent leur utilisation pertinente sans pour autant faire partie intégrante de ce document, même si elles en sont extraites en partie. Les métadonnées lient le document à l'activité dont il émane et l'environnement qui l'a vu naître. Elles servent à l'identification, la description et l'administration du document électronique[60]. En guise d'exemple, pensons aux métadonnées qui « *permettent de déterminer l'origine et la destination du message de données, ainsi que les indications de date et d'heure de l'envoi et de la réception* »[61]. En effet, la difficulté d'identifier un document électronique en fonction de sa provenance, particulièrement lorsqu'il naît dénué de tout *alter ego* papier, est réelle et exacerbée par le passage du temps ou l'intégration de données d'origines diverses dans des compilations matricielles sous forme de banques de données. Cette fusion rendue possible par la dématérialisation pose le risque de ne pouvoir inverser le flux des données et recréer l'un des documents d'origine. La fragilité des supports magnétiques actuels[62] rend inévitable la migration périodique des inscriptions. De là l'importance des métadonnées pour assurer l'intégrité des documents électroniques et leur traçabilité par rapport aux documents d'origine, au-delà de toute conversion de langage, migration d'aires de stockage ou développement informatique.

---

59 Le balisage sert à insérer des signes conventionnels dans un document afin de pouvoir délimiter des segments et en effectuer le marquage, soit des indications du contenu compris entre les balises d'un document structuré au moyen d'identifiants génériques et d'identifiants convenus par domaines. Rapport de synthèse du Chantier en ingénierie documentaire intitulé *La gestion des documents adaptés à l'inforoute gouvernementale*, *op. cit.*, note 48.

60 Pour une étude d'application de profils de métadonnées, consulter le Rapport synthèse du Chantier en ingénierie documentaire intitulé *La gestion des documents adaptés à l'inforoute gouvernementale*, *op. cit.*, note 48, c. 2, pp. 6-14.

61 Art. 10.1(c) de la *Loi type*, *infra*, section 2.2.2.1.

62 On évalue présentement à 50 ans la durée de vie utile d'un CDROM à surface d'argent et à 75 ans celle d'un disque dur à couche d'or.

Ces distinctions fondamentales découlent toutes, à des degrés variables, de la dématérialisation du document. Nous verrons que cette perte de substrat explique en bonne partie les risques et la problématique juridiques liés à l'utilisation et à l'archivage des documents électroniques[63].

1.1.3 La conservation du document électronique et sa finalité

La finalité de la conservation d'un document électronique est tributaire de sa valeur pour l'entreprise. Des auteurs[64] rappellent que cette valeur peut être d'ordre historique, légal, administratif, informatif ou technique. Ainsi, si le document sert à instruire, son archivage permet à l'entreprise de prouver qu'elle existe, qu'elle a un passé et qu'elle commerce, que l'entreprise désire cette mémoire en raison de sa valeur ou qu'on la lui impose pour se conformer à ses obligations légales.

1.1.3.1 Une question d'existence, de saine gestion et de mémoire pour l'entreprise

La compagnie est une personne morale qui aspire à vivre éternellement, du moins est-ce là l'opinion de bien des fondateurs d'entreprise à l'aube de sa constitution. Or, justement, la compagnie « *est une créature artificielle, créée sur papier ... [qui] se manifeste par ses écrits [car] c'est le seul moyen dont elle dispose pour se manifester dans un monde réel, palpable* »[65]. Il s'agit d'une personne dont la mémoire est aussi éphémère que ceux par qui elle s'exprime. Seules ses archives connaissent son passé, constituant de véritables banques de données renfermant les renseignements nécessaires à la conduite de ses affaires présentes et futures. Ces données, dont la valeur administrative s'estompe avec le passage du temps, gagnent une valeur historique du fait qu'elles permettent à l'entreprise de reconstituer fidèlement la réalité de son passé. L'archivage sert à constituer et à préserver la mémoire de l'entreprise et cette mémoire doit être donc conçue, structurée et enrichie de façon à garantir l'atteinte des objectifs d'affaires à des coûts raisonnables. Cela est encore plus évident à l'égard d'entreprises virtuelles œuvrant dans le cyberespace.

---

63 *Infra*, sections 1.2.1 et 2.1.

64 S. PARISIEN, P. TRUDEL, V. WATTIEZ-LAROSE, *La conservation des documents électroniques : Les phases post-transactionnelles du commerce électronique*, Faculté de droit de l'Université de Montréal, Centre de recherche en droit public, Montréal, 14 décembre 1998, pp. 26-34.

65 M. MARTEL, P. MARTEL, *La compagnie au Québec : les aspects juridiques*, vol. 1, Montréal, Wilson & Lafleur Ltée, 1996, p. 210.

1.1.3.2 La conservation à des fins probatoires

La décision de conserver un document sur support électronique, comme sur support papier, s'explique en partie par la possibilité qu'il puisse être requis pour prouver l'existence d'actes juridiques ou de faits matériels, entre autres dans le cadre de procédures de résolution de conflits. L'institution de procédures judiciaires, ou l'expectative raisonnable de l'existence de telles procédures, peut même faire naître, suivant les circonstances, une obligation de préserver toute preuve pertinente. La destruction volontaire d'éléments de preuve documentaire peut, par présomption ou inférence négative, nuire significativement aux intérêts judiciaires d'une partie, ou être sanctionnée par la Cour[66]. Or, la pertinence d'un document n'est pas le seul critère; encore faut-il que le document soit admissible en preuve au moment précis où il est offert ou exigé conformément aux règles de preuve applicables.

En cette matière, l'archivage électronique soulève d'emblée deux questions : (1) celle de l'admissibilité d'inscriptions informatisées *per se* et (2), celle du maintien de cet attribut tout au long du cycle de vie du document électronique, incluant la période d'archivage. La perte de cet attribut en raison de pratiques ou de systèmes d'archivage déficients entraînerait pour l'entreprise la perte d'un moyen de preuve utile et minerait inévitablement la fiabilité de sa mémoire documentaire.

Des auteurs québécois[67] s'entendent pour traiter de l'admissibilité d'inscriptions informatisées sur la base de la distinction faite entre l'acte juridique et le fait matériel. Par acte juridique, nous entendons « *toute manifestation de volonté individuelle qui est destinée à créer, modifier ou éteindre un droit* »[68] alors que le fait matériel vise « *tout événement autre qu'un acte de volonté impliquant une obligation ou*

---

66 A. GATHAN, *Electronic Evidence*, Toronto, Carswell, 1999, pp. 122-132.

67 P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *La preuve et la signature dans l'échange de documents informatisés au Québec*, Montréal, Les Publications du Québec, 1993; F. CHAMPIGNY, « L'inscription informatisée en droit de la preuve québécois », dans *Développements récents en preuve et procédure civile (1996)*, Cowansville, Éd. Y. Blais, 1996, pp. 1 et ss.; J. C. ROYER, *La preuve civile*, 2e éd., Cowansville, Éd. Y. Blais, 1995, no 402 et suiv.; C. FABIEN, *La communicatique et le droit de la preuve,* Actes du Colloque conjoint des Facultés de droit de l'Université de Poitiers et l'Université de Montréal, 1990, p. 159; L. DUCHARME, *Précis de la preuve*, 5e éd., Montréal, Wilson & Lafleur Ltée, 1996, nos 463 et suiv.; D. MASSE, *La preuve des inscriptions informatisées*, Montréal, 1997, disponible au site http://www.chait-amyot.ca/; G. LEFEBVRE, « La preuve en matière d'échange de documents informatisés », (1995) 74 *R. du B.* 619.

68 J.-L. BAUDOUIN, *Les Obligations,* 5e éd., Cowansville, Éd. Yvon Blais, 1998, p. 40.

une libération, ou autrement dit, tout événement autre qu'un acte juridique »[69]. Cette approche sur deux axes s'impose naturellement à la lecture des dispositions du *Code civil du Québec* consacrées à la preuve des inscriptions informatisées et dont le champ d'application est circonscrit aux seuls actes juridiques[70]. Au cœur de ces dispositions se trouve l'article 2837 C.c.Q., qui se lit comme suit :

> *« Art. 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. »*

Ainsi, avec l'entrée en vigueur du *Code civil du Québec* en janvier 1994, la preuve des données d'un acte juridique inscrites sur support informatique s'est vue consacrer pour la première fois en droit québécois une section propre intitulée *« Des inscriptions informatisées »*. Cette section comporte trois articles de droit nouveau, dont l'article 2837 C.c.Q., formant un tout ayant notamment pour objet, selon le législateur, de couvrir « *les contrats conclus à distance et les contrats verbaux, dont les données sont directement inscrites sur support informatique ... des contrats d'entreprise ou certains contrats de consommation qui interviennent par l'utilisation de guichets automatiques* ... »[71]. En revanche, le régime de preuve applicable aux faits matériels est contenu dans les règles générales énoncées aux articles 2803 et suivants du *Code civil du Québec.* Cette distinction existant entre l'acte juridique et le fait matériel est d'importance puisqu'elle dicte l'application de règles différentes au plan de la preuve de situations ou d'effets juridiques. L'application de ces régimes aux documents électroniques est discutée ailleurs au plan juridique[72].

---

69 P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *op. cit.*, note 67, p. 27. Pour Baudouin, le fait juridique vise « un événement qui entraîne des effets juridiques sans que ces effets aient été recherchés par l'individu qui en est l'auteur. Il est non volontaire dans le sens que, s'il y a volonté de la part de l'individu, cette volonté n'a pas pour but essentiel de créer, de modifier ou d'éteindre une situation juridique », J.-L. BAUDOUIN, *op. cit.*, note 68, pp. 41-42.

70 G. LEFEBVRE, *loc. cit.*, note 67, p. 621.

71 *Commentaires du ministre de la Justice*, t. 2, Québec, Publications du Québec, 1993, sous l'article 2837 C.c.Q. p. 1776.

72 *Infra*, section 2.2.1.

Le maintien de l'attribut d'admissibilité du document électronique est déterminant dans l'élaboration de la Convention, s'agissant là de l'un de ses objets premiers. Cette question prend pour point d'origine le délai qui s'écoule entre l'inscription des données et leur reproduction dans une forme intelligible pour l'homme. Posée simplement, la question est de savoir si les garanties de fiabilité requises à l'étape de l'inscription et de la reproduction du document électronique continuent d'être exigées pendant la conservation des données. En dépit du silence de l'article 2837 C.c.Q. à ce sujet, on ne peut douter de l'existence de l'obligation qu'a la partie qui produit un document électronique en preuve d'établir la fiabilité de chacune des étapes formant le cycle de vie de ce document. La sécurité d'un système se mesure au degré de fiabilité de son composant le plus faible, et des conditions d'archivage qui ne présenteraient pas des garanties de fiabilité suffisantes ne pourraient logiquement assurer la fiabilité d'un document électronique, ni sa recevabilité en preuve.

Vient donc la question plus pragmatique de la preuve des conditions garantissant la fiabilité du document électronique en cours de sa conservation. Cette preuve peut être circonstancielle[73] et reposer sur des politiques d'archivage des inscriptions informatisées[74]. Elle sera facilitée si la personne qui invoque le document électronique peut bénéficier de la présomption de fiabilité établie à l'article 2838 C.c.Q.[75] :

> *« Art. 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. »*

---

73 Article 2837 C.c.Q., alinéa 2.

74 À ce sujet, le lecteur peut se référer à la section 2.3.2.2 du présent mémoire pour une étude des outils de mise en œuvre de systèmes d'archivage fiables.

75 Cette présomption existerait en faveur des tiers du seul fait que l'inscription a été effectuée par une entreprise. En effet, on comprend qu'imposer au tiers le fardeau d'établir les carences d'un système informatique qui lui est étranger est lourd, tout comme il est illusoire de croire que l'entreprise s'efforcera de prouver ses propres carences pour échapper à la présomption de l'article 2838 C.c.Q. L'impasse est réelle, d'autant plus que la notion d'entreprise au sens de l'art. 1525 du C.c.Q. est large et inclut toute « activité économique organisée, qu'elle soit ou non à caractère commercial, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou dans la prestation de services ».

Ainsi, plutôt que de s'attarder à l'acte juridique lui-même, la personne voudra démontrer la fiabilité de l'environnement à l'intérieur duquel l'inscription, la conservation et la reproduction des données ont été réalisées. Des outils d'ordre technique, commercial et juridique constitueront la toile de fond permettant de démontrer l'existence d'un système de conservation de données sans lacunes, protégé contre les altérations accidentelles ou malveillantes.

Dans ce contexte, la définition préalable, par Convention, d'un environnement fiable à des fins probatoires constituera pour des partenaires commerciaux un outil de gestion du risque juridique dans l'hypothèse d'un différend, y compris un litige avec un tiers.

1.1.3.3 Les obligations d'archivage d'origine légale

Au Canada, en matière de conservation de documents, l'entreprise est assujettie à de nombreuses exigences légales libellées de façons multiples. Des lois imposent la tenue de registres[76] ou la conservation de documents spécifiques[77] alors que d'autres prohibent l'altération et la destruction d'écrits[78], ou encore requièrent de l'entreprise qu'elle puisse établir un fait ou un processus diligent[79] tout en lui laissant la discrétion d'identifier et d'archiver la preuve appropriée à cette fin. L'obligation mandatoire ou sous forme d'une prohibition sera généralement assortie d'un délai de conservation prescrit ou découlant du contexte et, dans certains cas, de modalités de conservation. Parmi celles-ci figureront le plus souvent le lieu d'archivage[80], le choix du média[81], l'identification d'une technologie autorisée[82] ainsi que des conditions susceptibles d'assurer l'intégrité et la confidentialité des données conservées[83]. On ne saurait parler d'obligation légale sans sanctions et le législateur n'a pas dérogé à la règle

---

76 Voir, par exemple, le chapitre XVI de la *Loi sur les compagnies du Québec*, L.R.Q., c. C-38, art. 123.11 et suiv.

77 Voir, par exemple, la *Loi sur les valeurs mobilières*, L.R.Q., c. V-1.1, art. 158.

78 Voir, par exemple, la *Loi sur la taxe d'accise* fédérale, c. E-15, art. 100(6).

79 *Id.*, art. 286.

80 Voir, par exemple, la *Loi sur les compagnies*, L.R.Q., c. C-38, art. 107.

81 Voir, par exemple, le *Règlement sur les valeurs mobilières*, R.R.Q., , c. V-1.1R1, art. 220.

82 Voir, par exemple, la *Loi sur les douanes*, L.R.C. (1985), ch. 1 (2e supp.) et son *Règlement visant les personnes autorisées à faire la déclaration en détail de marchandises occasionnelles* (DORS/95-418), arts. 7 et 8.

83 Voir, par exemple, la *Loi sur la protection des renseignements personnels*, L.R.Q., c. P-39.1, art. 10 et ss.

en matière d'archivage. Référence devra évidemment être faite aux textes spécifiques constitutifs de chaque infraction. En général, l'imposition d'amendes[84], de sanctions administratives ou professionnelles[85] ou d'un terme d'emprisonnement, dans les cas qui le justifient, viendront sanctionner le défaut de conserver.

Il n'est pas utile pour nos fins de répertorier et de reprendre ici l'ensemble des lois et des règlements provinciaux ou fédéraux pertinents ou d'en extraire les prescriptions relatives à l'archivage. D'excellents ouvrages de référence sont disponibles[86]. Il importe cependant de survoler quelques grandes catégories de documents d'entreprise qui nous permettront d'incarner les enjeux juridiques discutés plus loin[87].

A) Les documents corporatifs et administratifs

Les documents corporatifs incluent les statuts constitutifs de l'entreprise, les règlements administratifs, les livres et registres, les résolutions et procès-verbaux, les conventions d'actionnaires et les autres documents de même nature mentionnés dans les lois provinciales et fédérales régissant les compagnies[88]. Ces documents sont conservés sur une base permanente, bien que les lois habilitantes précisent rarement leur durée d'archivage. Ils doivent généralement demeurer à l'intérieur du territoire de constitution de l'entreprise, au siège social de cette dernière[89]. La plupart des provinces canadiennes, dont le Québec, permettent la conservation de ces documents sur support informatique ou autre support, incluant les microfilms. Toutefois, le fait pour une entreprise de respecter les exigences d'archivage imposées dans sa province de constitution ne la dispense pas des exigences imposées dans les autres provinces ou territoires où elle exerce des activités et auxquelles elle doit également se conformer. Aussi, le partage ou le cumul des

---

84 Voir, par exemple, la *Loi canadienne sur les sociétés par actions*, L.R.C. (1985) ch. C-44, art. 20(6).

85 Voir, par exemple, la *Loi sur les ingénieurs*, L.R.Q., c. I-9 et son *Règlement concernant les dossiers d'un ingénieur cessant d'exercer*, R.R.Q., c. I-9 r.4 sanctionné au *Code des professions*, L.R.Q., c. C-26, art. 91.

86 À titre d'exemple, on pourra consulter le volumineux *Records Retention, Statutes and Regulations*, vol. 3, Ontario, Carswell, 1999. On pourra également consulter l'excellent « Tableau synthèse » et « Tables des lois et règlements » fournis par S. PARISIEN, P. TRUDEL, V. WATTIEZ-LAROSE, *op. cit.*, note 64.

87 *Infra*, section 1.2.

88 *Loi sur les compagnies*, L.R.Q. c. C-38; *Loi canadienne sur les sociétés par actions*, L.R.C. (1985) ch. C-44.

89 *Loi sur les compagnies*, L.R.Q., c. C-38, art. 104(1), art. 123.111; *Loi canadienne sur les sociétés par actions*, L.R.C., (1985) ch. C-44, art. 20(1). *Records Retention, Law and Practice*, *op. cit.*, note 86, vol. 1, section 2-1, p. 2-1.

compétences entre paliers de gouvernement se répercute-t-il sur l'archivage et certaines sociétés doivent composer avec plus d'un régime.

Les documents administratifs font état des activités de l'entreprise dans le cours normal des affaires et représentent une gamme très large d'écrits, de la note de service interne au plan d'affaires, incluant les contrats et généralement tout autre document témoin de l'existence active de l'entreprise en relation avec ses partenaires et ses clients.

B) Les documents concernant l'emploi et la sécurité au travail

L'entreprise a le statut d'employeur et est tenue de colliger et de conserver des informations concernant ses employés conformément aux législations relatives, notamment, à l'assurance emploi, aux régimes de rentes et de pension et aux relations de travail[90]. Ces informations comprennent, outre le nom, l'adresse et le numéro d'assurance sociale de l'employé, l'ensemble des informations relatives aux tâches qu'il exerce, sa rémunération et ses conditions de travail ou encore, les risques liés à son emploi. L'employeur est également tenu de conserver des dossiers en matière de santé et de sécurité au travail, particulièrement dans certains secteurs d'activités à risques[91].

La durée de conservation de ces dossiers varie grandement, allant de dix ans pour certains documents d'ordre environnemental à six ans pour l'assurance-emploi, en passant par trois ans pour les dossiers personnels des employés, à moins que la loi ne soit silencieuse. Sous réserve d'exceptions ou de permissions obtenues suivant les règles prescrites, l'information doit généralement être conservée à la place d'affaire ou la résidence de l'entreprise au Canada, être confidentielle et raisonnablement accessible pour tout employé. Le recours à l'archivage électronique n'est pas interdit, du moins expressément, et cette possibilité doit être validée au cas par cas, suivant l'interprétation des textes pertinents.

---

90 *Code canadien du travail*, L.R.C. (1985) c. L-2; *Régime de pensions du Canada*, L.R.C. (1985) c. C-8; *Code du travail*, L.R.Q. c. C-27; *Loi sur l'assurance-chômage*, L.R.C. (1985) c. U-1; *Loi sur les produits dangereux*, L.R.C. (1985) c. H-3.

91 Règlement canadien sur la sécurité et la santé au travail SOR/86-304; SOR/88-68; SOR/92-544; SOR/94-263; *Code canadien du travail* [1985] c. L-2, art. 82; *Loi de 1985 sur les normes de prestation de pension* (1985) L.R.C. (1985) c. 32, art. 4, 38 . À titre indicatif, mentionnons la conservation de dossiers concernant des produits dangereux ou contrôlés, les accidents, les risques en milieu de travail ou l'exécution de travaux relatifs aux structures électrifiées, l'amiante, les chaudières, les ascenseurs et les appareils sous pression.

C) Les lois en matière fiscale

De loin les plus nombreuses et les plus arides pour le néophyte, les lois provinciales et fédérales en matière de conservation pour fins fiscales, et l'imposante réglementation qui en découle, peuvent occuper quotidiennement l'archiviste de l'entreprise. Ces textes souvent comparables, parfois complémentaires et, à l'occasion, incompatibles requièrent un examen comparatif dont les conclusions devront mener à l'élaboration de la stratégie d'archivage la plus susceptible d'éviter à l'entreprise la commission d'infractions. En dépit des efforts d'harmonisation déployés par les divers paliers de gouvernement, l'étude particulière des lois relatives à l'impôt sur le revenu, aux gains en capital, aux taxes d'accise ou à la valeur ajoutée sur les produits et services s'avère incontournable. Elle déborde toutefois largement le cadre de ce mémoire, et le lecteur pourra consulter des ouvrages spécialisés en la matière[92], gardant à l'esprit les thèmes pertinents à l'objet de notre exposé, dont la nature des documents à conserver, la durée et les méthodes d'archivage, le lieu où les documents sont archivés, l'inspection des livres et des registres et les pénalités en cas de contravention aux dispositions statutaires et réglementaires concernées.

En règle générale, le ministère fédéral responsable de l'impôt sur le revenu ne précise pas la nature des registres à tenir, étant entendu que toute personne faisant des affaires au Canada a l'obligation de conserver les documents permettant le calcul des impôts payables ou des taxes ou autres sommes qui doivent être perçues, retenues ou déduites par une personne. Parmi ces documents, mentionnons les livres et registres comptables, les pièces justificatives, les bons de commande, les factures, les documents d'importation, les inventaires ainsi que les comptes et états financiers[93]. La loi québécoise n'énumère pas davantage les dossiers qui doivent être conservés, sauf exception. Il est clair, cependant, que les types de documents qui doivent être conservés sont comparables, sinon identiques, à ceux visés par la loi fédérale relative à l'impôt sur le revenu.

---

92 *Records Retention Statutes and Regulations, op. cit.*, note 86, vol. 1 à 3. Aux Etats-Unis, voir B. WRIGHT, J. WINN, *The Law of Electronic Commerce*, 3e ed., New York, Aspen Law & Business, 1999.

93 Par exemple, l'art. 286 de la *Loi sur la taxe d'accise* précise que toute personne qui exploite une entreprise au Canada ou y exerce une activité commerciale doit tenir des livres et des registres en bonne et due forme pour qu'on puisse vérifier les responsabilités et obligations relativement à la taxe ou le montant du remboursement auquel elle a droit. Les livres et registres doivent être tenus dans une forme appropriée et renfermer les renseignements nécessaires pour permettre d'établir le montant de la taxe à payer ou à percevoir, ou encore le montant à rembourser ou à déduire de la taxe.

Sous réserve des exceptions et dérogations susceptibles d'émaner des ministères responsables, la règle générale applicable aux compagnies québécoises et fédérales relativement à la période de rétention est que celles-ci doivent conserver leurs dossiers fiscaux pour une période minimale de six ans à compter de la fin de la dernière année fiscale à laquelle ces dossiers fiscaux se rapportent. Cette période de rétention vise aussi les dossiers conservés sous forme électronique.

En général, les lois fiscales n'imposent pas une méthode unique de conservation des livres et registres et accordent la souplesse que les tribunaux ont prônée[94].

> *« The Act does not require the taxpayer to keep a specific accounting system, but such accounts that are sufficient to give the amount of income taxable, and the amount of tax owing. »*

Cette flexibilité est à l'origine de la reconnaissance par Revenu Canada de registres tenus sur support électronique. Mais avant d'implanter un tel système d'archivage électronique, l'entreprise devra absolument approfondir et faire siennes les normes et lignes directrices émises par les ministères concernés[95].

Nous aborderons maintenant le second thème principal de la première section, soit les risques juridiques liés à l'utilisation de documents électroniques et leur gestion conventionnelle.

1.2 LES RISQUES JURIDIQUES LIÉS À L'UTILISATION DE DOCUMENTS ÉLECTRONIQUES ET LEUR GESTION CONVENTIONNELLE

Nous avons brièvement évoqué en introduction l'existence de risques nouveaux liés au commerce électronique ainsi que la recherche, par l'entreprise, d'outils efficaces de gestion de ces risques. Le présent titre précise ces notions et traite plus spécifiquement des risques d'ordre juridique liés à l'utilisation du document électronique.

---

94 *Labbé* v. *M.N.R.*; [1967] Tax ABC 697, 67 TDC 483.

95 Circulaire d'information intitulée *Conservation et destruction des livres et des registres* no 78-10R2, juillet 1989 et 78-10R2SR, février 1995; Circulaire d'information *Livres, registres et autres exigences auxquelles doivent satisfaire les contribuables ayant des corporations étrangères affiliées*, n° 77-9R, juin 1983; Circulaire d'information *Customs and Excise Maintenance of Records and Books in Canada by Importers*, Memorandum D17-1-21, novembre 1993; Mémorandum sur la TPS 500-1, Livres et registres.

Nous verrons d'abord[96] que l'incertitude du droit dans le cyberespace est à l'origine du risque juridique. Des difficultés d'application au document électronique des notions traditionnelles d'écrit, de signature, d'original et de conditions de formes constituent des manifestations de cette incertitude. Nous verrons ensuite[97] que la Convention constitue un outil efficace de gestion de ces risques. Elle est licite en droit québécois et en phase avec la réalité du cyberespace ou l'autoréglementation et le consensualisme dominent. De plus, elle peut être négociée de gré à gré pour s'adapter aux situations juridiques prévalant entre partenaires commerciaux, tenant compte de leurs besoins et de leurs ressources et de l'évolution prévisible du droit et des technologies.

1.2.1 L'origine et les manifestations du risque juridique

1.2.1.1 L'incertitude comme facteur de risque

L'incertitude du droit dans le cyberespace est à l'origine du risque juridique lié à l'utilisation du document électronique. Les manifestations de ce risque sont intimement liées à la finalité du document électronique et à sa conservation; ainsi, le risque se cristallise et le préjudice survient quand le document électronique ne peut instruire, ni servir utilement à prouver que l'entreprise existe, qu'elle a un passé, qu'elle commerce et qu'elle se conforme à ses obligations légales.

Dans le cyberespace, « l'incertitude ne trouve pas sa source dans l'absence de droit, mais dans son trop-plein »[98]. Internet n'est assujetti à aucune loi spécifique qui lui soit dédiée mais n'est pas pour autant hors la loi[99]. Au contraire, Reinderberg nous rappelle que « le cyberespace est confronté à un cadre réglementaire complexe où l'on découvre une multiplicité de règles provenant de sources différentes et une ambiguïté quant à leur application »[100], soit une multi-normativité émanant du droit étatique d'ordre

---

96 *Infra*, section 1.2.1.

97 *Infra,* section 1.2.2.

98 E. MACKAAY, *op. cit.*, note 45, p. XVI.

99 En effet, le droit interne d'un État trouve application dans le cadre de transactions réalisées par Internet à l'intérieur d'une même juridiction et les règles de droit international privé pertinentes aux situations juridiques présentant un élément d'extranéité sont également applicables.

100 J.R. REINDERBERG, « L'instabilité et la concurrence des régimes réglementaires dans le cyberespace », dans *Les incertitudes du droit*, Montréal, Éd. Thémis, 1999, p. 137.

public et privé[101], de coutumes, de pratiques commerciales et de normes[102]. Cette « fluidité » du droit dans le cyberespace crée d'importantes ambiguïtés dans la classification d'une situation juridique et dans la délimitation des champs d'application des lois[103]. De plus, la montée des règles technologiques[104] et d'une véritable *lex informatica* comme outil normatif[105], le recul du droit étatique lent à réagir à l'environnement virtuel, et la multiplicité des sources de réglementation sont à l'origine d'une concurrence de régimes normatifs et de forums compétents. Cette concurrence accentue ces ambiguïtés et crée une forme d'instabilité et d'incohérence. L'incertitude juridique qui en découle dans le cyberespace réduit la capacité de l'entreprise de gérer ses relations d'affaires de façon rationnelle et bien informée. Pour Ejan Mackaay[106] :

> *« Les juristes s'inquiètent d'une incertitude du droit lorsque les sources habituelles du droit et les canons habituels d'interprétation ne leur permettent pas ou ne leur permettent plus d'arriver, d'une manière largement acceptée, à des conclusions sur ce qu'est le droit ou sur ce que les tribunaux décideront sur un point particulier. Les procédures d'argumentation juridique communément suivies ne rendent pas des services convaincants. »*

1.2.1.2 L'incertitude et le document électronique

L'incertitude du droit à l'égard du document électronique s'explique à l'étude de ses attributs distinctifs[107] parmi lesquels figure en première place la dématérialisation.

---

101 Consulter, à titre d'exemple, *Braintech Inc.* c. *John C. Kostiuk* [1999] B.C.J. n° 622; voir également *Bensusan Restaurant Corporation* v. *King*, U.S. Court of Appeal (Second Circuit) 10 septembre 1997; *Cybersell Inc.* v. *Cybersell Inc.*, 130 F. 3d 414, 419 (9th Cir. 1997); P. TRUDEL, *op. cit.*, note 44, chapitre 4, Les principes d'attribution et d'exercice de la juridiction, pp. 4-1 et ss.

102 Référence pourra être faite, par exemple, aux principes énoncés dans la Norme nationale du Canada intitulée Code type sur la protection des renseignements personnels, CAN/CSA-Q830-96, validée par le *Projet de loi C-6*.

103 J.R. REINDERBERG, *loc. cit.*, note 100, p. 137, donne l'exemple du traitement de l'information nominative qui concerne à la fois les textes législatifs sur la protection des données personnelles, la propriété intellectuelle, les télécommunications et les ententes de libre-échange économique.

104 Le développement de protocoles d'échange d'informations tel la norme PICS (*Plateform for Internet Content Selection*) ou P3P (*Plateform for Privacy Preferences*) et TRUSTE en matière de transfert de renseignements personnels et de protection de la vie privée témoignent de l'impact normatif de la technologie. Consulter à ce sujet, J.R. REINDERBERG, *The Use of Technology to Assure Intenet Privacy : Adapting Labels and Filters for Data Protection*, 1997, 3 Lex Electronica disponible au site http://www.lex-informatica.org/reidenbe.html.

105 J.R. REINDERBERG, « Lex informatica : The Formulation of Information Policy Rules Through Technology », (1988) 76 *Texas L. Rev.* 553.

106 E. MACKAAY, *op. cit.*, note 45, p. X.

107 *Supra*, section 1.1.2.

Se pose d'abord la question de savoir si le document électronique constitue bel et bien un document au sens des textes de loi applicables. Aux États-Unis, des lois reconnaissent le document électronique dans près de cinquante États suivant des définitions qui varient d'une législature à l'autre[108]. Au Canada, bien que des législatures aient déjà inclus spécifiquement les documents numérisés ou créés en langage machine dans la définition du concept de « documents » ou d' « écrits » aux fins de l'application ou de l'interprétation de lois particulières[109], les auteurs s'entendent pour conclure à l'existence de difficultés réelles, particulièrement en matière de preuve, où le document numérique est fréquemment grevé d'un statut fragile. L'exigence d'un formalisme documentaire[110] n'est pas sans fondement, ni sans objectifs légitimes dont :

> « *(1) veiller à ce qu'il y ait des preuves tangibles de l'existence et de la nature de l'intention manifestée par les parties de se lier entre elles;*
>
> *(2) aider les parties à prendre conscience des conséquences de la conclusion du contrat;*
>
> *(3) fournir un document lisible par tous;*
>
> *(4) fournir un document inaltérable et conserver en permanence la trace d'une opération;*
>
> *(5) permettre la reproduction d'un document de manière que chaque partie ait un exemplaire du même texte;*
>
> *(6) permettre l'authentification des données au moyen d'une signature;*
>
> *(7) assurer que le document se présente sous une forme acceptable par les autorités publiques et les tribunaux;*
>
> *(8) consigner l'intention de l'auteur de l'écrit de conserver la trace de cette intention;*
>
> *(9) permettre un archivage aisé des données sous une forme tangible;*

---

108 Pour une analyse des stipulations essentielles de ces lois américaines, consulter le site de la firme McBride Baker and Coles concernant le commerce électronique, disponible à l'adresse http://www.mbc.com/ecommerce/legis/.

109 Au Canada, voir *infra*, sections 2.2.2.3, 2.2.2.4 et 2.2.2.5. Pour une étude exhaustive des législations internationales, consulter A. ERLANDSSON, « Electronic Record Management, a Literature Review », Conseil national des archives, avril 1996, Études CIA 10.

110 Au Québec, par exemple, les articles 1385, 1414, 2934, 2822 et 378 C.c.Q.

> *(10) faciliter le contrôle et les vérifications ultérieures à des fins comptables, fiscales ou réglementaires; et*
>
> *(11) établir l'existence de droits et obligations juridiques dans tous les cas où un écrit était requis aux fins de validité.* »[111]

L'exigence d'une signature pose d'autres problèmes juridiques à l'égard du document électronique. Les différents concepts de signature électronique et l'étude comparative des attributs juridiques des signatures classique et électronique font à elles seules l'objet d'ouvrages de doctrine auxquels pourra se référer le lecteur désireux d'approfondir le sujet[112]. Rappelons simplement que le document électronique, par son caractère immatériel, ne peut être signé, du moins pas au sens classique du terme[113]. Au Québec, il peut néanmoins porter une marque qui est personnelle à son auteur et qu'il « utilise de façon courante, pour manifester son consentement »[114]. Cette marque ou signature peut s'obtenir aujourd'hui grâce à de puissants algorithmes de cryptographie asymétrique permettant d'assurer l'identification, l'intégrité, la confidentialité et la non-répudiation des messages[115].

Cette signature électronique, à l'instar de la signature classique, « sert, d'une part, à identifier le signataire et, d'autre part, elle exprime sa volonté d'adhérer au contenu de l'acte qu'il a signé ou de se l'approprier »[116]. Ces fonctions d'identification et de manifestation de la volonté de l'auteur servent de dénominateurs communs à ces deux formes de signature.

---

111 Conseil international des archives, *Guide for managing electronic records from an archival perspective*, *op. cit.*, note 50, p. 24.

112 Il est important de distinguer entre la signature électronique et la signature numérique. La signature numérique est typiquement fondée sur les systèmes de cryptographie asymétrique à clé publique suivant certaines technologies (RSA, NIST). Le concept plus large de signature électronique inclut, outre la signature numérique, d'autres technologies telles la cryptographie quantique et la biométrie. Pour en apprendre davantage, consulter S. PARISIEN, P. TRUDEL, V. WATTIEZ-LAROSE, *op. cit.*, note 24, pp. 93 et ss.

113 Selon le professeur QUIKENBORNE « Signer ce n'est pas seulement écrire son nom, c'est encore l'écrire d'une façon distinctive, en employant un graphisme personnel, essentiellement propre au signataire. Généralement, le signataire entoure son nom d'un certain nombre de traits et d'agréments, d'un « paraphe ». (…) La signature apparaît comme un « amalgame plus ou moins savant de formes et de lignes obéissant à une esthétique imprécise. »; M. QUIKENBORNE, « Quelques réflexions sur la signature des actes sous seing privé » (1985) *Revue critique de jurisprudence belge*, pp. 65 et 81, cité dans P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *op. cit.*, note 67, p. 59.

114 Art. 2827 C.c.Q.

115 S. PARISIEN, P. TRUDEL, V. WATTIEZ-LAROSE, *op. cit.*, note 24, pp. 93-117.

116 P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *op. cit.*, note 67, p. 62.

> *« Elle représente ainsi une métaphore pour désigner les mécanismes par lesquels les parties à une transaction ayant été effectuée par le truchement des moyens de communication électroniques vont s'identifier et manifester leur volonté de s'approprier le contenu d'un acte ou d'une transaction. Ce n'est donc que par la réalisation de cette double fonction que la signature électronique mérite son appellation de « signature » et rejoint la signature manuscrite au sens classique. »*[117]

L'existence de fonctions équivalentes n'élimine pas pour autant les obstacles à la reconnaissance et à la preuve de la signature électronique, ni ne diminue l'importance des risques technologiques qui en découlent. Ces risques[118], qui peuvent prendre la forme d'un accident informatique, d'une erreur de conception de logiciel, d'une erreur dans un programme ou, encore, d'une fraude ou d'un piratage, soulèvent le problème de l'authentification du document électronique signé et, par conséquent, du consentement qu'il exprime. L'existence de crypto-systèmes de signature numérique, de chiffrement et de scellement, le recours à des tiers certificateurs sont autant de moyens de sécurisation qui confortent les observateurs. Il reviendra néanmoins au tribunal d'évaluer, au cas par cas, si un document marqué d'une signature électronique permet d'identifier véritablement son auteur et de prouver l'existence d'un consentement valable.

En amont de l'appréciation de ces risques, la question de la reconnaissance légale de la signature demeure. Au Québec, il faut constater que, lors de la réforme de 1994, le législateur s'est donné une définition de la signature qui est « plus libérale que celle qui est traditionnellement retenue par la jurisprudence et la doctrine »[119] :

> *« 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. »*

Rien ne donne à penser à l'article 2827 C.c.Q. que la signature doit être manuscrite, ni qu'elle doit transcrire un nom. Au contraire, toute marque personnelle distinctive pourra, du fait de son usage courant, servir au signataire pour consentir valablement à un acte juridique. En ce sens, la signature électronique satisfait à

---

117 *Id.*, p. 83.

118 *Id.*, pp. 66 et ss.

119 *Id.*, p. 65.

l'article 2827 C.c.Q. et s'inscrit en droite ligne avec l'intention du législateur[120]. La situation au Canada évolue positivement, tout particulièrement avec le *Projet de loi C-6,* mais des difficultés de reconnaissance de la signature électronique demeurent[121]. Des lois fédérales[122] admettent l'utilisation d'une signature électronique et des tribunaux canadiens ont manifesté leur volonté de reconnaître l'évolution technologique au plan des échanges et des communications, mais des exigences strictes continuent de s'appliquer aux termes d'autres lois et des règles de *common law.* D'importantes lois fédérales d'application générale telles la *Loi sur la preuve du Canada* et la *Loi d'interprétation* n'autorisent pas encore[123] de façon expresse le remplacement d'une signature manuscrite par une signature électronique, et les juges aux prises avec cette difficulté devront autrement disposer de l'identification, de l'authenticité et de l'intégrité du document électronique en recherchant des garanties suffisantes de fiabilité. De plus, même si un magistrat jugeait que la présence d'une signature électronique permettait de satisfaire à l'exigence d'un document signé, on peut douter qu'il arriverait sans réticence au même genre de conclusion à l'égard d'autres exigences, comme celle d'obtenir copie d'un document signé « certifié », « notarié » ou « suivant la forme prescrite ».

Vient ensuite la question du document original. Cette quête en matière de preuve est avant tout dictée par la règle de la meilleure preuve. D'origine anglaise, cette règle consacrée au Québec à l'article 2860 C.c.Q. impose à la partie qui veut prouver le contenu d'un écrit, ou l'acte juridique constaté dans un écrit, le fardeau de produire l'original ou une copie qui légalement en tient lieu, sous réserve d'exceptions prévues à la loi, notamment dans le cas où, malgré sa bonne foi et sa diligence, la partie a été dans

---

120 *Commentaires du ministre de la Justice*, t. 2, Québec, Publications du Québec, 1993, sous l'art. 2827 C.c.Q., p. 1771, « Cette définition est suffisamment large pour comprendre, par exemple, un numéro de code spécifique permettant d'identifier une personne en matière d'inscriptions informatisées; en effet, la signature ne correspond pas uniquement à l'écriture qu'une personne fait de son nom. »

121 *Infra*, section 2.2.2.3. Consulter également, A. GATHAN, *op. cit.*, note 66, pp. 137-164.

122 Consulter à ce sujet les textes disponibles au site http://www.canada.justice.gc.ca en matière de documents électroniques, chapitres 2 à 9.

123 Nous verrons que l'entrée en vigueur du *Projet de loi C-6* aura un impact limité en l'absence de réglementation concernant la signature, *Infra,* section 2.2.2.3.

l'impossibilité de se ménager un écrit ou de le produire. Des règles comparables existent dans les provinces de *common law*[124].

La difficulté que pose le document électronique dans l'application de cette règle s'évalue suivant deux cas de figure. Dans un premier cas, le document électronique est créé simultanément à l'acte dont il atteste l'existence et n'existe que sous forme électronique, dans un langage machine incompréhensible pour le commun des mortels. L'EDI illustre ce premier scénario de façon typique dans la mesure où le listage sur support papier ne constituerait qu'une reproduction théoriquement irrecevable en preuve, sous réserve d'invoquer avec succès l'exception d'impossibilité visée au deuxième alinéa de l'article 2860 C.c.Q. Le plaideur soutiendra l'impossibilité, sinon l'inutilité de produire un original dématérialisé illisible.

Le second scénario vise l'acte juridique conclu oralement ou par écrit et dont les données sont subséquemment inscrites sur support informatique. Ce stockage d'informations intervenant postérieurement à l'acte juridique fait dire qu'en l'absence d'une véritable substitution, le support informatique ne saurait remplacer le support papier d'origine qui, suivant les règles de preuve, lui est hiérarchiquement supérieur pour faire preuve du contenu de l'acte. La situation est aggravée pour l'entreprise qui choisit de détruire l'original papier à la suite de la numérisation de ce dernier, puisqu'elle perd ainsi la possibilité d'invoquer le bénéfice de l'exception d'impossibilité prévue à l'article 2860 C.c.Q., à moins qu'elle ne puisse satisfaire aux exigences des articles 2840 à 2842 C.c.Q. étudiées en détail au second chapitre de l'exposé[125]. Cette problématique existe de la même façon dans les provinces de *common law*[126].

Ces deux scénarios témoignent de risques inhérents à l'utilisation de documents électroniques.

---

124 I. KYER, « Computer Record as Courtroom Evidence », *Computer Law*, vol. 1, no 8, août 1984, p. 56; I.W. OUTERBRIDGE, « The Admissibility of Computer-Produced Evidence », *The Advocate's Society Journal*, avril 1985, p. 4; L.C. SMITH, « The Evidence Act 1995 (cth): Should Computer Data Be Presumed Accurate? », *Monash University Law Review*, vol. 22, no 1, 1996, p. 165; C. KEN, « Computer-Produced Records in Court Proceedings », *Uniform Law Conference of Canada*, juin 1994; « Documents électroniques et preuve », chap. 9, *Groupe de travail sur les questions de droit, stratégie STI*, disponible au site http://www.canada.justice.gc.ca/commerce/chapitre/ch09-fr.txt; GREGORY ET TOLLEFSON, « Projet de loi uniforme sur la preuve électronique », Annexe N, *Conférence pour l'harmonisation des lois au Canada*, disponible au site http://www.law.ualberta.ca/alri/ulc.

125 *Infra*, section 2.2.1.3.

126 *Belland* c. *R.*, (1982) 65 C.C.C. (2d) 377 (CA); *McMullan* c. *R.*, (1979) 47 C.C.C. (2d) 499 (CA), (1978) 42 C.C.C. (2d) 67.

Un dernier point. L'expérience du plaideur fait souvent dire que certains différends n'existent qu'en raison de l'incertitude qui peut, à l'occasion, découler de la mise en place de nouvelles règles de droit, de l'apparition de nouveaux sujets de droit ou de l'interprétation de textes non conçus pour connaître de nouvelles réalités. On parlera alors de nouvel environnement juridique, de pluralité ou de concurrence de régimes ou encore, de droit transitoire pour qualifier de façon imparfaite l'absence de règles établies permettant aux justiciables de cerner et de comprendre clairement, précédents à l'appui, la règle de droit qui s'applique et agir en conséquence. Cette incertitude peut, selon nous, se traduire par l'institution de procédures qui, le temps et l'expérience judiciaire aidant, n'auraient pas été intentées ou auraient fait l'objet d'un règlement à l'amiable. On peut constater sans trop risquer de se tromper que de telles plages d'incertitudes existent dans les relations juridiques établies par les entreprises dans le cyberespace. Des litiges portant sur l'appropriation de noms de domaine[127], sur la responsabilité des intermédiaires pour violation de droits d'auteur[128] ou le respect de contrats de distribution ou de franchise territoriale dans le cyberespace[129] constituent des exemples très révélateurs.

Il faut admettre que cette dernière proposition demeure empirique. En outre, elle est affaiblie du fait que les relations établies sur Internet demeurent à ce jour passablement déjudiciarisées, peut-être parce que les internautes acceptent d'emblée les risques associés à ce monde virtuel. L'histoire judiciaire des prochaines années nous fournira des éléments d'analyse de l'effet net des pressions qui s'opposent. Un élément demeure incontournable cependant : la progression fulgurante de la valeur des échanges commerciaux dans le cyberespace et du nombre d'intervenants va causer un accroissement du nombre de différends. Or, la résolution de ces différends implique nécessairement un processus onéreux dont le résultat demeure incertain, d'où un risque pour toute entreprise.

---

127 Voir, par exemple, *British Telecommunications plc* v. *One In A Million Limited*, 148 NLJ 1179; *Panavision Int'l, LP* v. *Toeppen*, 141 F (3d) 1315 (9th Cir. 1998).

128 *Playboy Enterprises Inc.* v. *Frena*, 839 F. Supp. 1552 (N.D. Fla. 1993); *Sega Enterprises Limited* v. *Maphia*, 857 F. Supp. 679 (D.D. Cal. 1994); *Religious Technology Centre* v. *Netcom On-Line Communication Services*, 907 F. Supp. 1361 (N.D. Cal. 1995).

129 Voir les décisions commentées dans « Challenges of the Internet for Agency, Distribution and Franchising Agreements », *International Bar Association*, vol. 27, no 4, juin 1999, pp. 241-288.

1.2.2 La Convention comme outil de gestion efficace des risques

La Convention constitue un outil efficace de gestion de risques juridiques liés à l'utilisation de documents électroniques pour trois raisons principales : elle est licite, compatible aux réalités d'Internet et adaptable.

1.2.2.1 Une Convention licite en droit québécois

> *« Dans le régime de droit civil du Québec, sous réserve de ce qui est contraire à l'ordre public, pourvu que les parties aient la capacité de contracter, la convention des parties fait loi. »* [130]

Cet énoncé de la Cour rappelle que les stipulations des parties constituent la première source du droit qui les régit. Il nous renvoie aux principes généraux de l'autonomie de la volonté et de la liberté contractuelle consacrés à l'article 9 C.c.Q., tenant compte d'un régime d'exception relatif à l'ordre public[131] :

> *« Art. 9. Dans l'exercice des droits civils, il peut être dérogé aux règles du présent Code qui sont supplétives de volonté; il ne peut cependant être dérogé à celles qui intéresse l'ordre public. »*

Or, la Convention est une entente négociée de gré à gré entre partenaires commerciaux aux fins d'aménager un régime conventionnel de conservation et de preuve de documents électroniques. Elle n'est pas contraire à l'ordre public. Elle est le fruit d'un exercice licite de cette liberté contractuelle et devrait, par conséquent, être reconnue et appliquée par nos tribunaux, sous réserve du respect de dispositions d'ordre public que nous aborderons plus loin. Cette conclusion s'établit par référence au double objet[132] de la Convention, soit la conservation et la preuve de documents électroniques.

En matière de conservation, nous avons précédemment indiqué que l'entreprise est assujettie à des obligations légales d'archivage stipulées de façons

---

130 *Mousseau* c. *Société de gestion Paquin Ltée*, [1994] R.J.Q. 2005 (C.S.), p. 2008, appel rejeté.

131 Pour une discussion du concept d'ordre public, consulter J.-L. BAUDOIN, P.-G. JOBIN, *Les Obligations*, 5e éd., Cowansville, Éd. Y. Blais, 1998, pp. 150-170. Ces auteurs distinguent les concepts de bonnes mœurs, d'intérêt général et d'ordre public en référant dans ce dernier cas aux concepts d'ordre public politique et moral et d'ordre public social et économique de direction ou de protection afin de classifier les différentes manifestations de l'ordre public qui constituent aujourd'hui, sous l'empire du nouveau *Code civil du Québec*, un principe fondamental qui s'ajoute à ceux de l'autonomie de la volonté, de l'équité et de la bonne foi.

132 L'art. 1373 C.c.Q. prévoit que l'objet de l'obligation ne doit pas être contraire à l'ordre public.

diverses selon l'objectif du législateur[133]. Ces dispositions statutaires ou réglementaires fixent des balises ou imposent des exigences relatives, notamment, à l'identification des informations à conserver, à la durée ou au lieu d'archivage ou encore aux modalités de destruction de documents, pour ne donner que ces exemples. Certes, les parties contractantes devront prendre en compte ces prescriptions dans l'élaboration de la Convention afin de satisfaire à leurs obligations, d'autant plus qu'elles émanent généralement de lois d'ordre public. Il s'agit là d'un encadrement législatif contraignant à l'étape de l'élaboration du contenu de la Convention, mais qui ne limite pas le choix des moyens dont entend se servir l'entreprise pour rencontrer ses obligations statutaires. La légalité, *per se*, de la Convention n'est d'aucune façon mise en cause par ces dispositions, la question véritable étant plutôt de savoir si ces dispositions reconnaissent l'existence et les effets juridiques du document électronique.

À ce sujet, un bon nombre de lois d'importance en matière d'archivage acceptent déjà les documents sous forme numérique. En guise d'exemple, Revenu Canada reconnaît, outre les livres comptables traditionnels accompagnés de pièces justificatives, « *les registres tenus sur un support d'information assimilable par une machine qui peuvent être réassociés aux pièces justificatives et qui sont pris en charge par un système capable de produire une copie facile d'accès et facile à lire, ainsi que les microfilms ... de livres d'écriture originaires et de pièces justificatives qui sont produits, contrôlés et mis à jour* »[134] suivant une norme acceptable à cette fin[135]. On comprend par ailleurs que le ministère aurait comme pratique de conclure des ententes avec les contribuables relativement aux registres informatisés à conserver et au traitement de ces registres lors de vérifications subséquentes, de façon à éviter que les contribuables aient à conserver tous leurs documents électroniques et à s'assurer que les données soient disponibles lors de vérifications ultérieures[136].

Est également d'intérêt l'article 286 de la *Loi sur la taxe d'accise* relatif à la tenue de livres et de registres. On y apprend que les registres peuvent prendre différentes

---

133 *Supra,* section 1.1.3.3.

134 Circulaire d'information intitulée *Conservation et destruction des livres et des registres*, no 78-10 R2, juillet 1989, révisée no 78-10R2SR, février 1995, art. 7; Norme Can 2-72.11-79 *Microfilm et images électroniques* disponible au Centre des publications – Approvisionnement et Services, Gouvernement du Canada.

135 Pour comprendre les conditions d'acceptation d'un programme de microfilms, veuillez consulter la circulaire d'information intitulée *Conservation et destruction des livres et des registres*, *loc. cit.*, note 134.

136 *Id.*, art. 15.

formes, incluant *« des registres tenus au moyen d'un support d'informations assimilable par une machine qui peuvent renvoyer aux documents de base et qui sont appuyés par un système ayant la capacité de produire des exemplaires accessibles et visibles. »*[137]. Le ministère est donc prêt à reconnaître les images électroniques des registres et des livres *« pourvu que ceux-ci soient produits, contrôlés ou maintenus en conformité avec la Norme nationale du Canada, CAN/CGSB-72.11-93, intitulée Microfilms et images électroniques – Preuve documentaire »*[138]. Les principaux facteurs nécessaires à la mise en œuvre d'un programme acceptable de tenue de livres et registres sous forme électronique incluent : (1) l'obtention d'une autorisation écrite d'une personne habilitée par l'entreprise confirmant que le programme de gestion comptera parmi les activités régulières et courantes de l'entreprise, (2) la preuve que les systèmes et les processus du programme sont établis et documentés, (3) la preuve qu'est tenu un journal contenant la date de la saisie des images, les signatures des personnes qui autorisent et exécutent la saisie d'images et une brève description des registres dont l'image a été saisie, (4) la tenue d'un répertoire facilitant l'accès à tout registre, (5) la réalisation d'images électroniques de qualité commerciale, (6) l'établissement d'un système d'inspection et de contrôle de qualité et enfin, (7) un accès au matériel susceptible de permettre de visualiser ou reproduire l'image électronique[139].

Rappelons aussi que les déclarations d'intention du gouvernement québécois concernant l'inforoute[140], en phase avec celles des gouvernements canadien et américain, laissent peu de doute quant aux tendances actuelles en vue de l'usage de documents électroniques et de leur admissibilité devant les tribunaux de droit commun. Le *Projet de loi C-6*[141] constitue un précédent à ce sujet. D'une part, on y reconnaît expressément le document électronique et y trouve les amendements requis de la *Loi sur la preuve du Canada* pour donner effet à cette reconnaissance. D'autre part, il y est stipulé que, dans le cas où une disposition d'un texte législatif exige la conservation d'un document pour une période déterminée, la conservation du document électronique satisfait à cette obligation

---

137 *Exigences relatives à la tenue des registres (1995),* Farnham, Les Publications CCH/FM Ltée, Section 15.1, pp. 82,851-82,868.

138 *Id.*, pp. 82,856-82,857.

139 *Ibid.*

140 Voir les communiqués et déclarations du gouvernement disponibles au site http://www.gouv.qc.ca/recherche/index.html, sous l'expression « autoroute de l'information ».

141 *Projet de loi C-6, supra*, note 51.

aux conditions discutées à la section 2.2.2.3. D'autres lois et initiatives législatives au même effet sont notées par les auteurs, particulièrement aux États-Unis[142].

Pour ces raisons et celles évoquées précédemment, il nous semble que la Convention ne pourrait être déclarée illégale du fait de ses objectifs ou de sa fonction d'archivage. Son contenu devra néanmoins se conformer aux prescriptions légales pertinentes.

La question de la légalité de la Convention doit ensuite être abordée en regard de la légalité de dérogations conventionnelles aux règles concernant l'existence, l'objet, le fardeau, l'admissibilité ou la force probante d'une preuve. Ces règles sont établies au Livre septième du *Code civil du Québec*[143].

La légalité des conventions relative à la preuve a été traitée par certains auteurs québécois[144] qui font conclure au peu d'autorités sur cette question en général et à un vide quasi complet dans le cadre du commerce électronique. Cette question ferait toujours l'objet d'une controverse que nous exposerons brièvement pour ensuite juger de l'impact véritable de ces positions contradictoires sur la légalité de la Convention.

L'étude du droit de déroger d'avance par Convention à des règles de preuve nous renvoie nécessairement à la qualification d'ordre privé ou d'ordre public de ces règles de preuve. En effet, l'article 9 C.c.Q. ne permet pas de douter aujourd'hui du droit de s'exclure des règles du Code qui sont supplétives de volonté, ni de l'interdiction de déroger à celles qui intéressent l'ordre public.

Selon Trudel, Lefebvre et Parisien, on doit conclure au caractère licite de la Convention relative à la preuve[145]. Ces auteurs rappellent néanmoins, comme d'autres[146]

---

142 Consulter à ce sujet le dernier Rapport de la délégation canadienne à la trente-quatrième session du Groupe de travail de la CNUDCI sur le commerce électronique et les documents préparatoires disponibles au site http://www.canada.justice.gc.ca/Commerce/ un99gau_fr.html.

143 Les articles 2803 à 2874 forment le Livre septième du *Code civil du Québec* qui a été adopté et sanctionné le 18 décembre 1991 et constitue le nouveau droit de la preuve en matière civile au Québec.

144 J.-C. ROYER, *op. cit.*, note 67, p. 991; P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *op. cit.*, note 67, p. 98; N. L'HEUREUX, L. LANGEVIN, « La Pratique des cartes de paiement au Québec : l'Apport du droit comparé »,(1990) 50 *R. du B.* 237.

145 P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *op. cit.*, note 67, p. 99 : « Pour notre part, nous croyons que les parties sont, en principe, libres de déroger aux règles de preuve que prévoit le Code civil du Québec pour mieux adapter celles-ci à leurs besoins et à leurs préoccupations. »

146 N. L'HEUREUX, L. LANGEVIN, *loc. cit.*, note 144, p. 265; L. DUCHARME, *op. cit.*, note 67, p. 394, no 1325-1326; J.C. ROYER, *op. cit.*, note 67, p. 996, no 1611.

qu'il « *existe un certain nombre de cas où, pour des motifs d'ordre public, le juge doit imposer le respect strict des règles de preuve* »[147] et prévoient que nos tribunaux voudront élaborer « *une solution mitoyenne leur permettant de respecter le principe de la liberté contractuelle, tout en veillant à ce qu'il ne soit pas fait de celle-ci un « usage abusif », notamment en présence d'un contrat de consommation ou d'adhésion* »[148].

Le caractère privé des règles de preuve est également soutenu par Ducharme[149] et par Fabien[150] alors que la validité des conventions relatives à la preuve trouve d'importants appuis dans le droit français[151] et la *common law*. En effet, selon L'Heureux et Langevin[152] :

> « *En droit français, une partie de la doctrine et la jurisprudence admettent le caractère d'ordre privé des règles de preuve et donc la possibilité pour les parties de les modifier conventionnellement. « Une convention sur la preuve est au fond une convention sur le droit, donc, on peut disposer d'un droit, on peut également en régler conventionnellement l'attribution ou la perte et par conséquent la subordonner à un tel mode de preuve. » Il s'agit d'une conception individualiste du procès. Le droit anglais semble aussi admettre de telles conventions.* » (*Références omises*)

Caprioli[153] abonde dans le même sens à l'égard du droit français :

> « *De jurisprudence constante, les dispositions relatives à la preuve ne sont pas d'ordre public*[51] *de sorte que les parties peuvent aménager librement l'admissibilité et la force probante de leurs messages électroniques.* » (*Références omises*)

---

147 P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *op. cit.*, note 67, p. 99, cité de L. DUHARME, *Précis de la preuve*, 2e éd., Montréal, Wilson & Lafleur Ltée, 1985, p. 216.

148 P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *op. cit.*, note 67, p. 100.

149 L. DUCHARME, *op. cit.*, note 67, p. 396, no 1334.

150 C. FABIEN, « La communicatique et le droit civil de la preuve », *Actes du colloque conjoint des Universités de Poitiers et de Montréal*, Éd. Thémis, 1992, p. 182.

151 Des auteurs soulignent que la position dominante du droit français en la matière n'est pas exempte de critiques par la doctrine; N. L'HEUREUX, L. LANGEVIN, *loc. cit.*, note 144, p. 264; J.C. ROYER, *op. cit.*, note 67, p. 991, note 1605.

152 N. L'HEUREUX, L. LANGEVIN, *loc. cit.*, note 144, pp. 264, 265.

153 É.A. CAPRIOLI, « Les tiers de confiance dans l'archivage électronique : une institution juridique en voie de formation », dans *Les incertitudes du droit*, Montréal, Éd. Thémis, 1999, pp. 25, 44; voir au même effet A. LUCAS, « Le droit de l'informatique », *Presses universitaires de France*, 1994, p. 379.

Wigmore[154] résume ainsi la position dominante de la *common law* :

> « *A contract, made before a controversy has arisen, to alter the general rules of evidence applicable in jury trials may conceivably replace those rules in one of the four following ways: 1. A contract may require presentation by the promissee, for the benefit of the promissor, of more or other evidence than might suffice under the usual rules – eg (...) 2. The contract may permit, for the stipulating party, less or other evidence than might be required under the usual law. – eg (...) 3. The contract may exclude evidence that the usual law would admit. – eg (...) 4. The contract may admit, for the stipulating party, evidence that the usual law would exclude. – eg (...).* »

Au Québec, le professeur Royer diverge d'opinion. Il distingue le droit d'une partie de renoncer à la sanction de certaines règles d'irrecevabilité, dont l'inobservation ne porte pas atteinte à l'ordre public, du droit de cette partie de contractuellement renoncer d'avance à l'application des règles de preuve. Si le premier cas se pose sans difficulté, le second contreviendrait à l'ordre public, *a fortiori,* lorsqu'une clause dérogatoire est contenue dans un contrat d'adhésion[155] :

> « *À notre avis, ces clauses dérogatoires ne sont pas valables lorsqu'un litige est entendu devant un tribunal. Les règles de preuve ont un fondement et une finalité qui touchent à l'ordre public. Elles assurent les plaideurs que la justice sera rendue ou apparaîtra être rendue par les tribunaux selon les mêmes normes. Ainsi, selon nous, une partie ne peut contractuellement renoncer d'avance à l'application des règles de preuve. Il devra en être ainsi, a fortiori, lorsqu'une clause dérogatoire est contenue dans un contrat d'adhésion qu'une partie n'a même pas eu l'opportunité de discuter et de négocier.* »

L'auteur s'explique davantage en rappelant que les règles concernant l'objet, le fardeau, l'existence et la valeur probante de la preuve réglementent davantage le rôle du juge, qui se doit d'intervenir d'office ou sur demande, que celui des parties; ce faisant, il reprend les critiques de l'approche libérale traditionnelle du droit français et de la *common law* en cette matière.

Il nous semble que les positions exprimées par ces auteurs québécois convergent à bien des égards et qu'elles délimitent de façon cohérente le contenu d'une

---

154 J.-H. WIGMORE, *Evidence in Trials at Common Law*, vol. 1 no 7A, Toronto, Little, Brown & Company, 1983, p. 559. De très nombreux cas d'application et d'exceptions sont traités par Wigmore, aux pages 560 à 603 sous le titre « Agreements to vary Rules ».

155 J.-C. ROYER, *op. cit.*, note 67, pp. 994-995, no. 1607.

Convention licite. En effet, tous concluent à l'illégalité de dérogations conventionnelles contraires à l'ordre public et, partant, à l'existence de cas concrets où le juge devra voir au respect strict des règles de preuve. Le *Code civil du Québec*, nos tribunaux et les auteurs ont identifié de tels cas, notamment en matière d'atteintes aux droits et libertés fondamentales susceptibles de déconsidérer l'administration de la justice[156], de protection du secret professionnel ou gouvernemental[157], de contradiction d'un acte authentique[158], de preuve d'état des personnes[159], de réfutation de certaines présomptions légales[160], d'assermentation et de capacité des témoins[161], sans oublier les matières pénale et criminelle[162].

On a de la même façon identifié des règles de preuve conçues pour protéger les intérêts privés des parties, donc auxquelles il leur est possible de renoncer par Convention. Il en est ainsi, par exemple, en matière d'admissibilité de la preuve secondaire du contenu d'un écrit[163], d'admissibilité de la preuve testimoniale d'un acte juridique[164], de la contradiction des termes d'un écrit valablement fait[165], de la preuve d'un aveu extrajudiciaire[166] ou de la renonciation à certaines présomptions[167]. Il en est de même quant aux règles de preuve relatives à l'administration générale de la preuve, incluant, par exemple, l'interdiction de prouver un fait non allégué, la prohibition de poser des questions suggestives à son témoin, et les règles relatives à l'objet de l'interrogatoire en chef, du contre-interrogatoire et du ré-interrogatoire[168]. L'article 2859

---

156 Art. 2858 C.c.Q.; Protection de la Jeunesse – 661, J.E. 94-307 – C.Q. Montréal 500-03-001948-937; L. DUCHARME, *op. cit.*, note 67, p. 396, no 1333.

157 Art. 308 C.p.c.; J.C. ROYER, *op. cit.*, note 67, p. 997, no 1613; *Poulin* c. *Pratt*, [1994] R.D.J. 301 (C.A.).

158 Art. 2821 C.c.Q.

159 Art. 530 à 535 C.c.Q.; *Drouin c. Landry*, [1976] C.A. 763.

160 Art. 2866 C.c.Q.

161 Art. 297 C.p.c., J.C. ROYER, *op. cit.*, note 67, p. 1002, no 1622.

162 J. BELLEMARE, L. VIAU, « *Droit de la preuve pénale* », Montréal, Éd. Y. Blais, 1991.

163 *Blain* c. *Tawfik*, J.E. 96-379 (C.A.), C.A. Montréal, 500-09-000165-902.

164 Art. 1233 C.c.B.C.; *Landerman* c. *Landerman*, [1990] R.D.J. 542 (C.A.).

165 Art. 1234 C.c.B.C.; *Caisse Populaire Desjardins de St-Jacques* c. *Longpré*, J.E. 92-1199 (C.Q.), C.Q. Joliette 705-02-002376-911; *Nolin* c. *Bellavance*, [1979] C.A. 168, 173.

166 Art. 1244 C.c.B.C.; *McCallum* c. *Babineau*, [1956] B.R. 774, p.780; Art. 2867-2868 C.c.Q.

167 Art. 2866 C.c.Q.

168 J.-C. ROYER, *op. cit.* note 67, p. 1003, no 1622. Voir aussi *Tessier* c. *Ville de Québec*, [1979] R.P. 193 (C.S.); *Productions Serpent II inc.* c. *SOGIC*, J.E. 94-284 (C.S.), C.S. Montréal 500-05-013627-920.

C.c.Q. [169] prévoit d'ailleurs, référant à tout le chapitre deuxième du livre septième du C.c.Q. intitulé « Des moyens de preuve » que :

> « *Le tribunal ne peut suppléer d'office les moyens d'irrecevabilité résultant des dispositions du présent chapitre qu'une partie présente ou représentée a fait défaut d'invoquer.* »

Ces dispositions incluent tout particulièrement la règle de la meilleure preuve codifiée à l'article 2860 C.c.Q., une règle déjà traitée comme étant d'ordre privé sous l'ancien droit[170].

Ainsi, certaines règles de preuve intéressent l'ordre public, d'autres non. Des parties contractantes peuvent déroger aux secondes, non aux premières. Distinguer entre la renonciation constatée à la Cour, sous la forme d'un défaut d'objection, et la renonciation conventionnelle faite d'avance est inutile à l'égard des règles de preuve d'ordre public qui, dans tous les cas, pourront justifier l'intervention du tribunal. En effet, nos tribunaux d'appel ont déjà jugé qu'on ne pouvait renoncer d'avance à des dispositions d'ordre public (nullité absolue), ni même à des dispositions d'ordre public économique de protection (nullité relative), dans ce dernier cas, avant que la partie bénéficiaire n'ait acquis le droit ou le bénéfice découlant de ces dispositions et qu'elle soit en position de faire un choix éclairé[171].

Mais cela dit, peut-on reconnaître le droit d'une partie de renoncer devant la Cour à la sanction d'une règle de preuve d'ordre privé, tout en jugeant invalide la Convention préalable en vertu de laquelle cette partie convient d'avance de renoncer à la sanction de cette règle d'ordre privé? Nous croyons que non et que l'aménagement contractuel de règles de preuve en vue de la résolution de différends potentiels n'est pas, en soi, contraire à l'ordre public. En effet, on doit d'abord reconnaître que le décalage

---

169 L'introduction de l'art. 2859 C.c.Q. laisse peu de doute quant à l'intention du législateur de confirmer le droit antérieur à ce sujet. Dans son commentaire concernant l'art. 2859 C.c.Q., le ministre de la Justice déclare : « Cet article prescrit une règle bien établie en droit antérieur. Des considérations pratiques justifient son maintien. En effet, elle empêche l'ouverture, devant les tribunaux d'appel, de nouveaux débats sur des questions de preuve, puisque le défaut d'objection rend recevable la preuve offerte. Cette règle ne s'applique toutefois pas dans le cas où l'irrégularité de preuve porte atteinte à l'ordre public, ni en l'absence de la partie qui aurait intérêt à soulever l'illégalité d'une preuve offerte »; *Commentaires du ministre de la Justice*, t. 2, Québec, Publications du Québec, 1993, sous l'art. 2859 C.c.Q., p. 1791.

170 L. DUCHARME, *op. cit.*, note 67, p. 392, note 1321.

171 *Garcia Transport Ltée* c. *Cie Trust Royal*, [1992] 2 R.C.S. 499; J.L. BAUDOUIN, P.G. JOBIN, *op. cit.*, note 131, p. 172.

dans le temps de l'exercice du droit de renoncer à une règle de preuve ne change rien au caractère privé de cette règle et ne devrait pas davantage affecter la légalité de ce droit. Précisons ensuite qu'il n'est ici aucunement question de renonciation au droit d'une partie de demander la nullité de la Convention en cas d'un vice de consentement ou d'autres défauts de formation du contrat. Ce droit n'est pas en cause. De même, une partie à la Convention pourra toujours demander que soit frappée de nullité toute dérogation conventionnelle qui serait abusive, s'il devait s'agir d'un contrat d'adhésion par exemple, considérant là un droit d'ordre public consacré à l'article 1437 C.c.Q. Ces précisions paraissent utiles pour répondre aux préoccupations exprimées par les auteurs précités et rappeler que la Convention est un contrat et que sa reconnaissance comme telle l'assujettit aux mêmes régimes de sanction et de protection que ceux prévus pour tout autre contrat innommé, qu'il s'agisse de la sanction de vices de formation, d'abus de droit ou d'inexécutions contractuelles.

Mais plus fondamentalement, rappelons que les principes de l'autonomie de la volonté et de la liberté contractuelle constituent la règle et ont prédominance sur le principe de l'ordre public[172]. Ces principes doivent s'appliquer de la même façon au commerce électronique et l'étude du *Code civil du Québec* ou d'initiatives législatives internationales le confirme. À titre d'exemple, il est révélateur de noter que la *Loi type de la Commission des Nations-Unies pour le droit commercial international sur le commerce électronique* (la « *Loi type* »)[173] reconnaît spécifiquement, à son article 4, le principe de l'autonomie de la volonté et de l'élaboration d'un cadre contractuel privé pour régir la communication des messages de données[174] entre parties engagées dans le commerce électronique. Ces parties sont ainsi libres de convenir de règles relatives à la reconnaissance des messages de données ou de référer en la matière aux règles minimales proposées par la *Loi type*. Cette approche reconnaît, en pratique, que la solution aux difficultés que soulève l'utilisation de l'Internet se trouve facilitée par des accords contractuels. Plus spécifiquement, en matière de signature, l'article 7(1)(b) de la *Loi type* stipule que l'évaluation de la fiabilité de la signature électronique se fait « *compte tenu de toutes les circonstances, y compris de tout accord à la matière* ». De même, dans son

---

172 J.L. BAUDOUIN, P.G. JOBIN, *op. cit.*, note 131, p. 154, no 132.

173 *Infra*, section 2.2.2.1.

174 Le terme « message de données » désigne l'information créée, envoyée, reçue ou conservée par des moyens électroniques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l'échange de données informatisées, la messagerie électronique, le télégraphe, le télex et la télécopie.

projet de *Règles uniformes sur les signatures électroniques*[175], la Commission des Nations-Unies affirme, à l'article 5, qu'il « *est possible de déroger aux présentes Règles ou [de les modifier] [d'en modifier l'effet] par convention, à moins que lesdites Règles ou la loi de l'État adoptant en disposent autrement* »[176].

Le recours à la Convention privée trouve également appui au Canada dans la *Loi uniforme sur le commerce électronique* proposée par la Conférence pour l'harmonisation des lois au Canada[177], notamment en matière de signature électronique où la fiabilité des méthodes de signature doit s'établir « *à la lumière de toutes les circonstances, y compris toute entente pertinente...* »[178]. Il en est de même aux États-Unis[179].

Au Québec, dans le *Code civil du Québec* ou son prédécesseur, le *Code civil du Bas-Canada*, rien n'interdit la conclusion d'une Convention relative à la preuve, le législateur s'étant plutôt préoccupé de certaines règles de preuve particulières qu'il a formulées pour ne laisser aucun doute quant au fait qu'elles ne souffriraient aucune dérogation contractuelle. Quant aux tribunaux québécois, ils ne se sont guère prononcés sur la question à ce jour, si ce n'est en matière d'arbitrage et, dans ce cas, pour reconnaître depuis plus de 15 ans la validité de la clause compromissoire et le droit des parties de choisir des règles de droit substantif, incluant les règles de preuve qui leur conviennent[180]. Il suffirait donc aux parties d'adhérer à une clause compromissoire et d'y incorporer le dispositif de la Convention relatif à la preuve pour disposer de tout doute, s'il en demeure, quant à la validité de ce dispositif. D'ailleurs, le recours à l'arbitrage en

---

175 *Infra*, section 2.2.2.2.

176 *Infra*, section 2.2.2.2, Règles, art. 5.

177 *Infra*, section 2.2.2.3.

178 *Infra*, section 2.2.2.3, *Loi uniforme sur le commerce électronique*, art. 8(b).

179 Consulter à ce sujet, entre autres, le *Uniform Electronic Transactions Act* du National Conference of Commissioners on Uniform State Laws adoptée en août 1999. L'art. 5 de ce projet de loi uniforme américain stipule, au par. 5(d) « *Except as otherwise provided in this [Act], the effect of any of its provisions may be varied by agreement. The presence in certain provisions of this [Act] of the words "unless otherwise agreed" or words of similar import, does not imply that the effect of other provisions may not be varied by agreement.* »

180 *Condominiums Mont St-Sauveur* c. *Les Constructions Serge Sauvé*, [1990] R.J.Q. 2783; *Zodiak International Productions* c. *The Polish People's Republic*, [1983] 1 R.C.S. 529; Voir plus généralement, quant au caractère privé de l'arbitrage, A. REDFERN, M. HUNTER, M. SMITH, *Law and Practice of International Commercial Arbitration*, 2e éd, London, Sweet and Maxwell, 1991, p. 3; R. MERKIN, *Arbitration Law*, LLP, 1991, chap. 1.

matière de commerce électronique est logique et certes souhaitable compte tenu du caractère transnational d'Internet.

Cette référence à l'arbitrage révèle un autre argument militant pour la Convention. En effet, il est de ces matières où le droit doit prendre acte de la réalité du marché, des pratiques et des usages qui y prévalent. Le droit, tout comme l'ordre public, est dynamique et ne peut être figé[181]. Cet énoncé est bien incarné au Québec par la reconnaissance de l'arbitrage privé, un mode de résolution des conflits qui serait aussi vieux que le commerce :

> « *Commercial arbitration must have existed since the dawn of commerce. All trade potentially involves disputes, and successful trade must have a means of dispute resolution other than force. From the start, it must have involved a neutral determination, and an agreement, tacit or otherwise, to abide by the result, backed by some kind of sanction. It must have taken many forms, with mediation no doubt merging into adjudication. The story is now lost forever. Even for historical times it is impossible to piece together the details, as will readily be understood by anyone who nowadays attempts to obtain reliable statistics on the current incidence and varieties of arbitrations. Private dispute resolution has always been resolutely private.* »[182]

Or, à ce sujet, les propos de l'honorable juge Rothman dans l'affaire *Condominiums Mont St-Sauveur*[183] nous rappellent le caractère évolutif du concept d'ordre public.

> « *In Zodiac, the Supreme Court held that arbitration clauses under which the parties agreed to submit their disputes to binding arbitration, to the exclusion of the courts, were not against public order and were valid. It further held that the existence of such a clause was sufficient to remove the dispute from the jurisdiction of the courts.*
>
> *The Zodiac decision therefore represented not only a more liberal approach to the scope and use of arbitration agreements. It represented, as well, a significant evolution of the concept of "public order" in relation to arbitration clauses.*

---

181 À titre illustratif, J.-L. BAUDOUIN : « La protection du consommateur et la formation des contrats civils et commerciaux », (1975) 35 *R. du B.* 31, 42-43; P.G. JOBIN. « La rapide évolution de la lésion en droit québécois », (1977) 29 *Rev. Int. Droit comp.* 331, 336-337.

182 H. MUSTILL, « Arbitration: History and Background », (1989) 6 *Journal of International Arbitration*, p. 43.

183 Précitée, note 180, p. 2789.

> *The notion of "public order" is not an immutable concept. Nor does it involve the same requirements in every context.*
>
> *Some rules of public order are, by their nature, only susceptible of application or enforcement by the ordinary courts. It is difficult to imagine, for example, questions of criminal responsibility or the granting of a divorce, or a question of paternity, being decided by arbitration. The public order component goes directly to the jurisdiction of the body that is to decide the dispute.*
>
> *On the other hand, there are rules of public order that can be applied in arbitrations as easily and as appropriately as they are by courts. Building codes, zoning by laws, decrees in labour matters and other similar regulatory rules are all rules of public order. In a construction dispute, for example, arbitrators might well be obliged to apply the regulations under a building code when making their award. Or in the arbitration of a labour grievance, an arbitrator might well have to apply the regulations under a decree affecting a particular industry. The fact that these regulations are of public order does not deprive the arbitrators of their jurisdiction to hear the disputes or require that they be heard by the ordinary courts. »*

L'intégration de régimes privé et public en vue de résoudre efficacement un différend commercial ne devrait pas être à sens unique. Qui plus est, la reconnaissance d'une telle liberté contractuelle en matière de preuve correspondrait aux pratiques commerciales déjà reconnues dans le cadre d'échanges de documents informatisés. En effet, on constate aujourd'hui la reconnaissance à l'échelle internationale de contrats d'EDI contenant, au plan juridique, des dispositions relatives à la signature, la transmission de données, la confidentialité, la preuve, la force probante ainsi qu'à la conservation de documents électroniques. Il s'agit de conventions relatives à la preuve et à l'archivage de données dont la légitimité a, *de facto*, été reconnue.

En 1980, la Chambre de Commerce Internationale adoptait les *Règles de conduite uniformes pour l'échange de documents commerciaux par télétransmission,* désignées sous l'acronyme U.N.C.I.D. L'objectif de ces règles était de « *faciliter l'échange de données commerciales par télétransmission, en mettant à la disposition des parties engagées dans cette transmission, des Règles de Conduite acceptées par elles* »[184]. Ces Règles prévoient un régime spécifique relatif à la conservation des données

---

184 Règles de conduite uniformes pour l'échange de données commerciales par télétransmission, publiée par *La Chambre de Commerce Internationale*, Publications CCI n° 452, janvier 1988, art. 1.

et jouiraient d'une valeur juridique certaine, ou semi-légale[185]. Elles constitueraient une norme de base pouvant entrer dans le champ des règles juridiques et acquérir un caractère juridique obligatoire dans l'éventualité où nos tribunaux choisissaient de prendre « *à témoin une norme d'autoréglementation afin de juger d'un comportement* [et de chercher] *une façon de légitimer une décision en l'appuyant sur l'expertise de ceux qui ont développé la norme spécialisée* »[186].

S'il est bien vrai que la légalité d'un contrat ne résulte pas de son existence ou de sa popularité dans les milieux d'affaires concernés, on ne peut pour autant nier une convergence du droit et du commerce et la nécessité d'une telle convergence dans le cyberespace. À notre avis, cette convergence est inévitable et nos tribunaux voudront donner effet, avec encore moins de réticence dans le cyberespace que dans le mode tangible, à l'autoréglementation, aux normes volontaires, aux règles de l'art ou aux usages légitimes et raisonnables entre partenaires commerciaux. Là encore, il nous semble que l'évolution prévisible constituera une confirmation de la légalité de la Convention négociée pour disposer du « *risque de la preuve* »[187] dans le cyberespace.

Enfin, on ne pourrait conclure sans rappeler que la Convention ne constitue pas un contrat de consommation ni un contrat d'adhésion[188], réduisant du coup tant les risques d'abus et de déséquilibre obligationnel à l'origine d'un bon nombre de règles d'ordre public, que les préoccupations des auteurs en matière de preuve.

De tout ceci, nous concluons que la légalité de la Convention devrait être reconnue suivant le droit québécois. Il est entendu que les parties contractantes devront arrimer le contenu de la Convention aux exigences légales en matière d'archivage et en évaluer les effets, au terme de la négociation, en tenant compte des règles de preuve d'ordre public susceptibles d'intervenir suivant les termes négociés et l'objet de la transaction commerciale. À cet égard, l'élaboration du dispositif de la Convention relatif

---

185 Selon P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *op. cit.*, note 67, p. 103. Les règles U.N.C.I.D. ont acquis « une valeur juridique certaine par leur inclusion dans plusieurs contrats d'EDI et servent notamment de standard dans les conditions générales de télétransmission telles l'UN/EDIFACT, d'ODETTE, de CEFIC et de DISH ».

186 P. TRUDEL, « Les effets juridiques de l'autoréglementation », (1989) 19 *R.D.U.S.*, p. 247.

187 A. LUCAS, « Le droit de l'informatique », dans *Presses Universitaires de France*, Paris, Éd. Thémis, 1994, p. 382.

188 En effet, la Convention intervient entre partenaires commerciaux, en amont des consommateurs, dans un cadre où les stipulations essentielles qu'elle comporte sont librement discutées. Il ne pourrait ainsi s'agir de contrat d'adhésion ou de consommation au sens des art. 1379 ou 1384 C.c.Q.

à la preuve à l'intérieur d'un pacte compromissoire pour l'arbitrage de différends nous paraît souhaitable, bien que non nécessaire, dans le cyberespace.

1.2.2.2 Une Convention en phase avec la réalité du cyberespace

Tout outil, que ce soit celui du menuisier ou du chirurgien, n'est efficace que s'il est adapté aux circonstances. Or, nous savons qu'Internet est un environnement en constante mutation sous l'effet des pressions commerciales et technologiques qui s'y exercent. Aussi, un outil de gestion des risques doit nécessairement être souple, en phase avec la réalité du cyberespace et conçu pour fonctionner au-delà des frontières géographiques et géopolitiques.

Les avenues traditionnelles d'encadrement du risque juridique sont connues[189] et comprennent, notamment, le droit étatique, les normes internationales, les usages et pratiques, la réglementation judiciaire, la certification, la réglementation par l'intervention d'un organisme autonome ou encore l'institution d'un régime d'autoréglementation. C'est ce dernier régime qui nous intéresse tout particulièrement en regard de la Convention.

L'autoréglementation « fait référence aux normes volontairement développées et acceptées par ceux qui prennent part à une activité »[190]. Elle s'impose par l'adhésion d'une masse critique d'intervenants et sous-entend l'élaboration de règles et d'usages justes et équitables. « Elle est fondamentalement de nature contractuelle »[191] et présuppose un assujettissement volontaire en raison des avantages qu'elle procure. On dira que l'autoréglementation « joue un rôle indirect important dans l'application du droit » en ce que ces normes autoréglementaires peuvent acquérir une « force juridique par une décision d'autorité. Soit que le législateur trouve plus commode d'y référer dans ses textes, soit que le tribunal y trouve un corpus pratique lui décrivant ce qu'il faut faire en certaines circonstances »[192]. Pierre Trudel explique en ces termes ce mécanisme de réception des normes d'autoréglementation :

---

189 P. TRUDEL, F. ABRAN, K. BENYEKHLEY, S. HEIN, *op. cit.*, note 44, Les techniques de réglementation, pp. 3-1 et ss.

190 P. TRUDEL, « Introduction au droit du commerce électronique sur l'Internet », (1995) 55 *R. du B.* 521, 539.

191 *Ibid.*

192 P. TRUDEL, *loc. cit.*, note 186, p. 247.

> « *En raison de leurs origines, généralement intimement liées à la pratique et à l'expertise technique, les normes autoréglementaires fournissent, bien que cela ne soit pas leur finalité première, les préceptes de savoir-faire à partir desquels les tribunaux pourront juger les comportements.*
>
> *Le droit étatique ne peut s'appliquer en dehors de toute référence aux bonnes pratiques techniques ou aux bons comportements.* »[193]

On constate aujourd'hui que l'autoréglementation constitue une voie privilégiée dans le cyberespace. Les opérateurs de groupes de discussions et de babillards électroniques obtiennent l'adhésion des internautes à des politiques relatives à l'accès et au comportement « en ligne ». La majorité des institutions d'enseignement de niveau supérieur se sont dotées de politiques délimitant les droits et prérogatives de ceux qui font usage des capacités informatiques de ces institutions[194]. Des communautés d'usagers de réseaux interconnectés se dotent d'*Acceptable Use Policies*[195], soit des normes définissant des usages acceptables ou proscrits auxquels l'usager doit adhérer afin de conserver son accès au réseau. S'ajoutent les commandements de la « netiquette », sorte de règles d'éthique ou de civisme prévalant dans les groupes d'échanges collectifs articulés autour de sujets particuliers[196]. En juin 1999, une Cour supérieure reconnaissait d'ailleurs pour la première fois au Canada le caractère obligationnel des règles de la netiquette interdisant, dans le cadre d'un contrat de fourniture d'accès, le recours préjudiciable au *spamming* à des fins de marketing[197].

Pensons également aux fournisseurs d'accès et de services Internet, gestionnaires des points d'entrée sur les inforoutes, qui élaborent aujourd'hui des codes de conduite qui s'imposent contractuellement à leurs clients, sous peine de perte ou de suspension de leurs droits d'accès[198]. La décision de l'Association canadienne des fournisseurs Internet de publier un code de conduite pour ses membres est une initiative

---

193 *Id.*, pp. 285-286.

194 P. TRUDEL, *op. cit.*, note 190, p. 540.

195 P. TRUDEL, F. ABRAN, K. BENYEKHLEF, S. HEIN, *op. cit.* note 44, pp. 3-58.

196 *Id.*, pp. 3-62; A. RINALDI, *The Net: User Guidelines and Netiquette,* disponible au site http://www.enid.org/enidscools/co/enidhigh/internet.

197 *1267623 Ontario Inc.* v. *Nexx Online Inc.*, [1999] O.J., n° 2246, Ontario Superior Court of Justice, 14 juin 1999.

198 Pour une analyse des politiques des fournisseurs d'accès américains, voir http://www.cdt.org/privacy/online-services/chart.html.

dans cette direction[199]. On ne peut davantage ignorer l'apparition de mécanismes consensuels de résolution des différends dans le cyberespace, des *Virtual Magistrate* qui se veulent souples et adaptés aux réalités technologiques. Ces mécanismes témoignent d'une forme d'autoréglementation et procèdent de conventions compromissoires ou de médiation. Le recours à ces autorités d'adjudication plutôt qu'aux tribunaux étatiques s'explique en partie en raison des difficultés posées par la dématérialisation[200].

La popularité de ces régimes d'autoréglementation s'explique, entre autres, par référence au caractère a-national ou transnational d'Internet. Nous savons que le cyberespace est livré à l'application simultanée d'une pluralité de règles d'origines diverses[201]. La juxtaposition de ces règles est cause d'ambiguïtés et de contradictions, donc d'incertitude et de concurrence dans le cyberespace, « aucune autorité ne (pouvant) prétendre exercer un monopole sur la fonction d'énonciation des règles de même que sur celle reliée à leur application »[202]. Cet environnement, qui serait « ni le vide, ni le plein, mais l'enfer » [203], favorise donc la prise en charge par l'internaute des règles claires et prévisibles. L'autoréglementation est affranchie des limites d'un État et permet de s'arrimer au concept de communauté virtuelle[204] et « d'aborder les problèmes juridiques en fonction du cadre normatif le plus souple »[205].

---

199 Il faut reconnaître que ce code est à ce point général qu'il n'offre aucune solution immédiate aux fournisseurs aux prises avec une plainte selon laquelle l'un de leurs utilisateurs viole un droit d'auteur.

200 Selon T. E. HARDY, parlant des tribunaux virtuels : *How such a court would work mechanically is not entirely clear at this point, but the desirability of such action for just such circumstances as we are now discussing seems indisputable. The capability of communications networks is rapidly growing; almost certainly audio and full-motion video will be routinely available for cyberspace users in a matter of few years. It is easily possible to imagine on-line cyberspace hearings, with judges, juries, attorneys and whatever assortment of bailiffs and observers might be appropriate. The sanctions imposed could be usual private association sanction of expulsion or suspension from the relevant part of cyberspace.* T.E. HARDY, The Proper Regime for Cyberspace (1994-95) University of Pittsburg, L.R. 993, 1052-1053, cité dans P. TRUDEL, F. ABRAN, K. BENYEKHLEF, S. HEIN, op. cit., note 44, p. 3-43.

201 P. TRUDEL, F. ABRAN, K. BENYEKHLEF, S. HEIN, *op. cit.*, note 44, chapitre 3; J.R. REIDENBERG « L'instabilité et la concurrence des régimes réglementaires dans le cyberespace » dans *Les incertitudes du droit*, sous la direction de E. MACKAAY, Montréal, Éd. Thémis, Faculté de droit de l'Université de Montréal, p. 135.

202 P. TRUDEL, F. ABRAN, K. BENYEKHLEF, S. HEIN, *op. cit.*, note 44, p. 3-11.

203 J.R. REIDENBERG, *loc. cit.*, note 100, p. 137 reprenant A. BENSOUSSAN, *Internet : aspects juridiques*, Paris, Hermès, 1997, p. 11.

204 J. HAGEL III, A.G. ARMSTRONG, *Net Gain, Expanding markets through virtual communities*. Harvard Business School Press, 1997.

205 P. TRUDEL, F. ABRAN, K. BENYEKHLEF, S. HEIN, *op. cit.*, note 44, p. 3-38; J.R. REIDENBERG, *loc. cit.*, note 100.

Comment alors constater l'existence et la popularité de régimes d'autoréglementation dans le cyberespace sans conclure, à l'instar de Pierre Trudel[206], que le contrat est et doit demeurer un véhicule fondamental des règles du jeu dans Internet :

> « *Le consentement ou la faculté de le retirer qui réside dans le chef de l'usager paraît constituer un principe régulateur central dans l'Internet. L'importance de la concurrence entre les sites au plan de la régulation explique le rôle central que le contrat est appelé à jouer dans les environnements électroniques. Pour Robert Dunne, c'est même un véhicule normatif tout à fait approprié à ce qu'il perçoit comme étant la culture du cyberespace; il écrit :*
>
> « *Contract's traditional reliance on agreement by the individuals to be bound retains the element of individual responsibility that is an integral part of cyberian culture. Contract law permits localized enforcement mechanisms, dispensing with the need for a massive and complex central enforcement scheme. Furthermore, contract law, since it is enforced by agreement, transcends the problem of national borders. Contract in short, is a form of self-enforced law very much in keeping with the traditions and expectations of cyberians. It is far more likely to generate compliance than externally imposed and administered laws.* » »

Pour ces auteurs, le contrat définit un paradigme distinct au centre de la problématique de la réglementation des environnements électroniques, au point où il pourrait se développer une pratique de contrats-types dans un champ d'activité[207] servant de standard *de facto*. Selon Pierre Trudel[208] :

> « *Dans une large mesure, la proposition voulant que le régime juridique des environnements électroniques repose sur la loi des parties, le contrat, tend à illustrer la forte tendance vers l'autoréglementation qui est observée présentement. Plusieurs auteurs prédisent d'ailleurs que le régime juridique qui gouvernera les espaces électroniques sera en grande partie similaire à la lex mercatoria du Moyen-Âge, à savoir qu'il reposera sur un ensemble de coutumes commerciales élaborées et acceptées par tous, et appliquées en marge des institutions judiciaires traditionnelles. Les pratiques contractuelles suivies par les participants seront*

---

206 P. TRUDEL, *loc. cit.*, note 190, pp. 536-537 citant l'extrait de R.L. DUNNE, « Deterring Unauthorized Access to Computers : Controlling Behavior in Cyberspace Through a Contract Law Paradigm », (Fall 1994) 35 Jurimetrics Journal 1-15, p. 12, disponible à http://www.cs.yale.edu/pub/dunne/jurimetrics.html.

207 P. TRUDEL, *loc. cit.*, note 190, p. 538.

208 P. TRUDEL, F. ABRAN, K. BENYEKHLEF, S. HEIN, *op. cit.*, note 44, pp. 3-42.

vraisemblablement appelées à jouer un rôle prépondérant au chapitre de l'élaboration de ce régime juridique qui reste encore à être défini. Il pourrait également en être de même de la doctrine et de la jurisprudence, ainsi que des recommandations ou des codes-modèles adoptés par des institutions internationales spécialisées. »

Dans tout régime de concurrence, les lois du marché déterminent ultimement le modèle susceptible de s'imposer. Les marchés virtuels actuels ont déjà fait une place importante à l'approche consensuelle, sans attendre ni souhaiter l'interventionnisme étatique et le recours à la Convention s'en trouve facilité. Il s'agit, à notre avis, d'un outil de gestion pleinement compatible à la réalité du commerce électronique dans le cyberespace. L'émergence d'une autorité centrale, ou de régimes étatiques exclusifs au commerce électronique est évoquée[209] tant pour répondre aux lacunes de systèmes juridiques nationaux incompatibles et concurrents que pour questionner la pérennité d'une solution conventionnelle. On rappellera cependant que l'entreprise ne peut guère attendre le dénouement du long processus qui mène à la ratification éventuelle de traités internationaux et que l'interventionnisme réel ou appréhendé de l'État est un incitatif puissant à l'autoréglementation; à notre avis, la volonté d'adhérer à des normes croît avec le risque d'imposition de règles de droit strictes[210].

1.2.2.3 Une Convention négociée et adaptée à la spécificité des parties

L'utilité de la Convention pour disposer des problèmes de conservation et de preuve de documents électroniques dépend de son adaptation aux situations juridiques particulières prévalant entre cocontractants. Si l'apparition de clauses types et normatives est à prévoir, il faut rappeler que l'avantage premier de la Convention est de permettre aux parties d'exercer leur liberté contractuelle et de se doter de règles d'ordre privé utiles au développement durable de leurs affaires. Comme nous le verrons, la Convention repose en grande partie sur l'établissement d'équivalences fonctionnelles entre un monde papier et son droit positif, et un monde dématérialisé et ses incertitudes juridiques. Le processus de définition de ces équivalences fonctionnelles est l'occasion pour les parties de convenir librement, à titre d'exemple, de règles d'admissibilité en preuve de la signature numérique ou d'une copie électronique en tenant compte des caractéristiques de

---

209 Consulter à ce sujet le Rapport de la délégation canadienne sur la trente-quatrième session du Groupe de travail de la CNUDCI sur le commerce électronique, disponible au site http://canada.justice.gc.ca/Commerce/un99gau_fr.html.

210 À titre d'exemple, référence peut être faite à la publicité, l'intervention de l'État et l'autoréglementation concernant les jouets pour enfants.

leurs rapports commerciaux. C'est la négociation d'une Convention adaptée concrètement à la gestion des risques qui la distingue des autres outils normatifs. C'est pourquoi nous passerons maintenant à l'étude des lignes directrices dans l'architecture de la Convention.

2. L'ÉLABORATION DE LA CONVENTION RELATIVE À LA PREUVE ET À LA CONSERVATION DE DOCUMENTS ÉLECTRONIQUES D'ENTREPRISE

Les parties à la Convention devront convenir de principes à partir desquels le contenu obligationnel de la Convention pourra être échafaudé de façon cohérente. Ces règles s'imposeront pour l'atteinte des objectifs stratégiques des contractants et serviront de lignes directrices qu'il leur faudra considérer afin d'assurer la légalité de la Convention et son arrimage avec un corpus législatif concernant la conservation et la preuve électronique. Or, l'analyse révèle que ces règles constituent toutes des manifestations d'un même principe directeur, un principe de conformité à la loi, aux finalités poursuivies ainsi qu'aux régimes normatifs actuels ou proposés pour régir le commerce électronique. Ces trois volets distincts d'un même principe de conformité sont discutés à la section suivante.

2.1 LE PRINCIPE DE CONFORMITÉ DANS L'ARCHITECTURE DE LA CONVENTION

2.1.1 La conformité aux exigences légales applicables

Le principe de conformité exige des parties contractantes qu'elles exercent légalement leur liberté contractuelle suivant des règles de droit substantif leur reconnaissant cette autonomie[211]. En matière d'archivage, les parties devront arrimer le contenu de la Convention aux prescriptions statutaires pertinentes[212]. En matière de preuve, elles tiendront compte des exigences légales en vigueur, s'il en est, concernant la preuve de documents électroniques[213] et des règles d'ordre public susceptibles d'intervenir[214].

---

211 *Supra*, section 1.2.2.1.

212 *Supra*, section 1.1.3.3.

213 Nous verrons, par exemple, que le régime de preuve d'actes juridiques codifié aux articles 2837 à 2839 C.c.Q. est particulièrement pertinent à la Convention si le droit québécois s'applique. Il en est de même du régime de reproduction de documents visé aux articles 2840 à 2842 C.c.Q. ou encore du régime fédéral mis en place par le *Projet de loi C-6* à l'égard de la reconnaissance et de la preuve du document électronique.

214 *Supra*, section 1.2.2.1. Les parties pourront chercher l'appui du droit régissant l'arbitrage s'il leur paraît opportun d'intégrer le dispositif de la Convention relatif à la preuve dans un pacte compromissoire.

2.1.2 La conformité aux finalités poursuivies

La finalité de la Convention s'articule autour du concept de valeur du document pour l'entreprise. Le document n'a de valeur et son archivage d'intérêt que si le document sert utilement, le moment venu, aux fins pour lesquelles il existe. Il s'agit globalement d'une question de gestion[215], de preuve[216] et de conformité à la loi[217]. Ce premier niveau d'analyse doit cependant être précisé à l'étape de l'élaboration de la Convention. Aussi, les parties auront intérêt à identifier des catégories de documents correspondant à leur réalité d'affaires et à juger au préalable de la finalité de leur conservation. Ce faisant, elles tiendront compte de la spécificité de leur relation, des pratiques de l'industrie et des risques d'un défaut de conservation. Cette gestion de l'incertitude les obligera à jauger leur vulnérabilité technologique. L'approche microscopique au plan de la finalité permet d'identifier les obstacles prévisibles à l'application des notions d'écrit, d'original ou de signature en fonction des catégories de documents identifiées et de prioriser les investissements.

La Convention doit également être conçue pour satisfaire aux finalités recherchées dans une perspective à plus long terme. Elle doit être négociée pour gérer des risques associés au commerce, aux documents et à l'archivage électroniques alors même que ces risques peuvent ne pas avoir été pleinement perçus au moment de la transaction commerciale. La Convention doit donc reconnaître l'évolution prévisible du droit, des technologies et des besoins des contractants.

2.1.3 La conformité aux régimes normatifs actuels ou proposés pour régir le commerce électronique

Ce volet du principe de conformité vise en premier lieu la compatibilité de la Convention aux régimes normatifs actuels ou proposés pour régir ou uniformiser le traitement réservé aux documents électroniques. D'importantes initiatives législatives ont été prises au Canada et ailleurs[218] afin de favoriser ce que d'aucuns considèrent comme l'avènement d'un nouveau paradigme commercial. Ces initiatives phares prises par des

---

215 *Supra*, section 1.1.3.1.

216 *Supra*, section 1.1.3.2.

217 *Supra*, section 1.1.3.3.

218 *Infra*, section 2.2.2.

organismes internationaux publics ou privés et par des législatures[219], sous forme de lois uniformes ou de projets de lois, ont en commun qu'elles veulent faciliter le commerce électronique en l'occultant de ce qui le mine le plus à l'heure actuelle, soit le défaut de sécurité des transactions et l'incertitude juridique. Des projets de lois en matière de certification[220], de protection de la vie privée[221], de preuve et de signatures électroniques[222] constituent des exemples concrets.

Ce principe de conformité conduit en second lieu à l'étude des usages et des pratiques commerciales pertinents aux documents électroniques[223]. Le souci d'harmoniser le contenu obligationnel de la Convention avec des normes prévalant dans l'industrie en général, ou dans le secteur d'activités dans lequel œuvrent les contractants, favorise l'adhésion *de facto* à la Convention et la reconnaissance de son caractère raisonnable, en cas de contestation.

2.2 DES OUTILS ET DES GUIDES D'APPLICATION DU PRINCIPE DE CONFORMITÉ AUX FINS DE L'ÉLABORATION DE LA CONVENTION

L'application de ce principe de conformité n'a pas à se faire dans l'abstrait, en présence d'exigences légales, d'initiatives législatives phares et de pratiques commerciales s'imposant déjà dans le cyberespace. C'est à ces guides d'application que nous nous attarderons dans la prochaine section afin de nous aider à formuler, en fin d'exposé, des recommandations concrètes aux parties contractantes.

2.2.1 Les dispositions pertinentes du *Code civil du Québec* ou le respect d'exigences légales applicables

Les parties assujetties au droit du Québec s'intéresseront aux dispositions du *Code civil du Québec* en matière de preuve et de conservation de documents

---

219 *Infra*, sections 2.2.2.3, 2.2.2.4 et 2.2.2.5 au Canada et dans les provinces de la Saskatchewan et du Nouveau-Brunswick.

220 Pour un inventaire détaillé des approches législatives en matière de certification, consulter l'Inventaire des Approches à l'égard de l'authentification et de la certification dans une société mondiale de réseaux, préparé par le Groupe d'experts sur la sécurité de l'information et la vie privée du Secrétariat au commerce électronique de l'OCDE, Rapport DSTI/ICCP/REG (98) 3/Rev3.

221 Au Canada, le *Projet de loi C-6* constitue un exemple d'intérêt. *Infra*, section 2.2.2.3.

222 Consulter à ce sujet le *Summary of Electronic Commerce and Digital signature legislation* disponible au site http://www.mbc.com/ecommerce/legis.

223 Voir, à titre d'exemple, les contrats d'EDI, *infra*, section 2.2.3.1.

électroniques. Nous avons évoqué précédemment[224] la distinction faite par les auteurs entre l'acte juridique et le fait matériel en regard de la preuve au moyen d'inscriptions informatisées. Les juristes auront noté la codification de ces régimes distincts au Livre septième du *Code civil du Québec*. Il importe maintenant de nous attarder davantage à ces régimes.

2.2.1.1 L'inscription informatisée comme moyen de preuve d'un acte juridique

L'article 2837 du *Code civil du Québec* se lit comme suit :

> *« Art. 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. »*

Cet article, qui vise les données de l'acte juridique inscrites sur support informatique, donc en langage machine[225], ne précise pas si l'inscription doit nécessairement être concomitante de l'expression de la volonté des parties à l'acte, ni la façon dont il cohabite avec le formalisme imposé par des dispositions d'ordre public relatives à certaines transactions particulières. L'article 2837 C.c.Q. ne s'attarde pas davantage à la qualité civile ou commerciale des parties, contrairement aux règles qui prévalaient sous l'ancien *Code civil du Bas-Canada*[226], affranchissant du coup le plaideur d'un passé lourd en débats jurisprudentiels articulés autour de l'existence d'actes mixtes[227]. Il introduit « *un régime unitaire de preuve* »[228] et s'intéresse essentiellement au « document » qui, grâce aux données qu'il reproduit, fera preuve du contenu de l'acte juridique, à la condition qu'il soit intelligible et qu'il présente des garanties suffisamment sérieuses de fiabilité, sous réserve d'une preuve contraire permise « *par tous moyens* »[229].

---

224 *Supra*, section 1.1.3.2.

225 Selon la jurisprudence actuelle, la lettre télécopiée ne constitue pas une inscription informatisée mais un écrit instrumentaire sous seing privé. À titre d'exemple, consulter l'affaire *DuMay (1985) Inc.* c. *U.A.P.*, .C.Q. Longueuil 505-02-004177-964, 1997-02-28.

226 Art. 1233 C.c.B.-C.

227 G. LEFEBVRE, *loc. cit.*, note 67, p. 622.

228 G. LEFEBVRE, *loc. cit.*, note 67, p. 623.

229 Art. 2839 C.c.Q.

Certaines conclusions découlent de ce qui précède. Premièrement, le document visé à l'article 2837 C.c.Q. est une reproduction, que l'inscription informatisée résulte d'un acte juridique conclu directement par ordinateur[230] ou d'une transcription postérieure à la conclusion d'un acte juridique écrit ou verbal le constatant. Deuxièmement, la condition d'intelligibilité imposée à l'article 2837 C.c.Q. est déterminante[231] et commande une interprétation généreuse du mot « document » qui inclura, au-delà du support papier, « *toute forme de reproduction intelligible pour l'homme* »[232], notamment l'imprimé et l'affichage à l'écran. Enfin, les garanties de fiabilité exigées englobent les circonstances dans lesquelles les données ont été inscrites et le document reproduit, soit deux étapes distinctes séparées dans le temps par des activités d'archivage tout aussi distinctes.

Ces conclusions soulèvent des interrogations pertinentes à notre analyse des questions juridiques liées à la Convention. Le champ d'application de l'article 2837 C.c.Q. nourrit un débat chez les auteurs de doctrine. Cet article aurait-il pour effet d'écarter la règle de la meilleure preuve, d'abolir la hiérarchie établie des moyens de preuve et de placer sur un pied d'égalité le document d'origine et l'imprimé devant un tribunal?[233] À l'inverse, doit-on exclure du champ d'application de l'article 2837 C.c.Q. tout acte juridique par lequel la volonté des parties s'est d'abord exprimée verbalement ou par écrit, pour n'être consignée que postérieurement sous la forme d'inscriptions informatisées? Suivant cette seconde hypothèse, seule l'inscription concomitante à l'acte juridique serait couverte. C'est le cas, par exemple, d'un dépôt bancaire fait à un guichet automatique.

---

230 En matière d'EDI ou de certification en ligne, par exemple.

231 G. LEFEBVRE; *loc. cit.*, note 67, p. 626. Pour être intelligible, un document doit être accessible, clair et limpide selon le professeur Ducharme, s'appuyant en cette matière sur le Petit Robert 1; L. DUCHARME, *op. cit.*, note 67, p. 144, no. 476; F. CHAMPIGNY, « L'inscription informatisée en droit de la preuve québécois », dans *Développements récents en preuve et procédure civile (1996)*, Montréal, Ed. Y. Blais, p. 8.

232 P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *op. cit.*, note 67, p. 24.

233 Selon C. FABIEN, « La communicatique et le droit civil de la preuve » *dans Le droit de la communicatique* – Actes du colloque des Facultés de droit de l'Université de Poitiers et de l'Université de Montréal, 1990, p. 186. « Certes, la meilleure preuve de l'acte sera la « facture » signée par le client. Toutefois, le nouveau Code ne nous semble pas imposer une hiérarchie des moyens de preuve qui rendrait irrecevable le listage informatisé de la même opération, sous réserve de la qualité de sa preuve d'authenticité. Au stade de la recevabilité, l'art. 2837 C.c.Q. nous apparaît comme une disposition autonome qui peut mettre en concurrence, devant le tribunal, un listage d'opérations et les factures originales qui ont été inscrites dans le système. »

Les tenants de la seconde hypothèse évoquent l'interdiction de preuve par ouï-dire contenue à l'article 2843 C.c.Q. et la règle de la meilleure preuve de l'article 2860 C.c.Q. pour limiter l'application de l'article 2837 C.c.Q. au véritable cas de substitution du support informatique au support papier, excluant par là le stockage d'informations[234]. Cette hypothèse trouve appui dans les propos de la Cour du Québec dans l'arrêt *Transport Dragon Limitée* c. *Mauro Grillo Excavation*[235].

Leurs contradicteurs[236] plaident plutôt l'existence d'exceptions déjà reconnues à ces règles de preuve en matière de documents d'entreprise[237], que ces « *business records* » aient été numérisés lors de la transaction ou par la suite. Ils rappellent aussi la réalité des affaires et des pratiques commerciales, du moins dans certains secteurs de l'industrie[238]. Ils ajoutent l'argument de texte selon lequel, en l'absence de toute limitation claire, l'expression « *lorsque les données d'un acte juridique sont inscrites sur support informatique* » de l'article 2837 C.c.Q. est suffisamment large pour englober tout acte juridique, quand bien même l'inscription des données contenues à l'acte serait postérieure à la conclusion de celui-ci.

---

234 L. DUCHARME, « Le nouveau droit de la preuve en matières civiles selon le Code Civil du Québec », [1992] 23 *R.G.D.* 5, pp. 37-38; voir aussi L. DUCHARME, *op. cit.*, note 67, p. 143, no. 465. Voir également au soutien de cette seconde hypothèse G. MASSE, « Du témoignage apparemment admissible à titre de ouï-dire au ouï-dire apparemment admissible à titre d'écrit », *dans Développements récents en preuve et procédure civile*, Cowansville, Éd. Y. Blais, 1996, p. 193. Le professeur J.C. ROYER, *op. cit.*, note 67, rejette le critère de la simultanéité entre l'acte et l'inscription informatisée mais s'appuie sur les articles 2859 à 2868 C.c.Q. pour limiter, voire exclure, sauf circonstances exceptionnelles prévues aux articles 2860, 2862 ou 2863 C.c.Q., le document reproduisant l'inscription informatisée postérieure à l'acte juridique conclu verbalement ou par écrit.

235 *Transport Dragon Limitée* c. *Mauro Grillo Excavation,* C.Q Montréal 500-22-006747-979, 1997-08-07 (97BE-844), p. 4. Dans cette affaire, le tribunal déclarait irrecevable un document informatisé émanant de l'Inspecteur général des institutions financières du Québec produit pour établir le lieu du siège social d'une entreprise, précisant que l'article 2837 C.c.Q. ne pouvait trouver application en l'espèce, citant à l'appui le professeur Ducharme qui exclut du champ d'application de cet article le stockage d'informations sur support informatique survenu postérieurement à l'expression des consentements à l'acte juridique.

236 C. FABIEN, *loc. cit.*, note 233, pp. 181 et ss.; P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *op. cit.*, note 67, pp. 22-23; G. LEFEBVRE, *loc. cit.*, note 67, p. 624; J.C. ROYER, *op. cit.*, note 67, p. 225, no. 406.

237 G. LEFEBVRE, *loc. cit.*, note 67, p. 624. Pour une discussion de la force probante des registres et factures de commerce sous l'ancien droit, voir L. LILKOFF, « La force probante des registres et factures de commerce », (1967-68) *C de D* 794.

238 G. LEFEBVRE, *loc. cit.*, note 67, p. 625. Un cas d'application à l'égard de documents comptables est donné par l'affaire *Zellers Inc.* et *Syndicat des employés et employées des magasins Zellers d'Alma et de Chicoutimi* [1998] RJDT (TA), J.E. 98T-1076.

Nous pouvons tenter de résoudre cette controverse en rappelant, comme le fait à juste titre Francine Champigny, que l'article 2837 C.c.Q. ne « *crée pas une règle de recevabilité* »[239], ces règles étant contenues au titre troisième du Livre de la preuve, mais constitue plutôt un nouveau moyen de preuve assimilable à un écrit[240]. Ainsi, cet article doit être lu et interprété à la lumière des règles concernant la recevabilité des moyens de preuve énoncées aux articles 2859 à 2868 C.c.Q. Précisons d'emblée, en ce qui concerne la règle du ouï-dire, que la question de la simultanéité de l'acte juridique et de l'inscription informatisée n'affecte en rien le fait que l'auteur de l'inscription, contemporaine ou simultanée, doit être la personne ou l'agent de la personne dont le consentement est recherché par l'inscription.

Il est vrai que l'article 2837 C.c.Q. n'exige pas explicitement la concomitance de la conclusion de l'acte et de l'inscription des données sur support informatique. Tirer une autre conclusion tendrait selon nous à privilégier la recherche d'un résultat sur l'interprétation adéquate d'un texte. Cela dit, l'inscription informatique postérieure à l'acte juridique n'est pas pour autant admissible; encore faut-il que ce nouveau moyen de preuve de l'acte juridique soit recevable dans les circonstances, compte tenu de l'existence ou non d'une preuve primaire :

> *« Lorsque l'acte a été conclu directement par ordinateur, l'inscription informatisée constitue en quelque sorte l'écrit visé à 2860 et est la preuve primaire. Si cet acte juridique a d'abord été constaté dans un écrit instrumentaire et transcrit par la suite sur ordinateur, l'écrit dont parle 2860 est nécessairement ce premier écrit, l'inscription informatisée constituant une preuve secondaire, à moins d'obéir aux conditions des articles 2840 et suivants concernant la reproduction de certains documents : dans un tel cas, elle a la même valeur que l'original et constitue la copie qui légalement en tient lieu à laquelle réfère l'article 2860, donc la preuve primaire.[...]*
>
> *C'est donc dire que l'inscription informatisée qui reproduirait les données d'un acte juridique constaté par écrit et détruit dans des circonstances autres que celles des articles 2840 et suivants ne pourrait être utilisée que dans le cas où la preuve secondaire est admise.[...]*

---

239 F. CHAMPIGNY, *loc. cit.*, note 67, p. 10.

240 L'article 2811 C.c.Q. énonce que la preuve d'un acte juridique peut être établie par écrit, par témoignage, par présomption, par aveu ou par la présentation d'un élément matériel. Or, l'article 2837 C.c.Q. fait partie du chapitre premier, au titre consacré à l'écrit. Le document visé par l'article 2837 C.c.Q. est un écrit qui relate un acte juridique.

> *Comme on peut le constater, les positions des professeurs Ducharme et Royer se rejoignent dans la mesure où, indépendamment du fait qu'ils incluent ou non un tel document dans ceux visés à 2837, ils en limitent tous les deux la recevabilité en raison de l'article 2860 C.c.Q* ».[241]

La référence au régime de reproduction codifié aux articles 2840 à 2842 C.c.Q. que nous verrons plus loin[242] soutient efficacement l'approche de cette auteure. En effet, ce régime confirme la supériorité d'une preuve primaire, en l'occurrence l'original papier, sauf si ce dernier est remplacé par une reproduction fidèle obtenue en conformité avec les exigences de l'article 2840 C.c.Q ou encore, si les conditions donnant droit à l'application de l'une ou l'autre des exceptions à la règle de la meilleure preuve prévues aux articles 2859 à 2868 C.c.Q. sont réunies. Au surplus, cette approche nous paraît conforme aux commentaires du ministre de la Justice[243].

De façon concrète, il sera important, à l'étape de l'élaboration de la Convention, de bien saisir les notions d'intelligibilité du document et de fiabilité des systèmes informatiques de saisie, de reproduction et de conservation des inscriptions informatisées. Ces notions risquent d'affecter les spécifications techniques, le choix des produits informatiques, des systèmes de sécurité physique de même que le contenu obligationnel de la Convention. Il faudra aussi connaître les politiques d'entreprise à l'égard de la conclusion d'actes juridiques et départager les documents électroniques d'origine de leurs transcriptions.

2.2.1.2 L'inscription informatisée comme moyen de preuve d'un fait matériel

Les articles 2837 à 2839 C.c.Q. ne s'appliquent qu'à l'acte juridique. C'est donc au régime général de la preuve qu'il faut se rapporter pour connaître les règles qui régissent la recevabilité de documents électroniques offerts au soutien de faits matériels.

---

241 F. CHAMPIGNY, *loc. cit.*, note 67, p. 11-12.

242 *Infra*, section 2.2.1.3.

243 En effet, les *Commentaires du ministre de la Justice*, *op. cit.*, note 71, nous révèlent à la page 1776 que l'art. 2837 C.c.Q. « n'a toutefois pas la même utilité pour les actes juridiques constatés d'abord dans un écrit avant d'être inscrit sur support informatique, compte tenu de la règle de la meilleure preuve et du fait que les documents reproduisant ces 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 les 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 ».

« L'inscription informatisée d'un fait matériel doit être assimilée à un autre écrit rapportant un fait matériel » nous dit le professeur Royer[244]. Ainsi, l'utilisation d'un document électronique pour, par exemple, « déterminer l'origine et la destination du message de données, ainsi que les indications de date et d'heure de l'envoi ou de la réception »[245], se heurte tant à la règle de l'interdiction du ouï-dire, qu'à celle de la meilleure preuve.

En matière d'ouï-dire, la tâche du plaideur était déjà allégée, sous l'ancien Code, par la reconnaissance d'exclusions spécifiques[246]. Cette tâche est facilitée davantage aujourd'hui par l'ajout de l'article 2870 C.c.Q. :

> *« Art. 2870. La déclaration faite par une personne qui ne comparaît pas comme témoin, sur des faits au sujet desquels elle aurait pu légalement déposer, peut être admise à titre de témoignage, pourvu que, sur demande et après qu'avis en ait été donné à la partie adverse, le tribunal l'autorise.*
>
> *Celui-ci doit cependant s'assurer qu'il est impossible d'obtenir la comparution du déclarant comme témoin, ou déraisonnable de l'exiger, et que les circonstances entourant la déclaration donnent à celle-ci des garanties suffisamment sérieuses pour pouvoir s'y fier.*
>
> *Sont présumés présenter ces garanties, notamment, les documents établis dans le cours des activités d'une entreprise et les documents insérés dans un registre dont la tenue est exigée par la loi, de même que les déclarations spontanées et contemporaines de la survenance des faits. »*

Le libellé de cet article de droit nouveau, qui n'est pas sans rappeler, par son troisième alinéa, celui de l'article 2838 C.c.Q., consacre une large exception à l'interdiction du ouï-dire. Cette exception devrait favoriser l'utilisation des documents électroniques dans la preuve de faits matériels. En effet, des dizaines, voire des centaines d'auteurs différents peuvent être à l'origine d'une banque de données attestant un fait matériel, et il devient aussi difficile et déraisonnable d'exiger l'identification du témoin

---

244 J.C. ROYER, *op. cit.*, note 67, p. 225, no 405.

245 Art. 10 de la *Loi type de la CNUDCI sur le commerce électronique. Infra*, section 2.2.2.3.

246 À titre d'exemple, mentionnons la production du rapport d'une institution financière sur l'état des dépôts et des placements d'une personne. Il en va de même pour certains listages générés de façon autonome par des ordinateurs capables de produire de l'information ignorée de tout autre témoin. Qui sait, l'avènement d'ordinateurs dotés d'une intelligence artificielle sera peut-être un jour suffisant pour permettre à ceux-ci de se qualifier à titre de témoins compétents s'exprimant par écran cathodique et listage électronique

compétent que de vouloir contre-interroger un ordinateur à ce sujet. L'existence de garanties sérieuses de fiabilité devient dès lors l'élément central, dont la preuve est facilitée par la présomption définie au troisième alinéa de l'article 2870 C.c.Q. Cette présomption touche une gamme impressionnante de documents électroniques produits dans le cadre de relations commerciales[247].

Quant aux contraintes imposées par la règle de la meilleure preuve, là encore le *Code civil du Québec* confirme certains allégements en permettant la copie d'un écrit « *lorsqu'une partie ne peut, malgré sa bonne foi et sa diligence, produire l'original de l'écrit ou la copie qui légalement en tient lieu* »[248]. Lefebvre illustre en ces termes l'application de l'article 2860 C.c.Q. dans le contexte de l'EDI :

> *« La règle de la meilleure preuve suppose généralement dans le cas des écrits que ceux-ci soient présentés dans leur version originale. Dans le contexte de l'EDI, le problème que soulève cette règle provient du fait qu'il est possible de soutenir que l'original en question est représenté par les données contenues dans l'ordinateur sous forme magnétique ou électronique, c'est-à-dire dans un langage incompréhensible pour le commun des mortels. Le listage ou l'imprimé sur support-papier ne constituerait qu'une transcription ou une copie normalement irrecevable en preuve. [...]*
>
> *Ainsi, il sera possible de faire la preuve de faits matériels si l'on démontre que, malgré sa bonne foi et sa diligence, une partie ne peut pas produire le document original. Dans le contexte informatique cité ci-dessus, l'original étant indisponible ou n'ayant jamais existé, cet article permettra donc d'apporter en preuve des documents informatisés pour prouver des faits matériels. »* [249]

Nous verrons que la décision d'une entreprise de ne pas conserver l'original d'un écrit reproduit sur support informatique lui fait tout probablement perdre l'innocence nécessaire pour invoquer avec succès le bénéfice du second alinéa de l'article 2860 C.c.Q.

---

247 G. LEFEBVRE, *loc. cit.*, note 67, p. 630.

248 Art. 2860 C.c.Q.

249 G. LEFEBVRE, *loc. cit.*, note 67, p. 631.

La Convention devra reconnaître l'importance des présomptions codifiées aux articles 2860 et 2870 C.c.Q. et faciliter leur application au soutien de l'admissibilité des documents électroniques[250].

2.2.1.3 Un régime de reproduction de documents sous forme numérique

Le *Code civil du Québec* innovait en janvier 1994 en édictant aux articles 2840 à 2842 C.c.Q. des normes minimales dont le respect confère à toute reproduction la même valeur juridique qu'un original, du moins selon les textes. Ainsi, le législateur québécois ouvrait libéralement la voie à l'utilisation de l'ordinateur comme moyen d'archivage électronique, un moyen particulièrement bien adapté compte tenu de sa capacité sans cesse croissante de stocker des données de façon économique. En agissant ainsi, le législateur élargissait à toute forme de reproduction les exceptions à la règle du ouï-dire et de la meilleure preuve limitées jusque-là aux reproductions sous forme de microfilms[251].

L'article 2840 C.c.Q. permet la reproduction d'un document par n'importe quel moyen, incluant donc la numérisation, pour autant que la technologie utilisée permette une reproduction fidèle et indélébile de l'original et la détermination du lieu et de la date de reproduction. Celle-ci doit être faite en présence d'une personne spécialement autorisée à cette fin par l'État ou la personne de droit public ou de droit privé voulant se prévaloir de ce régime. La personne ainsi désignée devra, dans un délai raisonnable suivant la reproduction, en attester la réalisation par une déclaration assermentée mentionnant la nature du document reproduit ainsi que le lieu et la date de reproduction, et en certifier la fidélité. Cette déclaration assermentée sera jointe à la copie de la reproduction qui tiendra alors légalement lieu d'original.

---

250 Nous distinguons évidemment admissibilité et force probante. La force probante d'inscriptions informatisées admises en preuve d'un fait matériel sera appréciée par le tribunal selon l'art. 2845 C.c.Q., s'il s'agit d'un témoignage, ou 2856 C.c.Q, s'il s'agit d'un élément matériel de preuve. La force probante des données d'un acte juridique visé à l'art. 2837 C.c.Q. pourra être contredite par tout moyen de preuve, contrairement à l'écrit sous seing privé qui fait foi de son contenu, sous réserve d'une preuve légale contraire.

251 *Loi sur la preuve photographique des microfilms de documents*, L.R.Q. c. P-22, abrogée avec l'entrée en vigueur du C.c.Q. en janvier 1994.

Ces normes, qui constituent des normes minimales[252] mais essentielles[253], ne font pas l'unanimité[254] et présentent certaines difficultés d'application. Le critère de l'indélébilité est problématique en raison des caractéristiques actuelles des supports magnétiques dont la vie utile demeure limitée[255]. De plus, la notion de délai raisonnable introduite à l'article 2841 C.c.Q. demeure arbitraire, en l'absence de balises jurisprudentielles définitives, même si les tribunaux ont déjà fait preuve d'ouverture. Ainsi, dans *Bleau* c. *Bélair, compagnie d'assurance*[256], la Cour supérieure eut à juger de l'admissibilité de la reproduction d'une proposition d'assurance souscrite en 1992, puis détruite dans le cadre de la politique d'archivage sur microfilm de l'entreprise. Aucune déclaration assermentée n'avait été réalisée à l'époque de la reproduction de l'original. La copie offerte à la Cour près de sept années plus tard était plutôt appuyée d'un affidavit attestant de la fidélité de la reproduction réalisée, non pas à partir de l'original détruit, mais du microfilm conservé pendant des années. Notant d'abord le long délai écoulé, la Cour s'appliquera à rechercher la fiabilité de la reproduction plutôt qu'à définir une norme stricte.

> *« (...)La seule difficulté repose sur les mots « délai raisonnable » contenus à l'article 2842.*
>
> *La défenderesse a produit au dossier, sous réserve d'une objection de la part du procureur du demandeur, un affidavit de monsieur Martin Côté, directeur de gestion des documents chez Bélair. Cet affiant déclare qu'il est une personne spécialement autorisée par Bélair pour procéder à la reproduction des propositions d'assurance et que le document microfiche produit en preuve reproduit fidèlement le microfilm de l'original de la proposition d'assurance du demandeur. Il ajoute cependant qu'il a effectué la reproduction le 24 mars 1999 en se servant uniquement du microfilm car l'original de la proposition n'existe plus.*

---

252 B. TROTTIER, *loc. cit.*, note 56, p. 781.

253 En effet, dans l'affaire *Banque Nationale du Canada* c. *Simard*, J.E. 96-1172 (C.Q.), la Cour a jugé irrecevable la preuve d'un contrat d'utilisation d'une carte de crédit en raison de la piètre qualité de la reproduction et l'absence des informations requises à l'article 2841 C.c.Q. Il en a été de même dans l'affaire *Otis* c. *Équipements J.G.M.*, C.Q. 155-32-000132-968, 1997-09-02, où la Cour déclarait irrecevable la photocopie d'un chèque puisque non accompagnée de la déclaration sous serment requise par l'art. 2842 C.c.Q. *Contra*, voir *Bleau* c. *Bélair, compagnie d'assurance*, *infra*, note 256.

254 L. DUCHARME, « Le nouveau droit de la preuve en matière civile selon le Code civil du Québec », dans *Réforme du Code civil*, Québec , Les Presses de l'Université Laval, 1993, pp. 445, 457.

255 *Supra,* note 62.

256 C.S.Q. 505-05-000614-948, 1999-05-04.

> *L'affidavit de monsieur Côté n'est pas celui qu'exige l'article 2842; il faut le reconnaître. Toutefois, le tribunal a entendu la preuve de deux personnes en autorité, Adrienne Pearson et Jocelyne Palardy qui ont pris part à la reproduction du document en mars 1992 et leur témoignage ne peut être ignoré.*
>
> *Le délai qu'énonce l'article 2842 est une règle en vue d'assurer l'authenticité et la véracité du document objet de la reproduction. En l'espèce, la preuve faite concernant cette reproduction est ici gage de véracité et les objections formulées par la demanderesse quant à l'admissibilité du document reproduisant la proposition sont rejetées. »*

Ces trois articles de droit nouveau instaurent-ils un régime de preuve secondaire recevable uniquement lorsque l'original papier ne peut être offert en preuve primaire? La question est d'importance puisque la destruction volontaire de l'original suivant une procédure qui ne respecterait pas les exigences des articles 2840 à 2842 C.c.Q. interdirait tant la preuve primaire (l'original n'étant plus disponible et la reproduction étant irrecevable) que la preuve secondaire par l'inscription informatisée (la partie perdant le bénéfice de l'exception établie au second alinéa de l'article 2860 C.c.Q.). Dans ce contexte, l'entreprise prudente doit-elle voir à la préparation de déclarations assermentées attestant la destruction des documents reproduits? Bien que l'article 2842 C.c.Q. ne s'attarde qu'à la préparation d'attestations de reproduction, un auteur[257] suggère la tenue de registres d'affidavits de destruction comme mesure minimale, étant donné l'irrecevabilité probable de la reproduction préparée en présence d'un original résiduel qui lui est hiérarchiquement supérieur sur le plan de la preuve suivant l'article 2860 C.c.Q. Sachant que la reproduction devra entraîner la destruction de l'original, nous partageons l'avis de cet auteur puisque la mise en application de la mesure qu'il propose procurera un moyen de preuve et un témoin crédible pour établir que l'original n'existe plus (et qu'il est donc inutile de le chercher à grands frais) et que la partie n'a en sa possession qu'une reproduction valable, pour autant que les articles 2840 à 2842 C.c.Q. auront dicté son action.

Soulignons que la reproduction qui, suivant l'article 2840 C.c.Q., est reçue en preuve « *au même titre que l'original* », si elle respecte les conditions prévues à la loi, jouirait d'un traitement supérieur à la reproduction des données inscrites simultanément à l'acte juridique, un résultat jugé incohérent. Cette supériorité résulterait des règles de force probante particulières à l'article 2839 C.c.Q. qui permettent de contredire le

---

[257] B. TROTTIER, *loc. cit.*, note 56, pp. 782, 791.

document visé à l'article 2837 C.c.Q. par tout moyen, incluant des moyens de preuve autrement irrecevables pour contredire un écrit valablement fait. L'article 2839 C.c.Q. qui, de fait, « *limite la portée des règles contenues dans les articles 2837 et 2838* »[258], ne s'applique pas à la reproduction visée par l'article 2840 C.c.Q. Il en va de même pour l'article 2836 C.c.Q. si l'original reproduit constitue un écrit sous seing privé au sens de l'article 2826 C.c.Q. Or, 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[259]. Il sera tenu pour reconnu s'il n'est pas contesté de la manière prévue au *Code de procédure civile*[260] par des moyens de preuve recevables[261]. Ainsi, la reproduction d'un acte sous seing privé suivant l'article 2840 C.c.Q. jouirait en apparence, par l'effet des articles 2837, 2839, 2840 et 2862 C.c.Q., d'un statut supérieur à celui du document visé à l'article 2837 C.c.Q., du moins dans la hiérarchie des moyens de preuve.

À notre avis, cette incohérence apparente s'estompe si on rappelle que l'article 2837 C.c.Q. introduit un nouveau moyen de preuve et que le document qui reproduit l'inscription informatisée n'est pas un acte sous seing privé, mais bien un document assimilé à un écrit sur lequel des humains n'auront parfois aucun contrôle. C'est pour cette raison qu'il peut être contredit par tous les moyens[262].

La question est donc de savoir si la reproduction de l'original d'un écrit qui jouit du statut conféré aux actes sous seing privé doit perdre ce statut du fait de sa reproduction. Dit autrement, le processus de reproduction doit-il en soi justifier un changement de statut? De deux[263] choses l'une : ou bien la reproduction est fidèle, indélébile et complète suivant les normes établies et elle devra alors recevoir un

---

258 *Commentaires du ministre de la Justice, op. cit.*, note 71, p. 1776.

259 Art. 2829 C.c.Q.

260 Art. 89 C.p.c. Celui qui veut contester la signature ou une partie importante d'un écrit sous seing privé doit l'alléguer expressément et appuyer sa contestation d'un affidavit.

261 En effet, l'art. 2863 C.c.Q. prévoit que 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 même, l'art. 2862 C.c.Q. édicte que la preuve d'un acte juridique ne peut, entre les parties, se faire par témoignage lorsque la valeur du litige excède 1 500 $.

262 *Commentaires du ministre de la Justice, op. cit.*, note 71, p. 1776.

263 En cela, nous excluons une troisième voie, soit celle d'accepter ces deux avenues mutuellement exclusives, tout en refusant d'accepter que le respect des conditions prévues à l'article 2840 C.c.Q. soit suffisant pour conférer à la reproduction la fiabilité de l'original. Les tribunaux verront selon nous à interpréter les articles 2840 à 2842 C.c.Q. de façon à garantir cet objectif

traitement identique à l'original, ou bien cette reproduction est viciée et ne peut valoir comme original, ni être recevable, pas même sous le déguisement d'un autre écrit[264].

Pour conclure, nous estimons que l'article 2840 C.c.Q. n'ajoute pas à la liste des écrits visés au chapitre premier du titre deuxième de la preuve, comme le fait l'article 2837 C.c.Q. Il ne régit que la reproduction d'écrits déjà reconnus à l'intérieur d'une hiérarchie qu'il n'entend pas bousculer. Ainsi la comparaison, s'il en est une, ne doit pas être faite entre l'article 2840 C.c.Q. et l'article 2837 mais bien entre les articles 2837 et 2826 C.c.Q.

La pertinence des articles 2840 à 2842 C.c.Q. est manifeste dans l'élaboration de la Convention régie par le droit québécois : ils fixent des conditions substantives et formelles d'admissibilité d'une reproduction électronique et imposent à l'entreprise des contraintes d'ordre humain[265] et administratif[266].

2.2.2 Des initiatives législatives phares au Canada et ailleurs ou la recherche d'un arrimage conventionnel

La présente section, qui ne prétend pas revoir l'ensemble des lois ou projets de lois proposés pour encadrer le commerce électronique, portera sur certaines initiatives législatives signifiantes en raison de leur contenu et de leur pertinence à l'objet de ce mémoire. Il ne s'agit pas d'une étude critique ou de droit comparé, mais de l'identification de balises pouvant nous guider aux fins de la Convention, sachant que ces initiatives ont reçu l'endossement d'États par voie d'adoption ou de référence dans le droit interne.

2.2.2.1 La Loi type de la CNUDCI sur le commerce électronique

En décembre 1996, la Commission des Nations-Unies pour le droit commercial international, la CNUDCI, adoptait la *Loi type sur le commerce électronique* (la « *Loi type* ») ainsi qu'un Guide pour son incorporation dans le droit interne des

---

264 Art. 2831 C.c.Q.

265 Notamment par le besoin d'affiants formés à la reproduction conforme de documents.

266 Notamment par la tenue de registres détaillés et l'imposition de délais pour l'exécution de taches administratives.

États[267]. Ce faisant, la CNUDCI invitait les États à prendre en considération la *Loi type* au moment de rédiger ou de réviser leurs lois internes, « *compte tenu de la nécessité d'assurer l'uniformité du droit applicable aux moyens autres que les documents papier pour communiquer et conserver l'information* »[268]. Nous verrons que le gouvernement canadien a répondu en partie à cet appel par l'adoption du *Projet de loi C-6*[269].

La *Loi type* comporte deux parties, la première portant sur le commerce électronique en général[270], la seconde sur le commerce électronique dans des secteurs économiques particuliers limités, pour l'heure, au transport des marchandises[271]. Elle constitue une loi cadre flexible et suppose l'adoption, par les États, de règles juridiques et techniques précisant des modalités de mise en application, tenant compte des situations nationales particulières. Son fondement réside dans l'acceptation d'une « *approche fondée sur l'équivalent fonctionnel* »[272] des notions « d'écrit », de « signature » et « d'original ». Cette approche repose sur l'analyse des objectifs et des fonctions traditionnels du document papier et sur la détermination de moyens techniques propres au commerce électronique pouvant assurer ces objectifs ou fonctions. La recherche d'un document authentique, intègre, fiable, accessible, intelligible, lisible et reproductible, selon le cas, traduit ces objectifs et ces fonctions, tout en dictant les exigences requises pour la reconnaissance de telles équivalences fonctionnelles pour certaines catégories de documents.

Le cœur juridique de la *Loi type*, aux fins du présent mémoire, se trouve au chapitre II intitulé « Application des exigences légales aux messages de données ». Les auteurs de la *Loi type* rappellent que les dispositions contenues dans ce chapitre ont pour but de faciliter l'utilisation de techniques modernes de communication[273]. Ces dispositions doivent donc être considérées comme énonçant des conditions minimales et doivent, pour cette raison, être considérées comme obligatoires, sauf dispositions contraires. Ce « minimum acceptable » ne doit pas cependant être interprété pour autant

---

267 *Loi type sur le commerce* électronique et Guide *pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur le commerce électronique* (le « Guide »), disponible au site http://www.un.or.at/uncitral/.

268 Résolution adoptée par l'Assemblée générale (A/51/628), par. 2.

269 *Infra*, section 2.2.2.3.

270 *Loi type*, précitée, note 267, art. 1 à 15 inclusivement.

271 *Id.*, art. 16 et 17.

272 *Guide, op.cit.*, note 267, par. 16.

273 *Id.*, par. 21.

comme invitant les États à poser des conditions plus strictes que celles proposées par la *Loi type*[274]. Ce chapitre II est ainsi consacré à la reconnaissance juridique des messages de données[275], aux notions d'écrit[276], de signature[277], et d'original[278], à l'admissibilité et à la force probante d'un message de données[279] et enfin, à la conservation de ces messages[280].

L'article 5 de la *Loi type* prévoit que « *L'effet juridique, la validité ou la force exécutoire d'une information ne sont pas déniés au seul motif que cette information est sous forme de message de données* »[281]. Cette reconnaissance juridique de l'information contenue dans le message de données apparaît sous la forme d'un principe de non-discrimination, ou d'égalité de traitement. L'article 5 n'établit donc pas, en soi, la valeur légale du message de données, ni n'ajoute aux exigences énoncées de façon plus spécifique aux articles 7 à 10 de la *Loi type*. Ce principe de non-discrimination est néanmoins central dans la *Loi type* et son application déborde le cadre du chapitre II.

La *Loi type* traite également de la notion « d'écrit » et de son équivalent fonctionnel pour le document électronique. Ainsi, on dira que le message de données satisfait à l'exigence qu'une information soit présentée ou conservée sous forme d'écrit si « *l'information qu'il contient est accessible pour être consultée ultérieurement* »[282] par l'homme ou par l'ordinateur[283]. Le critère de l'accessibilité implique « *qu'une information se présentant sous la forme de données informatisées doit être lisible et interprétable et que le logiciel qui pourrait être nécessaire pour assurer la lisibilité de*

---

274 *Ibid.*

275 *Loi type*, précitée, note 267, art. 5.

276 *Id.*, art. 6.

277 *Id.*, art. 7.

278 *Id.*, art. 8.

279 *Id.*, art. 9; L'expression « message de données » est définie à l'art. 2(a) de la *Loi type* et désigne « l'information créée, envoyée, reçue ou conservée par des moyens électroniques ou optiques ou des moyens analogues notamment, mais non exclusivement, l'échange de données informatisées (EDI), la messagerie électronique, le télégraphe, le télex et la télécopie ».

280 *Id.*, art. 10.

281 *Id.*, art. 5.

282 *Id.*, par. 6(1). Aux fins d'accroître l'accessibilité de la *Loi type*, les États jouissent, au troisième paragraphe de l'art. 6 de même qu'aux articles 7 et 8 vus ci-après, d'un droit d'exclure certaines situations pour lesquelles le principe d'équivalence fonctionnelle ne serait pas applicable. Ces situations ne sont pas précisées dans la *Loi type*, sous sa forme actuelle.

283 *Guide*, *op. cit.*, note 267, par. 50.

pareilles informations doit être préservé »[284]. Il s'agit là d'un critère objectif préférable, selon la CNUDCI, aux critères trop stricts de durabilité ou d'inaltérabilité ou aux critères trop suggestifs tels l'intelligibilité. L'exigence de l'écrit, nous rappelle la CNUDCI[285], est la strate inférieure de la hiérarchie des conditions de forme et se distingue des exigences légales plus strictes comme la production d'un « écrit signé », d'un « original signé » ou d'un « acte juridique authentique ».

L'article 7 de la *Loi type* s'attarde à deux fonctions essentielles de la signature, soit l'identification de l'auteur et la confirmation qu'il approuve l'information contenue dans le message de données. L'auteur d'un document électronique ne peut le signer au sens classique mais peut y apposer une marque électronique distinctive pour atteindre les mêmes objectifs[286]. Ainsi, l'exigence légale de la signature sera satisfaite si ces deux fonctions sont remplies suivant une méthode dont la fiabilité est suffisante « *au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière* »[287]. L'approche de la CNUDCI est un modèle de souplesse. D'abord elle reconnaît des niveaux de fiabilité en fonction de la finalité du document électronique, ouvrant du coup le recours à des signatures électroniques à niveau de sécurité et à coût variables. Ensuite, elle permet la prise en compte de l'évolution des techniques et des algorithmes de cryptographie garantissant les niveaux de sécurité recherchés tout en maintenant une neutralité technologique. Cette approche assure également que l'ensemble des circonstances pertinentes sera considérée à l'étape de l'étude de la fiabilité de la signature[288]. Enfin elle

---

284 *Ibid.*

285 *Id.*, par. 49.

286 Au titre des fonctions habituellement mentionnées pour la signature, mentionnons celles d'identifier une personne, d'attester sa présence, sa participation personnelle ou son intention d'être liée par la teneur d'un acte juridique, d'associer cette personne à la teneur d'un texte ou encore d'en confirmer la paternité.

287 *Loi type*, précitée, note 267, art. 7(1)(b).

288 Le *Guide*, *op. cit.*, note 267, part. 57, établi par la CNUDCI identifie un ensemble de facteurs juridiques techniques et commerciaux à prendre en considération, incluant (1) le degré de perfectionnement du matériel utilisé par chacune des parties; (2) la nature de leurs activités commerciales; (3) la fréquence avec laquelle elles effectuent entre elles des opérations commerciales; (4) la nature et l'ampleur de l'opération; (5) le statut et la fonction de la signature dans un régime législatif et réglementaire donné; (6) la capacité des systèmes de communication; (7) les procédures d'authentification proposées par les opérateurs des systèmes de télécommunication; (8) la série de procédures d'authentification communiquée par un intermédiaire; (9) l'observation des coutumes et pratiques commerciales; (10) l'existence de mécanismes d'assurance contre les messages non autorisés; (11) l'importance et la valeur de l'information contenue dans le message de données; (12) la disponibilité d'autres méthodes d'identification et le coût de leur mise en œuvre; (13) le degré d'acceptation ou de non acceptation de la méthode d'identification dans le secteur ou domaine pertinents.

reconnaît le recours à la convention privée en matière de signature, étant entendu que la méthode de signature négociée ne sera pas fiable du seul fait qu'elle est convenue dans le cadre d'un accord entre partenaires commerciaux.

La quête de l'original d'un document électronique est abordée à l'article 8 de la *Loi type*. Cette quête doit avant tout être axée sur la préservation de l'intégrité de l'information, en l'absence de tout original au sens strict[289]. Cet énoncé est manifeste à la lecture de l'article 8 repris en partie ci-dessous :

> *« Article 8 – Original*
>
> *1. Lorsque la loi exige qu'une information soit présentée ou conservée sous sa forme originale, un message de données satisfait à cette exigence :*
>
> *a) S'il existe une garantie fiable quant à l'intégrité de l'information à compter du moment où elle a été créée pour la première fois sous sa forme définitive en tant que message de données ou autre; et*
>
> *b) Si, lorsqu'il est exigé qu'une information soit présentée, cette information peut être montrée à la personne à laquelle elle doit être présentée. »*[290]

Ici encore, la *Loi type* propose des règles minimales pour établir l'équivalence fonctionnelle originalité-intégrité, dès la création du message de données sous sa forme définitive jusqu'à sa présentation, y compris la phase de conservation. L'intégrité doit s'apprécier en se référant à l'enregistrement systématique de l'information, à l'assurance que l'information a été enregistrée sans lacune et à la protection des données contre toute altération, exception faite de certains ajouts ou modifications qui n'affectent en rien le caractère original du message[291]. La garantie de fiabilité doit couvrir tout le cycle de vie du document électronique, incluant l'étape de la numérisation d'un document papier vers un support électronique[292]. Le niveau de fiabilité s'apprécie avec souplesse au regard de l'ensemble des circonstances. L'article 8 fait comprendre toute l'importance des systèmes

---

289 Le destinataire du document électronique reçoit une copie dans tous les cas si l'on entend par original le support sur lequel l'information a été fixée pour la première fois. *Guide*, *op. cit.*, note 267, par. 62.

290 *Loi type*, précitée, note 267, par. 8(1)(a) et (b).

291 Référence est faite, par exemple, aux endossement, authentification ou autres certifications ajoutés à la fin du message de données pour attester l'identité de l'expéditeur ou encore des métadonnées requises pour opérer la transmission.

292 En effet, l'expression « à compter du moment où elle a été créée pour la première fois sous sa forme définitive » inclut le document papier et exige la preuve d'une numérisation fiable.

d'informations[293], y compris les systèmes d'archivage présentant les garanties de fiabilité suffisantes pour satisfaire aux exigences imposées.

Le principe de non-discrimination est repris à l'article 9 de la *Loi type* concernant l'admissibilité du document électronique. Ainsi, aucune règle d'administration de la preuve ne peut être invoquée dans une procédure légale contre l'admissibilité d'un message de données produit comme preuve au motif qu'il s'agit d'un message de données ou, s'il s'agit de la meilleure preuve que celui qui la présente peut raisonnablement escompter obtenir, au motif que le message n'est pas sous sa forme originale[294]. Le paragraphe 9(2) stipule que la force probante du message de données s'apprécie eu égard à la fiabilité du mode de création, de conservation ou de communication du message, à la fiabilité du mode de préservation de l'intégrité de l'information, à la manière dont l'expéditeur a été identifié et à toute autre considération pertinente.

Enfin, c'est à l'article 10 de la *Loi type* qu'est abordée la question de l'archivage :

> *« Lorsqu'une règle de droit exige que certains documents, enregistrements ou informations soient conservés, cette exigence est satisfaite si ce sont des messages de données qui sont conservés, sous réserve des conditions suivantes :*
>
> *a) L'information que contient le message de données doit être accessible pour être consultée ultérieurement;*
>
> *b) Le message de données doit être conservé sous la forme sous laquelle il a été créé, envoyé ou reçu, ou sous une forme dont il peut être démontré qu'elle représente avec précision les informations créées, envoyées ou reçues;*
>
> *c) Les informations qui permettent de déterminer l'origine et la destination du message de données, ainsi que les indications de date et d'heure de l'envoi ou de la réception, doivent être conservées si elles existent. »*

---

293 Le terme « système d'information » désigne, en vertu de l'article 2 f) de la *Loi type*, « un système utilisé pour créer, envoyer, recevoir, conserver ou traiter de toute manière des messages de données ».

294 *Loi type*, précitée, note 267, art. 9(1)(a) et (b).

Cet article propose des règles pour l'élaboration d'un régime d'archivage interne, ou par impartition[295], qui doit satisfaire au droit étatique en matière de conservation de documents, d'enregistrement ou, plus généralement, d'informations. Le premier alinéa reprend les critères d'accessibilité et de consultation énoncés à l'article 6(1) de la *Loi type* relativement à l'exigence d'un écrit, alors que le second alinéa pose le principe de la conservation du message sous sa forme d'origine, sans pour autant « *exiger que l'information soit conservée sans modification puisqu'en général les messages sont décodés, comprimés ou convertis pour pouvoir être conservés* »[296]. L'alinéa c) vise la conservation des métadonnées[297] à l'exception de celles qui n'ont d'autre objet que de permettre l'envoi ou la réception de message de données[298]. L'article 10 ne stipule pas de durée de conservation, considérant sans doute la diversité des exigences légales de chaque État.

La *Loi type* peut donc être d'une grande utilité à l'étape de l'élaboration d'une Convention. Elle consacre le principe de non-discrimination à l'égard du document électronique en vue de sa reconnaissance et de son admissibilité en preuve. Elle propose des conditions minimales pour la reconnaissance d'équivalents fonctionnels aux notions d'écrit, de signature et d'original et recherche une neutralité technologique des méthodes de signature. Elle souligne toute l'importance de systèmes de conservation fiables pour assurer l'intégrité du document électronique et fournit des balises pour garantir cette fiabilité. Enfin, elle invite à la conclusion d'accords entre partenaires commerciaux et à la référence à des normes reconnues.

2.2.2.2 Le Projet de la CNUDCI de Règles uniformes sur les signatures électroniques

En décembre 1999, le Groupe de travail sur le commerce électronique de la CNUDCI livrait son dernier projet disponible de règles uniformes sur les signatures électroniques[299] (les « Règles »). Ce projet de Règles compatibles avec la *Loi type* aborde

---

295 Le paragraphe 3 de l'article 10 prévoit que, pour satisfaire aux conditions énoncées au paragraphe 1, un destinataire ou un expéditeur peut avoir recours aux services de toute autre personne, et pas uniquement d'un intermédiaire; *Guide*, *op. cit.*, note 267, par. 75.

296 *Guide*, *op. cit.*, note 267, par.73.

297 Les métadonnées sont des renseignements contextuels relatifs à l'origine, à la destination, à l'envoi et à la réception du message de données pouvant s'avérer nécessaire à l'identification ou au maintien de l'intégrité du message.

298 Pensons par exemple au protocole de communication lui-même.

299 A/CN.9/WG.IV/WP.84, 8 décembre 1999, disponible au site http//www.uncitral.org/fr-index.htm.

des questions juridiques relatives aux signatures électroniques et aux autorités de certification, aux nouvelles techniques d'authentification, à l'applicabilité de la certification aux relations commerciales internationales, à la répartition des risques et des responsabilités entre intervenants et à la preuve des messages de données[300]. Elles constituent un ensemble de normes en matière de certification[301], en particulier dans les cas de certification transnationale[302] et tentent de préserver le principe de neutralité ou d'égalité de traitement des signatures électroniques fiables, quelle que soit la méthode de signature envisagée[303].

Ces Règles sont d'intérêt aux fins du présent mémoire. Rappelons d'entrée de jeu qu'elles font une large place à l'autonomie des parties et à leur liberté contractuelle, puisqu'elles peuvent à la fois servir de normes obligationnelles incorporées par référence et de normes minimales supplétives dans un environnement où les parties sont régies par convention. La pertinence d'un accord entre partenaires commerciaux est reconnue expressément en matière de signature électronique[304]. La CNUDCI rappelle, comme nous l'avons fait ailleurs[305], qu'il ne s'agit pas de porter atteinte à l'ordre public ou aux lois impératives applicables aux contrats, telles les dispositions relatives aux contrats léonins. De plus, l'article 5 laisse aux parties la liberté de déroger aux dispositions des Règles ou de les modifier :

> *« Il est possible de déroger aux présentes Règles ou [de les modifier] [d'en modifier l'effet] par convention, à moins que lesdites Règles ou la loi de l'État adoptant en dispose autrement. »*

D'autre part, ces Règles apportent des précisions utiles pour la mise en œuvre de la *Loi type* et des notions d'équivalents fonctionnels dans une vaste gamme d'activités commerciales[306]. À titre illustratif, on y précise la notion de « signature électronique renforcée »[307], notion jumelle de la « signature électronique sécurisée » proposée par le

---

300 *Projet de Règles uniformes sur les signatures électroniques* (les « Règles »), art. 1.

301 *Id.*, art. 10, 11 et 12.

302 *Id.*, art. 13.

303 *Id.*, art. 3.

304 *Id.*, art. 6(1).

305 *Supra*, note 131.

306 La notion d'activités commerciales est définie très largement aux *Règles*, consulter à ce sujet la définition proposée à l'art. 1.

307 *Règles*, précité, note 300, art. 2(b) et commentaires.

Projet de loi C-6 du gouvernement fédéral[308]. Ainsi, la signature électronique renforcée se distingue par l'application d'une procédure ou d'une méthode démontrant : (1) qu'elle est particulière au détenteur de la signature aux fins pour lesquelles elle est utilisée, (2) qu'elle a été créée et apposée au message de données par le détenteur de la signature ou à l'aide d'un moyen dont seul ce détenteur a le contrôle et (3), qu'elle a été créée et est liée au message de données auquel elle se rapporte d'une manière qui offre une garantie fiable quant à l'intégrité du message[309]. De même, les Règles précisent les exigences à l'origine d'une présomption réfragable de fiabilité d'une signature électronique, abordant les notions de contrôle[310], d'intégrité[311], d'identification[312], d'approbation[313], d'intention[314] et de fiabilité technique[315]. Elles servent également à confirmer une présomption « d'originalité » du document électronique lorsqu'il porte une signature électronique offrant une garantie suffisante de fiabilité à compter du moment où le document a été créé[316].

Ces Règles confirment les tendances lourdes envisagées en vue de lever l'incertitude juridique dans le cyberespace et consacrent le bien-fondé du recours à des accords entre partenaires commerciaux.

2.2.2.3 Le Projet de loi C-6

Le 26 octobre 1999, la Chambre des communes adoptait le *Projet de loi C-6* sur la protection des renseignements personnels et les documents électroniques[317], plus d'un an après le dépôt de son défunt prédécesseur, le projet de *Loi C-54*[318].

---

308 *Projet de loi C-6*, art. 48, *infra*, section 2.2.2.3.

309 *Règles*, précité, note 300, art. 2(b).

310 *Id.*, art. 6(3)(b).

311 *Id.*, art. 6(3)(c).

312 *Id.*, art. 6(3)(d).

313 *Id.*, art. 6(3)(c).

314 *Id.*, art. 4(a).

315 *Id.*, art. 6(3)(a).

316 *Id.*, art. 7.

317 *Projet de loi C-6*, précité, note 51.

318 En effet, le 1er octobre 1998, le gouvernement fédéral déposait en première lecture un projet de loi fédéral C-54 concernant la protection des renseignements personnels et les documents électroniques, lequel fera l'objet de modifications par la suite.

Cette loi veut faciliter et promouvoir le commerce électronique suivant trois axes principaux, soit en protégeant les renseignements personnels recueillis, utilisés ou communiqués dans certaines circonstances, en prévoyant l'utilisation de moyens électroniques pour communiquer ou enregistrer de l'information et des transactions et en modifiant la *Loi sur la preuve au Canada*[319], la *Loi sur les textes réglementaires*[320] et la *Loi sur la révision des lois*[321].

Une première partie, qui rappelle à certains égards la *Loi sur la protection des renseignements personnels dans le secteur privé au Québec*[322], a pour objet de fixer, en cette nouvelle ère technologique, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tienne compte du droit des individus à la vie privée[323]. Le législateur souscrit à cette fin aux principes énoncés dans le code type CAN/CSA-Q830-96 publié en 1995 sous l'égide de l'Association canadienne des normes relativement à la protection des renseignements personnels[324]. La seconde partie a pour objet de prévoir l'utilisation de moyens électroniques par l'établissement d'un régime d'équivalences fonctionnelles pour le document électronique, tel que défini dans le *Projet de loi C-6*[325], dans les cas où des textes législatifs émanant d'entités fédérales envisagent l'utilisation d'un support papier pour enregistrer ou communiquer de l'information ou des transactions[326]. Le gouvernement entend adopter une réglementation précisant ces équivalences fonctionnelles et les modalités d'application de la loi, notamment « *pour prévoir des technologies ou des procédés pour l'application de la définition de signature électronique sécurisée* »[327]. Enfin, le législateur fédéral propose des modifications à la *Loi sur la preuve au Canada*,

---

319 *Loi sur la preuve au Canada*, L.R., ch. C-5; L.R., ch. 27 (1er suppl.), ch. 19 (3e suppl.); 1992, ch. 1, 47; 1993, ch. 28, 34; 1994, ch. 44; 1995, ch. 28; 1997, ch. 18; 1998, ch. 9.

320 *Loi sur les textes réglementaires*, L.R., ch. S-22; L.R., ch. 31 (1er suppl.), ch. 31, 51 (4e suppl.); 1993, ch. 28, 34.

321 *Loi sur la révision des lois*, L.R., ch. S-20; 1992, ch. 1.

322 *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q. ch. P-39.1.

323 *Projet de loi C-6*, précité, note 51, art. 3 à 30 inclusivement.

324 *Projet de loi C-6*, précité, note 51, Annexe 1.

325 *Id.*, art. 31(1).

326 *Projet de loi C-6*, précité, note 51, art. 31 à 51.

327 *Id.*, art. 48(1).

la *Loi sur les textes réglementaires* et la *Loi sur la révision des lois*[328] donnant effet à la reconnaissance du document et de la signature électroniques.

C'est à ces deux dernières parties du *Projet de loi C-6* que nous nous attarderons, non pour critiquer des textes déjà controversés quant à leur architecture, leur constitutionnalité ou leur applicabilité aux entreprises québécoises[329], mais plutôt pour y puiser des valeurs sûres aux fins d'échafauder la Convention.

Précisons immédiatement que le *Projet de loi C-6* découle en partie de l'engagement du Canada de « *prendre dûment en considération la Loi type lorsqu'ils promulgueront des lois ou réviseront leur législation* »[330]. On ne se surprendra donc pas de retrouver dans le *Projet de loi C-6* les principes de non-discrimination ou d'égalité de traitement[331], d'équivalence fonctionnelle[332] et de neutralité technologique[333]. On ne pourrait davantage étudier le *Projet de loi C-6* sans rappeler qu'elle reprend de larges pans de la *Loi uniforme sur le commerce électronique* (la « *LUCE* ») et de la *Loi uniforme sur la preuve électronique* (la « *LUPE* ») proposées dès 1998 par la Conférence pour l'harmonisation des lois au Canada (la « CHLC »)[334]. Ces lois uniformes, elles-mêmes inspirées de la *Loi type* et des principes qui y sont incarnés, tiennent compte des réalités juridiques canadiennes, particulièrement aux fins de l'utilisation de documents électroniques dans les relations de l'individu avec le gouvernement[335].

Le champ d'application du *Projet de loi C-6* est défini à l'article 4. La partie II sur le document électronique s'adresse d'abord aux personnes morales dont un ministre

---

328 *Id.*, art. 52 à 72 inclusivement.

329 Des juristes ont exprimé l'avis que la protection des renseignements personnels et la notion de signature, déjà traitée à l'art. 2837 C.c.Q., et plus généralement le commerce électronique dans le cyberespace ne peuvent être de compétence fédérale exclusive et relèvent davantage des compétences provinciales en matière économique de la propriété et des droits civils. À ce sujet, on peut consulter l'avis du CAI concernant le *Projet de loi C-6* disponible au site http//www.cai.gouv.qc.ca/9981514htm ainsi que les mémoires de l'Association du Barreau canadien concernant le *Projet de loi C-6* et de l'Association du Barreau du Québec, respectivement de mars 1999 et de février 1999.

330 Résolution adoptée par l'assemblée générale sur le rapport de la sixième commission, 85ième séance plénière, (A/51/628), 16 décembre 1996, p. 2.

331 *Loi type*, précitée, note 267, art. 5.

332 *Loi type*, précitée, note 267, art. 7.

333 *Loi type*, précitée, note 267, art. 2(a).

334 Consulter, relativement à la Conférence, le site http://www.law.ualberta.ca/alri/ulc.

335 Consulter à ce sujet la partie II de la *LUCE*.

est responsable devant le Parlement fédéral[336]. Elle s'applique à une loi fédérale et à tout texte législatif pris sous le régime d'une loi fédérale ou en vertu d'une prérogative royale[337]. Ainsi, dans le cadre des relations entre la personne et l'État, le *Projet de loi C-6* reconnaît aux citoyens le droit d'effectuer des paiements[338], d'effectuer un dépôt[339], de transmettre de l'information[340], de prescrire[341] et de compléter des formulaires[342] par des moyens électroniques.

De plus, le *Projet de loi C-6* semble permettre à des personnes de droit privé de convenir de la fourniture de documents ou d'informations sous forme électronique pour satisfaire à leurs obligations statutaires. Ainsi, selon l'article 40 :

> « ***40.*** *Dans le cas où une disposition d'un texte législatif - à l'exclusion d'une disposition visée aux articles 41 à 47 - exige qu'une personne fournisse à une autre un document ou de l'information, la fourniture du document ou de l'information sous forme électronique satisfait à l'obligation si les conditions suivantes sont réunies :*
>
> *a) la disposition ou le texte législatif est inscrit sur la liste figurant à l'annexe 2 ou 3;*
>
> *b) les intéressés ont convenu de la fourniture du document ou de l'information sous forme électronique;*
>
> *c) le document ou l'information sous forme électronique sera mis à la disposition exclusive de la personne à qui le document ou l'information est fourni et sera lisible ou perceptible de façon à pouvoir servir à la consultation ultérieure.* »

Or, l'exclusion des articles 41 à 47 traitant du document sous forme écrite, du document original, de la signature électronique, de la déclaration sous serment, de l'affidavit, de la signature devant témoin et de la fourniture d'exemplaires réduit à peu de choses l'utilité de cette disposition prometteuse aux fins de la Convention.

---

336 *Projet de loi C-6*, précité, note 51, art. 33. Le *Projet de loi C-6* permet également à cette personne ou cet organisme d'opter pour l'utilisation d'un moyen électronique en l'absence de dispositions l'interdisant dans le texte législatif concerné.

337 À l'exception d'un texte pris sous le régime de la *Loi sur le Yukon*, de la *Loi sur les Territoires du Nord-Ouest* ou de la *Loi sur le Nunavut*.

338 *Projet de loi C-6*, précité, note 51, art. 34.

339 *Id.*, art. 35(2).

340 *Id.*, art. 35(3).

341 *Id.*, art. 35(4).

342 *Id.*, art. 35(1).

En bref, le législateur fédéral tente par cette loi de lever l'incertitude du droit évoqué précédemment[343] à l'égard du document électronique, de son authenticité et de son intégrité et, partant, de son admissibilité en preuve. Son objectif ne pouvait logiquement être atteint qu'en abordant les concepts de document, de signature et d'écrit électroniques, d'original, de forme, de conservation et de preuve.

a) Le document électronique

Le document électronique est défini dans le *Projet de loi C-6* pour inclure l'ensemble des données enregistrées ou mises en mémoire sur quelque support que ce soit par un système informatique ou un dispositif semblable et qui peuvent être lues ou perçues par une personne ou par un tel système ou dispositif. Sont également visés tout affichage et toute sortie imprimée de ces données[344]. Le mot « donnée » comprend toute forme de représentation d'informations ou de notions[345]. Certes, cette définition est suffisamment large pour inclure à l'heure actuelle la quasi-totalité des documents d'entreprise dans le cours normal des affaires. Certains diront cependant que cette définition est restrictive en ce qu'elle limite l'origine des documents électroniques aux systèmes informatiques, à l'exclusion de moyens optiques ou analogues ou « *d'autres moyens capables d'enregistrer ou de mettre en mémoire de l'information sous forme numérique ou électronique* »[346].

b) Le document original

L'article 42 du *Projet de loi C-6* traitant du document électronique original demeure incomplet, en l'absence de la réglementation et des annexes habilitantes[347]. Pour l'heure, nous savons que le document électronique pourra satisfaire à l'exigence d'un original émanant de textes législatifs désignés[348] s'il comporte une signature électronique sécurisée, ajoutée lors de la production originale du document électronique dans sa forme

---

343 *Supra*, section 1.2.1.2.

344 *Projet de loi C-6*, précité, note 51, art. 31(1).

345 *Id.*, art. 31(1).

346 *LUCE*, art. 1. Voir aussi la définition de « messages de données » à l'art. 1 de la *Loi type*. Pour une étude comparative des définitions de documents électroniques en droit américain, consulter McBride, Baker & Coles disponible au site http://www.mbc.com/ecommerce/legis/table02.html. On s'interrogera également sur la logique d'inclure le relevé imprimé ou toute sortie analogue, s'agissant là plutôt d'une reproduction sur papier de données contenues sur support informatique.

347 *Projet de loi C-6*, précité, note 51, art. 48(1).

348 *Projet de loi C-6*, précité, note 51, art. 42(a).

définitive, qui puisse être utilisée pour établir qu'il n'a pas été modifié[349]. L'approche adoptée par le gouvernement fédéral diffère de celle de la *Loi type*[350] et de la *LUCE*[351] en ce que ces deux dernières lois n'imposent pas le recours à une signature électronique sécurisée ou renforcée. On y recherche plutôt la preuve d'une garantie fiable de l'intégrité de l'information contenue dans le document électronique.

Nous verrons aussi que le libellé de l'article 42(b) est plus limitatif que l'article 37(a) du *Projet de loi C-6*, forçant l'archivage de l'original dans sa forme d'origine, sans modification. Ainsi, la qualité d'original du document électronique pourrait être perdue par son archivage sous une forme qui ne modifie en rien l'information qu'il contient.

c) L'écrit

Le *Projet de loi C-6* reconnaît que le document électronique peut satisfaire à l'exigence légale d'un écrit[352]. Cette reconnaissance est assujettie à un règlement d'application dont les conditions demeurent inconnues à ce jour. Pour l'instant, nous ne pouvons que spéculer sur la teneur de ces conditions par référence à la *Loi type* ou à la *LUCE*. L'article 6 de la *Loi type* fonde l'équivalence d'un écrit électronique sur l'accessibilité de l'information qu'il contient pour consultation ultérieure[353]. L'article 5 de la *LUCE* se fait plus onéreux en exigeant que le document électronique soit « *sous le contrôle de la personne à qui l'information est fournie et l'information contenue dans le document électronique sera accessible et utilisable pour consultation ultérieure* »[354]. Dans la mesure où la notion d'accessibilité implique un certain niveau de contrôle de la part de celui qui rend l'information accessible, on pourra s'interroger sur la portée véritable de cet ajout de la notion de contrôle par la *LUCE*[355].

---

349 *Projet de loi C-6*, précité, note 51, art. 42(b).

350 *Loi type*, précitée, note 267, art. 8.

351 *LUCE*, art. 7.

352 *Projet de loi C-6*, précité, note 51, art. 41.

353 *Loi type*, précitée, note 267, art. 6(1).

354 *LUCE*, art. 5.

355 On notera que l'art. 12 de la *Uniform Electronic Transactions Act*, *infra*, section 2.2.2.6, utilise l'expression « *remains accessible for later reference* ».

d) La signature électronique

Les notions de signature électronique et de signature électronique sécurisée forment l'épicentre de l'alternative électronique offerte par le *Projet de loi C-6*. Ces notions y sont définies. La signature électronique est constituée d'une ou de plusieurs lettres, ou d'un ou de plusieurs caractères, nombres ou autres symboles sous forme numérique incorporée, jointe ou associée à un document électronique[356]. La signature électronique sécurisée est une signature électronique qui résulte de l'application d'une technologie ou d'un procédé prévu par règlement pris en vertu du paragraphe 48(1) de la loi[357], conformément à certains critères conçus pour garantir la fiabilité de cette signature. Le paragraphe 48(2) prévoit que le gouvernement en conseil peut prévoir par règlement[358] une technologie ou un procédé, s'il peut être établi, que :

> *« a) la signature électronique résultant de l'utilisation de la technologie ou du procédé est propre à l'utilisateur;*
>
> *b) l'utilisation de la technologie ou du procédé pour l'incorporation, l'adjonction ou l'association de la signature électronique de l'utilisateur au document électronique se fait sous la seule responsabilité de ce dernier;*
>
> *c) la technologie ou le procédé permet d'identifier l'utilisateur;*
>
> *d) la signature électronique peut être liée au document électronique de façon à permettre de vérifier si le document a été modifié depuis que la signature électronique a été incorporée, jointe ou associée au document. »*

Aucun règlement n'a été adopté à ce jour et ce vide a pour effet pratique d'interdire l'application de cette seconde partie de la loi. En l'absence de règlement et, du coup, de signature électronique sécurisée, il devient légalement impossible de se munir d'un document électronique tenant lieu d'original[359], d'apposer l'équivalent électronique

---

356 *Projet de loi C-6*, précité, note 51, art. 31(1).

357 *Id.*, art. 31(1).

358 Le règlement envisagé peut contenir des règles visant la technologie à utiliser pour faire ou envoyer le document électronique ou pour faire ou vérifier une signature électronique (art. 50(2)(a) et 50(2)(e)) ou concernant le format, le lieu et les circonstances relatives à l'envoi et la réception du document électronique (art. 50(2)(b) et 50(2)(d)) et l'existence de présomption (art. 50(2)(c)). Des règles minimales sont également établies pour l'échange de documents ou d'informations électroniques entre personnes privées (art. 50(3)).

359 *Projet de loi C-6*, précité, note 51, art. 42.

d'un sceau[360], de confectionner l'équivalent électronique d'un certificat public admissible en preuve[361], de faire une déclaration sous serment ou une affirmation solennelle sous forme électronique[362], d'obtenir un affidavit électronique[363] ou la signature d'un témoin sur un document électronique[364].

La notion de signature électronique sécurisée n'est pas l'invention du législateur canadien, même si on ne l'a retrouve pas dans la *Loi type*. Le concept de signature renforcée ou sécurisée a été abordé ces dernières années par le Groupe de travail de CNUDCI sur les signatures électroniques, notamment dans le contexte d'infrastructures à clé publique[365]. L'utilité ou le maintien de cette seconde catégorie de signature à degré élevé de fiabilité ferait toujours l'objet d'un débat[366]. Pour l'heure, et dans l'absence d'une réglementation utile, il importe de rappeler que la simple signature électronique pourra satisfaire à l'exigence légale d'une signature, dans les cas prévus à cette fin aux annexes 2 et 3 du *Projet de loi C-6*, lorsque les conditions établies aux règlements à cette fin auront été rencontrées. Aucun règlement n'existe à ce jour et le juriste canadien ne peut qu'attendre et s'en remettre aux principes généraux reconnus dans la *Loi type* et d'autres textes législatifs tels la *LUPE*. Dans les deux cas, on reconnaît

---

360 *Id.*, art. 39.

361 *Id.*, art. 36.

362 *Id.*, art. 44(a).

363 *Id.*, art. 45.

364 *Id.*, art. 46.

365 On comprend des rapports et documents de consultation de ce Groupe de travail que l'apparition du concept de signature renforcée découle de problèmes non résolus liés à l'utilisation de signatures numériques, tel qu'envisagé par l'art. 7 de la *Loi type*. D'abord, à quel moment une technique donnée respectera-t-elle le critère de la fiabilité suffisante de la *Loi type*? Ensuite, comment ignorer que dans la plupart des pays, le destinataire d'une signature doit supporter les conséquences d'une signature qui n'est pas authentique? Ce risque augmente en matière de commerce électronique global transfrontalier. C'est alors qu'aurait été envisagée l'adoption de règles accordant à certaines techniques de signature électronique une valeur juridique supérieure afin de réduire ce risque. Tendant d'abord vers la recherche de signatures numériques appuyées d'une infrastructure à clé publique, les États auraient évolué en vue d'adopter des techniques de signature plus neutres et d'élargir le spectre des signatures électroniques acceptables, tout en haussant leur niveau de fiabilité par référence au concept de signature renforcée ou sécurisée déjà introduit dans les lois de la Californie et de l'Illinois ainsi que dans la *Uniform Electronic Transactions Act*. Rappelons également que le Projet de Règles uniformes prévoit que les signatures électroniques sécurisées bénéficient d'une présomption réfutable selon laquelle le document sur lequel la signature a été apposée n'a pas été modifié depuis qu'il a été signé, que la signature est celle de la personne à laquelle il est lié et que l'auteur de la signature a apposé celle-ci dans le but de signer le document.

366 Pour en connaître davantage concernant les positions qui s'affrontent à ce sujet, consulter le compte rendu de la réunion de janvier 1998 du Groupe de travail de la CNUDCI sur le commerce électronique disponible au site http://canada.justice.gc.ca/ commerce/uncon98-fr-html.

comme fonction fondamentale de la signature l'identification de l'auteur et la confirmation qu'il approuve l'information contenue dans le message de données.

e) Des conditions de forme

La *LUCE* traite de la fourniture d'informations dans un formulaire prévu sous une forme autre qu'électronique. Cette exigence sera satisfaite si certaines conditions sont rencontrées[367]. Un tel article est absent dans la *Loi type* mais trouve écho dans le *Projet de loi C-6* au titre général des moyens électroniques pour transiger avec le gouvernement par l'envoi d'une version électronique d'un formulaire d'origine législative[368]. La question du format demeure problématique si l'on juge qu'il constitue une information relative aux documents électroniques et que la perte ou la modification du format vicie l'intégrité du document, ou sa fiabilité, aux fins de sa conservation et de sa reconnaissance à titre d'original ou d'écrit admissible.

f) L'archivage électronique

Un seul article du *Projet de loi C-6* traite spécifiquement de la conservation de documents électroniques et des équivalences recherchées à cette fin. Il s'agit de l'article 37, libellé en ces termes :

> *« **37.** Dans le cas où une disposition d'un texte législatif exige la conservation d'un document pour une période déterminée, à l'égard d'un document électronique, la conservation du document électronique satisfait à l'obligation si les conditions suivantes sont réunies :*
>
> *a) le document électronique est conservé pour la période déterminée sous la forme dans laquelle il a été fait, envoyé ou reçu, ou sous une forme qui ne modifie en rien l'information qu'il contient;*
>
> *b) cette information sera lisible ou perceptible par quiconque a accès au document électronique et est autorisé à exiger la production de celui-ci;*

---

367 Aux termes de l'art. 6, LUCE, si l'information est fournie dans un formulaire similaire qui comporte le même arrangement visuel, si le document électronique est sous le contrôle de la personne à qui l'information est fournie et si l'information contenue dans le document est accessible et utilisable pour consultation ultérieure.

368 *Projet de loi C-6*, précité, note 51, art. 35(1).

> *c) si le document électronique est envoyé ou reçu, l'information qui permet de déterminer son origine et sa destination, ainsi que la date et l'heure d'envoi ou de réception, doit être conservée. »*

D'une part, on notera que le paragraphe 37(a) reprend l'article 9 de la *LUCE* et l'article 10(1)(b) de la *Loi type* quant aux formes d'archivage préférées ou tolérées s'intéressant, quant aux formes alternatives, à l'intégrité de l'information plutôt qu'à des critères formels[369]. D'autre part, les notions d'accès et de lisibilité énoncées au paragraphe 37(b) sont reprises à l'article 10(1)(b) de la *Loi type*, l'article 9(b) de la *LUCE* et l'article 2837 C.c.Q., et convergent pour autant que l'on accepte que les concepts de lisibilité et d'intelligibilité décrivent une même réalité, en l'occurrence ce qui est compréhensible[370]. Il en est de même de la conservation de certaines métadonnées[371] concernant l'origine et la destination du message ou la date et l'heure d'envoi visées aux paragraphes 37(c) du *Projet de loi C-6*, 9(c) de la *LUCE* et 10(1)(c) de la CNUDCI. On notera que l'article 37 du *Projet de loi C-6* n'aborde pas le recours à l'impartition auprès de tiers, contrairement à l'article 10(3) de la *Loi type*.

Enfin, le *Projet de loi C-6*, pas plus que la *Loi type* ou la *LUCE*, ne prescrit de délai de conservation, préférant s'en remettre aux règles applicables.

g) La preuve

Des équivalents électroniques au document papier et à la signature classique ont peu d'utilité en l'absence d'une reconnaissance judiciaire, d'où la modification nécessaire de la *Loi sur la preuve au Canada*, tout particulièrement de son article 31[372], par l'introduction d'un régime distinct de preuve du document électronique. Ce nouveau régime s'inspire largement des principes inscrits dès 1997 par la CHLC dans la *LUPE*. À titre illustratif, le lecteur pourra noter la similitude des textes en matière d'authentification des documents électroniques[373], de traitement du relevé imprimé[374],

---

369 On pourra se demander si le format d'un document constitue de l'information et, partant, si un changement de format ne limite pas considérablement la portée de l'art. 37(a) du *Projet de loi C-6*, précité, note 51.

370 Voir définition du *Petit Robert*, Dictionnaire de la langue française.

371 L'art. 10(2) de la *Loi type* exclut la conservation de données qui n'ont d'autre objet que de permettre l'envoi ou la réception du message de données, *LUCE*, art. 9(c).

372 Précitée, note 319.

373 *LUPE*, art. 3; *Projet de loi C-6*, précité, note 51, art. 56(31.1).

374 *LUPE*, art. 4(2); *Projet de loi C-6*, précité, note 51, art. 56(31.2(2)).

d'application de la règle de la meilleure preuve[375], de présomption d'intégrité du document électronique[376], de normes applicables pour juger de l'admissibilité du document électronique[377], de preuve par affidavit[378] et de contre preuve[379], sans compter le recours à des définitions de donnée, de document électronique et de système d'archivage électronique analogues[380].

Dit simplement, le législateur fédéral accepte, tel que proposé par la *LUPE*, d'établir l'authenticité et l'intégrité d'un document électronique, et donc d'en permettre l'admissibilité en preuve, par la démonstration de la fiabilité des systèmes informatiques utilisés pour enregistrer, mettre en mémoire et conserver les données de ces documents. La fiabilité des systèmes informatiques se substitue donc à la fiabilité du document électronique. Cette substitution ne garantit pas l'intégrité du document électronique mais permet d'en admettre le contenu en raison du niveau de fiabilité suffisant des systèmes dont il est le produit[381]. Le juge demeure maître d'apprécier la force probante du document, au-delà de son admissibilité.

Cette substitution s'imposait au législateur en raison des attributs du document électronique vu précédemment[382], plus particulièrement de sa dématérialisation, de la désuétude du concept d'original dans les environnements électroniques et de l'existence indépendante de l'information dénuée de tout support physique permanent. En cela, le gouvernement fédéral s'autorise d'un large consensus à l'origine de la *LUPE*, des articles 5 à 10 de la *Loi type*, tout comme l'avait fait le législateur québécois par l'adoption des articles 2837 à 2839 C.c.Q. Ainsi, il incombera à la personne qui cherche à faire admettre un document électronique d'établir sa fiabilité au moyen d'éléments de preuve suffisants dans le respect des règles générales du droit relatives à l'admissibilité de la preuve, à l'exception des règles de droit régissant l'authentification et la meilleure

---

375 *LUPE*, art. 4(1); *Projet de loi C-6*, précité, note 51, art. 56(31.2(1)).

376 *LUPE*, art. 5(a) à 5(c); *Projet de loi C-6*, précité, note 51, art. 56(31.3).

377 *LUPE*, art. 6; *Projet de loi C-6*, précité, note 51, art. 56(31.5).

378 *LUPE*, art. 7; *Projet de loi C-6*, précité, note 51, art. 56(31.6(1)).

379 *LUPE*, art. 8; *Projet de loi C-6*, précité, note 51, art. 56(31.6(2)).

380 *LUPE*, art. 1; *Projet de loi C-6*, précité, note 51, art. 56(31.8).

381 Suivant l'art. 31.8 de la *Projet de loi C-6*, sont assimilés au système d'archivage électronique, le système informatique et tout dispositif semblable qui enregistre ou met en mémoire des données ainsi que les procédés relatifs à l'enregistrement ou à la mise en mémoire de documents électroniques.

382 *Supra*, section 1.1.2.

preuve[383]. Dans ce dernier cas, les exigences de la règle de la meilleure preuve seront satisfaites lorsque la fiabilité du système d'archivage électronique ayant servi à l'enregistrement et à la conservation des documents électroniques sera démontrée[384]. Cette preuve sera facilitée par la présomption de fiabilité établie par l'article 31.3 du *Projet de loi C-6*, ou encore par la présomption annoncée par règlement pris par le gouverneur en conseil à l'égard de documents portant une signature électronique numérisée[385]. Il est intéressant de noter les trois cas d'application donnés à l'article 31.3. Sauf preuve contraire, sera réputé fiable le système d'archivage électronique si la preuve administrée par affidavit[386] ou autrement permet de conclure :

> *« a) qu'à l'époque en cause, le système informatique ou autre dispositif semblable fonctionnait bien, ou, dans le cas contraire, son mauvais fonctionnement n'a pas compromis l'intégrité des documents électroniques, et qu'il n'existe aucun autre motif raisonnable de mettre en doute la fiabilité du système d'archivage électronique;*
>
> *b) que le document électronique présenté en preuve par une partie a été enregistré ou mis en mémoire par une partie adverse;*
>
> *c) que le document électronique a été enregistré ou mis en mémoire dans le cours ordinaire des affaires par une personne qui n'est pas partie à l'instance et qui ne l'a pas enregistré ni ne l'a mis en mémoire sous l'autorité de la partie qui cherche à la présenter en preuve. »*

Le premier cas de figure fonde la présomption sur la preuve de fiabilité du système informatique ayant créé le document électronique et sur celle du système d'archivage électronique utilisé pour le conserver. Cette présomption peut être invoquée par toute personne à l'égard de tout document électronique et n'impose aucun critère quant aux moyens de preuve.

Le second cas de figure renvoie à la preuve documentaire communiquée par une partie, présumément contre son intérêt, dans le cadre d'une procédure de résolution d'un différend. La partie à qui le document électronique est opposé est certes en

---

383 *Projet de loi C-6*, précité, note 51, art. 31.1 et 31.7.

384 *Projet de loi C-6*, précité, note 51, art. 31.2.

385 *Projet de loi C-6*, précité, note 51, art. 31.4. Suivant cet article, l'importance pratique de ces présomptions est indéniable compte tenu du statut plus que privilégié conféré à la signature électronique sécurisée telle que vue précédemment.

386 *Projet de loi C-6*, précité, note 51, art. 31.6.

possession des informations susceptibles de réfuter la présomption, alors que la proposition inverse n'est pas nécessairement vraie, d'où la présomption. En pratique, cependant, il faut convenir que la preuve par cette partie des lacunes de ses propres systèmes informatiques est pour le moins inusitée au plan commercial et risquée en ce qu'elle fournit à l'adversaire des moyens de contestation de l'admissibilité de la preuve électronique de cette partie.

Le troisième scénario rappelle l'exception à la règle du ouï-dire concernant les documents d'affaires ou bancaires en élargissant ces exceptions pour les étendre à toute organisation, y compris des organisations à but non lucratif. La présomption exclut la partie et la personne sous l'autorité d'une partie à l'instance, le tiers archiviste par exemple.

Ajoutons que ces trois cas de figure ne sont pas mutuellement exclusifs et une personne pourra se rabattre sur la présomption visée à l'article 31(3)(a) si elle ne peut bénéficier des allègements apportés par les paragraphes (b) et (c).

Soulignons également l'apport de l'article 31.5 aux fins de l'élaboration de la Convention.

> *« 31. Afin de déterminer si, pour l'application de toute règle de droit, un document électronique est admissible, il peut être présenté un élément de preuve relatif à toute norme, toute procédure, tout usage ou toute pratique touchant la manière d'enregistrer ou de mettre en mémoire un document électronique, eu égard au type de commerce de l'entreprise qui a utilisé, enregistré ou mis en mémoire le document électronique ainsi qu'à la nature et à l'objet du document. »*

D'une part, le législateur y reconnaît la pertinence des normes et des usages commerciaux ou techniques qui seront, nul doute, abondamment évoqués au soutien des expertises produites, sous forme d'affidavits, concernant la fiabilité du système d'archivage électronique. D'autre part, le tribunal pourra considérer, lors de l'instruction de la preuve, le type d'entreprise ou de commerce concerné ainsi que la nature et l'objet des documents électroniques. Les parties à la Convention auront donc tout intérêt, bien que le *Projet de loi C-6* ne le rende pas obligatoire, de connaître et de suivre les normes prévalant dans leur secteur d'activités[387], de comparer les produits technologiques

---

[387] Par exemple, les normes ISO ou celles publiées par l'Association canadienne concernant l'imagerie électronique et l'utilisation de microfilms.

envisagés et leurs caractéristiques, à ceux dominant les marchés et de prévoir, le cas échéant, des catégories de documents électroniques selon leur importance stratégique pour l'entreprise. De plus, rien n'interdit aux parties à la Convention de se doter de leurs propres normes internes ou de normes applicables conçues aux fins de la Convention afin d'établir, en temps opportun, leur adhésion à ces normes[388].

Ajoutons que le *Projet de loi C-6* n'exige pas la production de la version originale papier d'un document numérisé, pour autant que les critères de fiabilité prévus sont rencontrés, ni ne permet de tirer une inférence négative de la destruction de l'original dans le cadre normal des affaires.

Enfin, un régime distinct est prévu pour les sorties imprimées. Sauf preuve contraire, le document électronique sous forme de sortie imprimée satisfera la règle de la meilleure preuve si la sortie imprimée a, de toute évidence ou régulièrement, été utilisée comme document relatant l'information enregistrée ou mise en mémoire[389]. Cette disposition serait justifiée en raison des fichiers électroniques transitoires effacés après usage. L'exemple du courrier d'affaires est donné[390]. Une lettre est d'abord créée à l'aide d'un logiciel de traitement de textes puis imprimée et conservée sous forme papier. La version électronique est subséquemment détruite, laissant seule la copie papier comme moyen de preuve. L'article 31.2(2) du *Projet de loi C-6* permet d'offrir cette copie papier à titre de meilleure preuve.

2.2.2.4 La *Loi sur la preuve* du Nouveau-Brunswick

Le régime de preuve électronique en vigueur au Nouveau-Brunswick depuis 1996 mérite d'être souligné, d'abord parce qu'il constituait une première canadienne[391], ensuite parce qu'il témoigne d'une approche qui se veut sensible, peut-être trop d'ailleurs, aux pratiques d'entreprises. L'approche est simple et se présente en deux temps.

---

388 Il s'agit d'ailleurs là d'une suggestion de la CHLC qui défend la validité et le caractère exécutoire de la Convention relative à la preuve et à l'archivage du document électronique.

389 *Projet de loi C-6*, précité, note 51, art. 56(31.2(2))

390 *LUPE*, commentée par la CHLC, disponible au site http://www.law.ualberta.ca/alri/ulc/current/eeeact.htm.

391 En effet, par amendement à la *Loi sur la preuve* du Nouveau-Brunswick, c. E-11, amendée en 1996 c. 52, le législateur du Nouveau-Brunswick innovait par l'ajout, aux articles 47.1 et 47.2, d'un régime autonome de preuve du document conservé électroniquement. La Loi est disponible au site http://www.gov.nb.ca/acts/lois/e-11.htm.

Une première disposition, l'article 47.1, s'intéresse aux documents sur support papier reproduits sous forme électronique. Dans ce cas, une sortie sur imprimante est admissible en preuve dans tous les cas et pour toutes les fins pour lesquelles le document original eût été admissible, à condition : (1) que le document original a été copié par un procédé de prise d'images électroniques ou un procédé semblable et a été enregistré ou conservé électroniquement dans le cours d'une pratique établie afin de garder une preuve permanente du document, (2) que le document original a été détruit après avoir été copié et enregistré ou conservé conformément à l'alinéa 1 et (3), que la sortie sur imprimante est une copie certifiée conforme du document original[392]. La preuve que ces conditions ont été rencontrées peut être livrée oralement ou par affidavit notarié par toute personne qui a connaissance des faits[393].

On rappellera la pertinence pour l'entreprise d'établir et de documenter l'existence et le respect d'une politique d'archivage, tant au plan administratif que probatoire. L'obligation statutaire de détruire l'original a le mérite de justifier une décision autrement risquée au plan de la preuve et de résoudre certaines difficultés posées par la règle de la meilleure preuve en présence de l'original papier[394]. Enfin, à l'instar du régime québécois, la présence et le témoignage d'un représentant de l'entreprise sera, en pratique, nécessaire pour l'admissibilité de l'imprimé.

Les lacunes de ce premier article émanent de sa simplicité. D'abord, l'article 47.1 est avare de précisions quant aux conditions de temps, de lieux et d'attestation de la numérisation, contrairement au régime québécois. Ensuite, l'article 47.1 demeure muet quant à la fiabilité du processus de numérisation à l'origine de la copie électronique et du système d'archivage électronique duquel provient le relevé imprimé. L'article 47.1 préfère plutôt aborder, en aval, la conformité du relevé imprimé au document original, au moment de la numérisation. Or, l'original étant subséquemment détruit, toute altération en cours d'archivage pourrait théoriquement échapper au témoin, faute d'outils comparatifs. Aussi, l'absence cumulative de conditions strictes à l'étape de

---

392 *Loi sur la preuve*, précitée, note 391, art. 47.1(3).

393 *Loi sur la preuve*, précitée, note 391, art. 47.1(4).

394 En effet, au Québec, nous avons vu que la destruction volontaire de l'original papier peut faire perdre le bénéfice de l'article 2860 C.c.Q. en cas d'impossibilité de produire la meilleure preuve. Voir l'obligation de détruire l'original suivant le régime des articles 2040 à 2042 C.c.Q. traité à la section 2.2.1.3.

la numérisation et de la preuve de fiabilité des systèmes d'archivage électronique[395] risquent d'engendrer des débats à la Cour. En pratique, toute contestation de la recevabilité du document électronique mènera le juge à considérer l'ensemble des circonstances relatives à l'environnement dans lequel les informations offertes ont été saisies, inscrites, conservées et reproduites électroniquement.

Un second article, l'article 47.2, vise le document directement créé sous forme électronique. Lorsque, dans le cours normal des affaires, un document[396] créé sous forme électronique est conservé électroniquement afin d'en garder une preuve permanente, une sortie sur imprimante du document engendré par des archives informatiques ou sur support électronique est admissible en preuve dans tous les cas et pour toutes les fins pour lesquelles le document eût été admissible s'il avait été créé sous une forme tangible. Certaines conditions doivent cependant être rencontrées. Premièrement, le document doit être enregistré ou conservé électroniquement dans le cours normal des affaires ou des affaires internes de l'entreprise[397]. Deuxièmement, le contenu du document offert doit être tel qu'il a été originalement enregistré et conservé et ne pas avoir été altéré[398]. La référence au cours normal des affaires fait écho à l'exception à la règle d'exclusion du ouï-dire concernant le document d'affaires[399] et l'étend aux documents internes non directement liés au commerce de l'entreprise. La condition de maintien de l'intégrité du document, exprimée en termes simples et onéreux au plan technique, n'est allégée d'aucune présomption de fiabilité du document liée à la fiabilité des systèmes informatiques en cause, contrairement au régime québécois[400] et requiert une preuve orale ou par affidavit notarié[401].

On déduit de ces textes que le législateur du Nouveau-Brunswick est prêt, à des fins probatoires, à reconnaître le document électronique en tout point exact à l'original papier ou l'original électronique intègre, pour autant que cette conformité ou

---

395 Si ce n'est par l'emploi du mot « permanent » à l'art. 47.1(3)(b) et la reconnaissance du concept d'archive électronique à l'art. 47.1(2).

396 Aux fins de l'art. 47.2, le mot « document » comprend, à moins que le contexte ne l'exige autrement, tout enregistrement de renseignements, peu importe la façon dont ils sont enregistrés ou conservés, que ce soit sous forme imprimée, sur pellicule, par moyen électronique ou autrement.

397 *Loi sur la preuve*, précitée, note 391, art. 47.2(2)(a).

398 *Loi sur la preuve*, précitée, note 391, art. 47.2(2)(b).

399 Art. 2870 C.c.Q.

400 Art. 2838 C.c.Q.

401 *Loi sur la preuve*, précitée, note 391, art. 47.2(3).

cette intégrité, jugée dans l'environnement normal des affaires de l'entreprise, puisse être prouvée de façon directe plutôt que par référence à l'environnement électronique duquel il émane. Cela dit, le plaideur ne pourra éviter, en pratique, de prouver la fiabilité de cet environnement.

2.2.2.5 Le *Electronic Information and Document Act* de la Saskatchewan

En décembre 1999, l'Assemblée législative de la province de la Saskatchewan déposait en première lecture le projet de loi 11 intitulé « *An Act Respecting Electronic Information and Document* »[402]. Ce projet de loi dédiée à la reconnaissance du document et de la signature électroniques rappelle la *Loi type* à maints égards en reprenant le principe de non-discrimination et en s'attaquant aux exigences de forme et de fond susceptibles d'interdire le dépôt en preuve du document dématérialisé.

Ce projet de loi entend lier la Couronne provinciale[403]. Sa portée est cependant réduite pour exclure certains actes juridiques spécifiques[404] et donner préséance à d'autres lois[405]. Le dispositif prévu est simple. Il prévoit qu'aucun document ou renseignement ne doit être privé d'effet juridique contraignant du seul fait qu'il est sous forme électronique[406]. L'exigence légale d'un écrit est satisfaite par le document électronique accessible pour utilisation future par un tiers[407]. Des conditions de forme sont remplies par le document électronique accessible à un tiers dans une forme identique ou substantiellement équivalente et susceptible d'être retenue par cette personne pour utilisation future[408]. Le document électronique sert d'original s'il existe une garantie fiable de l'intégrité de l'information qu'il contient depuis sa création, que ce document ait été à l'origine un document papier ou non, et qu'il demeure accessible et susceptible d'être retenu par la personne à qui il s'adresse pour utilisation future[409]. La notion d'intégrité repose sur le maintien d'un document complet, exempt d'altérations, à l'exception de modifications survenant dans le cadre normal de la communication, de

---

402 *An Act Respecting Electronic Information and Document*, Projet de Loi 11, Législature de la Saskatchewan.

403 *Id.*, art. 5.

404 *Id.*, art. 3(1) et 3(2).

405 *Id.*, art. 3(3) et 3(4).

406 *Id.*, art. 6.

407 *Id.*, art. 8 et 9.

408 *Id.*, art. 10.

409 *Id.*, art. 11(1) et 11(2).

l'archivage ou de sa présentation[410], tenant compte de sa finalité[411] et des autres circonstances pertinentes. Le projet de loi 11 reconnaît la signature électronique fiable aux fins de l'identification de la personne[412] et de l'établissement d'un lien entre cette personne et le document électronique, suivant sa finalité[413].

En matière d'archivage, il est dit que tout ministère ou agence du gouvernement pourra utiliser la forme électronique pour entreposer un document, sauf stipulation contraire dans une loi[414]. D'autres dispositions traitent de la formation de contrat en ligne[415], du rôle d'intermédiaires[416], de l'effet relatif des documents électroniques grevés d'erreurs[417] ou de la vente d'effets[418].

En bref, le législateur de la Saskatchewan s'en est tenu à des principes connus. Ce projet de loi confirme tout de même l'importance d'assurer la fiabilité des systèmes informatiques de création et d'archivage des documents électroniques et la sécurité de l'environnement à l'intérieur duquel ces systèmes évoluent.

2.2.2.6 Le *Uniform Electronic Transactions Act*

Aux États-Unis, la *National Conference of Commissioners on Uniform State Laws*, pendant américain de la Conférence pour l'harmonisation des lois au Canada, publiait en août 1999 le *Uniform Electronic Transactions Act* (le « UETA »)[419].

L'UETA a pour objet le document et la signature électroniques[420] dans le cadre de relations contractuelles et traite, à l'instar d'autres textes législatifs, des

---

410 *Id.*, art. 11(3)(a).

411 *Id.*, art. 11(3)(b).

412 *Id.*, art. 14(a).

413 *Id.*, art. 14(b).

414 *Id.*, art. 17.

415 *Id.*, art. 18.

416 *Id.*, art. 19.

417 *Id.*, art. 20.

418 *Id.*, art. 22.

419 Ce projet de loi uniforme est disponible au site http://www.law.upenn.edu/library/ulc.

420 *UETA*, art. 3.

questions d'écrit[421], d'original[422], d'archivage[423], d'admissibilité en preuve[424], d'identification[425] et de forme[426]. En fait, l'UETA s'inspire largement de la *Loi type* en ce qu'on y trouve bien incarné le principe de non-discrimination à l'égard du document, de la signature et du contrat électroniques[427] ainsi que la recherche d'équivalents fonctionnels[428].

L'UETA vise avant tout les relations prévues entre partenaires commerciaux convenus de transiger à l'aide de moyens électroniques[429], sans pour autant créer d'obligation de commercer à l'aide de tels moyens[430], et leur reconnaît le droit de déroger à ses dispositions par contrat,[431] sauf exception[432]. Ce projet vise également, de façon distincte, les agences gouvernementales qui conservent un droit discrétionnaire d'accepter des documents ou des signatures électroniques et d'y recourir aux fins d'exercer leurs fonctions auprès des administrés de l'État[433]. Les critères de fiabilité, d'intégrité, d'accessibilité, de lisibilité ou d'inaltérabilité vus précédemment lors de l'examen de la *Loi type* sont essentiellement repris par l'UETA[434].

2.2.2.7 Le *Utah Digital Signature Act*

La recherche de balises en matière de preuve et d'archivage électronique conduit à l'étude des règles encadrant l'activité des autorités de certification chargées d'attester l'existence « *d'un lien formel entre une personne et une paire de clés*

---

421 *Id.*, art. 8.

422 *Id.*, art. 12.

423 *Id.*, art. 12 et 13.

424 *Id.*, art. 13.

425 *Id.*, art. 9.

426 *Id.*, art. 12.

427 *Id.*, art. 7.

428 *Id.*, art. 8, 9, 10, 11 et 12 inclusivement.

429 *UETA*, art. 5(b).

430 *Id.*, art. 5(c).

431 *Id.*, art. 5(d).

432 *Id.*, art. 8(3)(d), pour citer un exemple en matière de contenu minimal du document électronique.

433 *Id.*, art. 17 et 18.

434 Il n'est pas utile, aux fins du présent exposé, de nous attarder aux différentes interprétations des textes ou de modalités de mise en œuvre de ces grands principes vus précédemment si ce n'est pour référer le lecteur à certains auteurs. Consulter les commentaires de droit comparé joints à la *Loi uniforme sur le commerce électronique au Canada* du CHLC au site http://www.law.ualberta.ca/abri/ulc/acts/fueca.htm.

asymétriques »[435] par l'émission d'un certificat d'identification, véritable document électronique échangé entre partenaires commerçant sur les inforoutes.

Dans le cours normal des affaires, ces autorités doivent conserver une quantité impressionnante d'informations relatives aux certificats émis, suspendus ou révoqués et démontrer le caractère diligent et raisonnable du processus ayant mené à l'émission, à la suspension ou à la révocation de certificats, notamment dans le cadre de litiges. En mai 1995 entrait en vigueur le *Utah Digital Signature Act*[436], l'une des premières lois, sinon la première loi consacrée à la signature numérique et plus généralement à la certification. Les paragraphes R-154-10-303, (5) et (6) des *Digital Signature Administrative Rules* édictés en application de l'article 501(1)(f) du *Utah Digital Signature Act* se lisent comme suit :

> *« (5) A licensed certification authority shall retain its records of the issuance, acceptance, and any suspension or revocation of a certificate for a period of not less than 10 years after the certificate is revoked or expires. The licensed certification authority shall itself retain custody of such records unless the licensed certification authority turns over its records to the division of another licensed certification authority upon ceasing to act as a certification authority.*
>
> *(6) A licensed certification authority shall keep its records under circumstances of safekeeping and security which are commercially reasonable in light of the recommended reliance limits of the certificates. »*[437]

Ces dispositions sont d'intérêt parce qu'elles fixent la durée de conservation des documents électroniques à un minimum de dix ans et imposent à l'agent certificateur l'obligation personnelle d'archiver, à l'exclusion de toute sous-traitance, sauf en cas de cessation d'activités.

Au titre des équivalences fonctionnelles auxquelles nombre d'initiatives législatives nous ont habitués, la loi de l'Utah se distingue par la spécificité de l'approche choisie. Cette approche adhère strictement à l'utilisation d'algorithmes de signature numérique par cryptographie à clé publique et reconnaît cette signature pour autant qu'elle soit vérifiée par référence à la clé publique contenue dans un certificat d'identification émis par une autorité de certification. Il importe que la signature

---

435 S. PARISIEN, P. TRUDEL, V. WATTIEZ-LAROSE, *op. cit.*, note 24, p. 117.

436 *Utah Digital Signature Act*, Administrative Rules, Utah Administrative Code R-154-10.

437 *Id.*, R-154-10-33(5) et (6).

numérique soit apposée par son détenteur avec l'intention de signer et de faire sien le message de données. Il importe également que le récipiendaire soit dans l'ignorance d'une quelconque situation susceptible de compromettre la clé[438].

L'approche est similaire quant à l'exigence d'un écrit, sachant que le document signé numériquement constituera un écrit valide et exécutoire s'il porte la signature numérique complète de son auteur vérifiée par l'émission d'un certificat valable auprès d'une autorité de certification licenciée[439]. On dira également que la copie d'un message signé numériquement aura la valeur de l'original sauf si l'auteur choisit d'élire à titre d'original unique une version du document électronique qu'il désigne à cette fin[440].

2.2.2.8 La Directive du Parlement européen

Le 13 décembre 1999, le Parlement européen et le Conseil de l'Union Européenne proposait la Directive 1999/93/CE[441]. L'objectif de cette Directive est de faciliter l'utilisation des signatures électroniques et de certains services de certification et de contribuer à leur reconnaissance juridique. À cette fin, la Directive demande aux États membres qu'ils veillent à ce que les signatures électroniques[442] répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier et qu'elles soient recevables comme preuve en justice[443]. Ils doivent également veiller à ce que l'efficacité juridique et la recevabilité comme preuve en justice d'une signature électronique ne soient pas refusées au seul motif que la signature se présente sous forme électronique, qu'elle ne repose pas sur un certificat qualifié ou qu'elle n'est pas créée par un dispositif sécurisé de création de signatures[444]. La Directive propose un cadre uniforme pour la prestation de services de certification des

---

438 La Règle 46-3-401, paragraphe c) du *Utah Digital Signature Act* prévoit en effet que « *the recipient has no knowledge or notice that the signer either breached a duty as a subscriber; or ii) does not rightfully hold the private key used to affix the digital signature* ».

439 *Id.*, Règle 46-3-403.

440 *Id.*, Règle 46-3-404.

441 Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, Journal officiel, no. L 013 du 19/01/2000, p. 0012-0020.

442 Le concept de signature électronique est défini pour inclure toute « donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification », Directive, article 2.

443 Directive, précitée, note 441,article 5.1.

444 Directive, précitée, note 441, article 5.2.

signatures électroniques, insistant sur l'interopérabilité des produits de signature afin de garantir le bon fonctionnement du marché intérieur. Bien que la Directive ne porte pas sur l'utilisation de documents électroniques, elle met en relief l'importance d'une uniformisation de traitement et souligne à juste titre que « toute divergence dans les règles relatives à la reconnaissance juridique des signatures électroniques et à l'accréditation des prestataires de services de certification dans les États membres risque de constituer un sérieux obstacle à l'utilisation des communications électroniques ou au commerce électronique »[445]. Ce souci d'uniformisation est à l'origine du principe de conformité évoqué précédemment[446] qui nous paraît fondamental dans l'élaboration de la Convention.

2.2.3 Des normes et pratiques pertinentes ou l'adhésion *de facto* à la Convention

2.2.3.1 Les contrats d'échange de données informatisées ou l'EDI.

L'entreprise fait appel à la télématique depuis de nombreuses années pour conclure des transactions commerciales[447]. Ce commerce électronique rendu possible grâce à des ordinateurs interconnectés s'effectue véritablement sans intervention humaine par le transfert de données à haute vitesse et à coût réduit, suivant des protocoles d'échanges et un langage codé. Ainsi, les parties procèdent à l'échange de données informatisées (EDI) dans le cadre de conventions négociées pour normaliser leur relation et répondre à des besoins commerciaux spécifiques. Ces conventions d'ordre privé ont pour objet, notamment, de gérer le risque juridique inhérent à cette nouvelle manière de transiger. Il est donc utile de référer à certains modèles contractuels reconnus pour connaître les réponses proposées en matière d'archivage et de preuve.

Certains modèles de contrats semblent s'imposer selon la doctrine consultée : les *Règles de conduite uniformes pour l'échange de données commerciales par télétransmission* de la Chambre de Commerce Internationale (« UNCID »), le *Standard Electronic Data Interchange Agreement* (« EDIA ») de *l'EDI Association of the United Kingdom*, le *Model Electronic Data Interchange Trading Partner Agreement* de

---

445 Directive, précitée, note 441, dispositions introductives, paragraphe 4.

446 *Infra*, section 2.1.

447 Référence est faite notamment au secteur du transport maritime, du commerce au détail de produits alimentaires et du transport aérien. Voir également, B. WRIGHT, J. WINN,, *op. cit.*, note 92, ch. 12, *Clarifying the Legal Status of Electronic Commerce through Contracts*, p. 12-1 et ss.

l'Association du Barreau Américain (« ABA »), le contrat type d'interchange du Centre International de Recherche et d'Étude de Droit de l'Informatique et des Télécommunications (« CIREDIT »), le *Standard EDI Agreement* publié par le *New-Zealand Electronic Data Interchange Association* (« NZEDIA »), les *Guidelines for Interchange Agreement* de l'Organisation l'Interchange par Télécommunication en Europe (« ODETTE »), le *Model Electronic Data Interchange Agreement* de l'*EDI Counsel of Australia* (« EDICA ») et enfin, plus près de chez nous au Québec, le contrat type commenté proposé par des chercheurs du Centre de recherche en droit public de l'Université de Montréal (« CRDP »). L'étude comparative de ces modèles révèle une structure en trois axes centrés sur des aspects techniques, des aspects de sécurité et des considérations que nous qualifierons de juridiques. C'est dans ce troisième axe que l'on aborde l'essentiel des dispositions en matière de conservation et de preuve.

En matière d'archivage, tous ces contrats-types imposent aux parties, en des termes semblables, l'obligation de créer, de mettre à jour et d'assurer la protection de registres pour la conservation des messages de données envoyés et reçus dans le cours des affaires. Cette obligation est de durée variable[448] suivant les exigences légales applicables et les besoins des parties[449], de façon à leur garantir en temps utile l'authentification des documents électroniques et l'intégrité de leur contenu. Les messages de données, comprenant les métadata[450], doivent être archivés sans modification[451] et pouvoir être récupérés[452], imprimés[453] et lus[454], parfois suivant un format prédéterminé[455]. Le témoignage de l'archiviste responsable peut être requis par Convention pour certifier l'exactitude de toute reproduction,[456]. De même, les parties pourront stipuler des vérifications internes périodiques du contenu de leurs registres

---

448 Un an, CIREDIT, art. 7.3; trois ans, UNCID, art. 10(c); sept ans, EDICA, art. 5; des durées indéterminées sont laissées à la discrétion des parties dans EDIA, art. 7.2 et NZEDIA, art. 7.2.

449 CIREDIT, art. 7; EDIA, art. 7.2; NZEDIA, art. 7.2; ODETTE, art. 6.

450 *Supra*, note 60. Particulièrement les données relatives à la datation et l'horodation; par exemple, CRDP, art. 6.5.

451 CIREDIT, art. 7; UNCID, art. 10(c); EDIA. art. 7.1; NZEDIA, art. 7.1; CRDP art. 6.2(1); ODETTTE, art. 6.

452 UNCID, art. 10(b); EDIA, art. 7.3; ODETTE, art. 6; EDICA, art. 5.

453 CIREDIT, art. 7; CRDP, art. 6.2(1).

454 UNCID, art. 10(b); EDIA, art. 7.3; CRDP, art. 6.2(1); ODETTE, art. 6; EDICA, art. 5.

455 NZEDIA, art. 7.3.

456 UNCID, art. 10(d); EDIA, art. 7.5; NZEDIA, art. 7.5; CRDP, art. 6.2(5); ODETTE, art. 6.

respectifs[457]. Des procédures distinctes d'audit peuvent être établies[458] suivant la nature du document, sa finalité, sa confidentialité ou son caractère privilégié. Le recours au tiers archiviste[459] ou au vérificateur[460] de registres est reconnu dans certains modèles, à certaines conditions, notamment à l'égard du maintien de la responsabilité contractuelle de la partie ayant recours à l'intermédiaire externe[461].

En matière de preuve, l'essentiel des dispositions contractuelles insérées dans ces modèles de contrats d'EDI visent à faire reconnaître par les parties et sanctionner par le droit national le statut des messages de données, leur admissibilité en preuve et leur force probante à l'égard des échanges qu'ils attestent. L'une des voies privilégiées pour ce faire, certes inspirée par les débats liés à l'élaboration de la *Loi type*, repose sur les principes de non-discrimination et d'équivalence fonctionnelle : d'une part, les parties renoncent à contester l'utilisation ou la recevabilité du message de données du seul fait qu'il constitue un document électronique[462]; d'autre part, elles confèrent à ces messages la qualité d'équivalents fonctionnels aux fins probatoires pour lesquelles ils sont créés[463]. Concrètement, ces principes seront appliqués aux notions de signature, d'écrit, d'original et de force probante. Ainsi, les parties conviennent, sauf circonstances particulières[464], que la signature électronique apposée sur le document EDI aura la même valeur et liera les parties de la même manière que la signature manuscrite[465]. Elles reconnaissent la qualité d'écrit[466] et d'original [467] aux documents EDI, comme s'il s'agissait de documents sur support papier[468]. Elles s'entendent pour que les registres de transactions soient admissibles dans le cadre d'une procédure de résolution de conflits, y compris des

---

457 CRDP, art. 6.2(6).

458 CIREDIT, art. 8; ABA, art. 1.4.

459 UNCID, art. 10(d); EDIA, art. 7.4.

460 CRDP, art. 5.6.

461 EDIA, art. 8; NZEDIA, art. 8; ODETTE, art. 4; ABA, art. 1.2.3.

462 CRDP, art. 6; EIDA, art. 5.1; ABA, art. 3.3.4; EDICA, art. 8; ODETTE, art. 8.

463 CRDP, art. 6; ABA, art. 3.3.3 et 3.3.4; NZEDIA, art. 5.1.

464 Les modèles CIREDIT et NZEDIA donnent l'exemple de la fraude ou de la corruption des systèmes informatiques.

465 CRDP, art. 6.1; ABA, art. 1.5 et 3.3.2; CIREDIT, art. 6; EDICA, art. 3 et 8.

466 CRDP, art. 6.3(1); ABA, art. 3.3.2; CIREDIT, art. 2; EDICA, art. 8.

467 CRDP, art. 6.3(1); ABA, art. 3.3.2; CIREDIT, art. 2.

468 CRDP, art. 6.3(1); ABA, art. 3.3.2 et 3.3.4. L'art. 2 du modèle CIREDIT donne une priorité aux documents EDI, tels que définis par les parties, ne donnant à la copie papier qu'une valeur confirmative.

procédures judiciaires, et qu'ils feront alors preuve de leur contenu comme s'il s'agissait de documents originaux[469].

On notera que ces dispositions en matière de preuve sont libellées en termes généraux servant à intégrer ces principes au cadre particulier de l'EDI, sans préciser de modalités d'application adaptées à un type particulier de commerce électronique. L'application de ces principes n'a pas, en soi, pour effet d'interdire aux parties de contester l'admissibilité ou de miner la force probante de documents électroniques pour d'autres raisons que celle de leur dématérialisation, ni d'exclure d'autres conditions d'admissibilité qui seraient imposées par le droit substantif régissant les parties. Référence peut être faite, par exemple, aux conditions et présomption de fiabilité des inscriptions informatisées visées aux articles 2837 à 2842 C.c.Q. L'application de ces principes ne pourrait davantage déplacer des règles de preuve d'ordre public.

2.2.3.2 Le projet d'infrastructure à clé publique du gouvernement fédéral

En 1993, sous la direction du Centre de la sécurité des télécommunications, et en collaboration avec des partenaires ministériels, le gouvernement fédéral confiait au groupe Bell Northern Research[470] le mandat d'établir une autorité de certification œuvrant à l'intérieur d'une infrastructure à clé publique (« ICP »).

L'ICP a pour objectif déclaré d'aider le gouvernement fédéral à atteindre son objectif de mener le plus d'activités possibles par la voie électronique, de faciliter le commerce électronique à l'échelle nationale et internationale dans un environnement sûr et d'appuyer la vision du gouvernement consistant à faire du Canada la nation la plus branchée du monde[471]. L'ICP sert donc à créer l'environnement de confidentialité et de confiance nécessaire pour les opérations électroniques protégées du gouvernement fédéral par l'utilisation de clés pour le chiffrement et de signatures numériques assurant la confidentialité de l'information, l'authentification des intervenants, l'intégrité des données, la non-répudiation des actes et le contrôle de l'accès. De son côté, l'autorité de certification constitue un véritable tiers de confiance. Ses services d'identification, de vérification et de gestion des clés destinées à la signature numérique et au chiffrement ont pour fonction essentielle d'établir un lien entre une personne et une paire de clés

---

469 CRDP, art. 6.3(1); ABA, art. 3.3.4; CIREDIT, art. 2.

470 Maintenant Entrust Technologies Limited.

471 Secrétariat du Conseil du Trésor du Canada, relativement à l'ICP du gouvernement fédéral disponible au site http ://www.cio-ppi.gc.ca/pki/initiatives/initiatives-f.html.

asymétriques. Depuis 1993, le développement d'une ICP fédérale s'est appuyé sur un réseau de ministères et d'organismes fédéraux, de comités et de groupes de travail dédiés à l'architecture de l'ICP et à l'élaboration de politiques de certification reflétant le niveau d'assurance offert par diverses catégories de certificats. Or, ces certificats constituent des documents électroniques, d'où notre intérêt en matière de conservation.

Cette question est abordée dans le cadre des politiques de certification[472]. Il y est prévu que la documentation relative à la vérification des certificats et l'intégrité des systèmes en assurant l'exactitude soit conservée pendant une période minimale de six ans et qu'une copie de sécurité soit archivée dans un autre site doté d'équipement de sécurité physique, atmosphérique et technologique. L'intégrité du contenu de la documentation conservée doit être vérifiée de façon périodique. Les observateurs de l'ICP du gouvernement fédéral soulignent l'importance de « *prévoir une période minimale [de conservation] et d'obliger l'utilisateur à demander une période de conservation plus longue ou plus courte, consulter chaque ministère clé afin d'établir la période de conservation nécessaire, et informer l'utilisateur de l'expiration de la période de conservation avant de détruire ou de transférer des documents donnant ainsi à l'utilisateur la possibilité de réévaluer ses besoins*»[473]. En cela, l'ICP du gouvernement fédéral tient compte de diverses exigences d'origine statutaire[474]. L'ICP reconnaît également les besoins particuliers des utilisateurs qui voudront conserver des documents pendant des années dans le but de se défendre en cas de poursuites ou d'établir la propriété de certains biens.

2.2.3.3 Les *Digital Signature Guidelines* de l'ABA

En 1995, l'*American Bar Association* publiait les *Digital Signature Guidelines*[475] avec pour principal objectif de faciliter le commerce électronique et mettre de l'avant des méthodes d'authentification fiables. L'article 3.5 de ces *Guidelines*, au titre

---

472 Consulter le *Digital Signature and Confidentiality Certificate Policies* publié en avril 1999, version 3.02 du gouvernement fédéral, notamment la clause 4.6. Des modèles d'ententes contractuelles conclues entre l'autorité de certification et l'abonné aux fins de l'émission du certificat sont disponibles au site http ://www.tbs-sct.gc.ca/pubs-pol/ciopubs/pki/pki3-f.html.

473 Chapitre 10, Signature numérique, Chiffrement de confidentialité et Infrastructure à clé publique, p. 26 de 37, disponible au site http://Canada.justice.gc.ca/commerce/chapitre/ ch10fr.txt.

474 Dont celles incluses dans la *Loi sur les archives nationales*, la *Loi canadienne sur les sociétés par actions*, la *Loi sur les banques*, la *Loi de l'impôt sur le revenu*, la *Loi sur l'assurance-chômage*, le *Régime de pension du Canada* et la *Loi sur la gestion des finances publiques*.

475 « *Digital Signature Guidelines* (« Guidelines ») disponibles au site http ://www.law.vill.edu/v/s/ student_home/courses/computer-law.

des registres, prévoit que la « *certification authority must (1) document all facts material to the issuance, suspension or revocation by it of a certificate and (2), retain that documentation for an appropriate period of time.* » Cette durée n'est pas spécifiée, quoique certains facteurs pertinents sont mentionnés dont les « *contractual obligations to subscribers, statutory record retention requirements, and business needs, »*, à savoir des facteurs similaires à ceux identifiés à la section 1.1.3 des présentes, auxquels doit s'ajouter le maintien de l'admissibilité des moyens de preuve en cas de différends.

La notion de signature électronique est ici réduite à celle de signature numérique, tel qu'envisagée par la cryptographie asymétrique[476]. Comme pour le *Utah Digital Signature Act*, les exigences visant l'écrit[477], la signature[478] et l'original[479] sont essentiellement satisfaites par l'apposition d'une signature numérique vérifiée et l'émission d'un certificat d'identification confirmant le lien entre l'auteur du message et la clé publique contenue dans ce certificat. Par ailleurs, l'article 5.3 des *Guidelines* prévoit certaines situations où la signature numérique n'offre pas les garanties de fiabilité suffisantes pour sa reconnaissance alors que l'article 5.4 identifie des critères propres à permettre cette évaluation. Enfin l'article 5.5 établit certaines présomptions réfragables liées à l'utilisation de la signature numérique vérifiée par certificat facilitant la preuve de la confection et de l'intégrité du contenu du document électronique signé et de son admissibilité en preuve, sous réserve d'une preuve contraire laissée à la partie s'opposant au document numérique[480].

---

476 L'art. 1.11 des *Guidelines* définit la signature numérique comme « *a transformation of a message using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and 2), whether the initial message has been altered since the transformation was made.* »

477 L'article 5.1 des *Guidelines* prévoit qu'un message « *bearing a digital signature verified by the public key listed in a valid certificate is as valid, effective and enforceable as if the message had been written on paper.* »

478 L'article 5.2 des *Guidelines* prévoit que « *where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature which is (1) affixed by the signer with the intention of signing the message and (2) verified by reference to the public key listed in a valid certificate.* »

479 L'article 5.3 des *Guidelines*.

480 À titre illustratif, l'article 5.6 crée une présomption que le contenu du message d'un document signé numériquement n'a pas été altéré depuis sa création et que l'information qu'il contient est correcte depuis sa signature. Il est également présumé que la clé publique apparaissant sur le certificat appartient au signataire.

2.3 DU CONTENU DE LA CONVENTION

Partant de l'identification d'un principe de conformité[481], nous avons étudié divers régimes normatifs[482], avec pour objectif d'en extraire ce qui permettra d'élaborer un outil conventionnel efficace de gestion de risques juridiques. À notre avis, l'exercice est déterminant en ce que la compréhension de ce corpus législatif dictera l'élaboration d'importants volets de la Convention. Mentionnons, en guise d'exemples, les clauses d'égalité de traitement des documents électroniques, quel que soit leur support, la détermination d'équivalences fonctionnelles concernant le document écrit, signé, original ou en forme spécifique, l'admissibilité et la force probante des messages de données, l'évaluation de la fiabilité des systèmes informatiques utilisés pour créer ou conserver les documents électroniques, l'application de règles de preuve particulières, le traitement du relevé imprimé, les présomptions de fiabilité et d'autres dispositions qui reflèteront certains consensus à l'échelle internationale. De même, l'étude de normes concernant les échanges dématérialisés sera à l'origine de clauses relatives à la tenue de registres, à la période de conservation des documents électroniques, au lieu d'archivage, à la modification des documents électroniques aux fins de leur conservation, à la destruction des documents, au recours à des tiers archivistes ou certificateurs ou encore, au choix des médiums et de la technologie de conservation. La bonne compréhension des exigences légales en vigueur dans certaines juridictions conduira les parties à l'adoption de clauses d'élection de domicile, de forum compétent et de droit applicable, d'arbitrage, de reconnaissance des règles d'ordre public ou encore, de dissociabilité des dispositions de la Convention jugées illégales. La pertinence de ces régimes normatifs nous semble donc acquise dès l'étape de l'élaboration du contenu obligationnel de la Convention, tant pour dresser l'inventaire des clauses susceptibles d'être négociées que pour en déterminer la teneur. Leur pertinence devient manifeste suivant une approche prospective en ce que ces régimes permettent d'identifier d'avance les voies privilégiées par les législatures et les marchés. Autrement dit, la compréhension de ces régimes donnent aux parties la possibilité de s'affranchir de règles de droit inadaptées et de rejoindre la technologie en tête de peloton, si ce n'est de la dépasser en traçant son évolution prévisible.

Il importe également de comprendre que, bien qu'elle n'ait d'effet qu'à l'égard des parties, la Convention doit stipuler des conditions de conservation permettant la reconnaissance des documents électroniques archivés à des fins statutaires ou à

---

[481] *Supra*, section 2.1

[482] *Supra*, section 2.2

l'encontre de tiers, d'où la pertinence d'une Convention en phase avec ces régimes normatifs étatiques. L'étude de ces régimes fait d'ailleurs comprendre que nous sommes loin de l'adoption à l'échelle internationale d'un régime juridique unifié relatif à la preuve et la conservation de documents électroniques, présumant même qu'il s'agisse là d'un idéal à atteindre, et que d'importantes zones de divergences perdurent en dépit des dénominateurs communs évoqués précédemment. Cette mouvance constitue en soi un facteur pertinent dans l'élaboration d'une Convention adaptable.

Fort de notre étude des caractéristiques du document, du commerce et de l'archivage électronique, de l'incertitude juridique qui en découle et des régimes normatifs évoqués précédemment, nous croyons maintenant utile d'aborder de façon concrète le contenu obligationnel de la Convention en livrant certaines réflexions pertinentes à la négociation et la mise en œuvre de cet outil conventionnel. À cette fin, nous avons jugé opportun de grouper, sous quatre rubriques distinctes, des clauses contractuelles au cœur de la Convention. Nous aborderons, dans l'ordre, des dispositions générales, des dispositions relatives à la conservation et à la preuve et enfin, des dispositions finales.

2.3.1 Des dispositions générales

Cette première partie de la Convention doit contenir des dispositions générales s'intéressant davantage à la Convention et à sa reconnaissance qu'à son contenu obligationnel spécifique. Ces dispositions auront pour objectif de définir l'objet, la portée et la durée de la Convention, d'affirmer son caractère licite, contraignant et prioritaire sur le droit étatique et de confirmer l'engagement mutuel des parties à satisfaire aux obligations qui y sont énoncées.

En définissant son objet et sa portée, les parties exerceront leur liberté contractuelle[483] pour se doter de règles d'ordre privé tributaires de certains facteurs incluant la spécificité de leurs rapports commerciaux, les catégories de documents attestant leur réalité d'affaires et leur vulnérabilité technologique. Les parties donneront ainsi plein effet à la finalité de la Convention[484].

---

[483] Conformément au principe de l'autonomie de la volonté et au consensualisme dans le cyberespace, *supra*, sections 1.2.2.1, 1.2.2.3.

[484] Conformément au principe de conformité aux fins poursuivies par la Convention et la finalité de la Convention, *supra*, sections 1.1.3 et 2.1.

En convenant d'une durée, les parties voudront s'assurer que la Convention est conçue pour demeurer en phase avec l'évolution prévisible du commerce électronique et des technologies[485]. Elles chercheront un outil de gestion de l'incertitude, pour une période déterminée[486].

Des clauses d'acceptation de la légalité et de la préséance de la Convention disposeront de tout doute quant à la volonté des parties d'être régies par des stipulations en matière de preuve et de conservation, à l'exclusion du droit étatique supplétif. Les clauses envisagées seront libellées pour garantir le respect de régimes d'ordre public et permettre de dissocier de la Convention toute disposition jugée illégale. Elles rappelleront le caractère obligatoire de la Convention en limitant ses effets aux parties, à l'exclusion de tiers. Les parties voudront fortifier leur accord d'une forte probabilité de reconnaissance judiciaire et convenir à cette fin de clauses d'élection de domicile, du droit applicable et du forum compétent ainsi que d'un pacte compromissoire[487]. L'exercice de cette autonomie dans le cadre du commerce électronique trouve d'importants appuis[488].

Comme tout autre contrat valablement formé, la Convention aura une cause. Celle-ci s'établira non pas dans l'existence d'une contrepartie monétaire, mais dans l'exécution réciproque des prestations. Ainsi, on trouvera sous le titre des dispositions générales l'engagement des parties de se doter d'une infrastructure technologique et de systèmes informatiques adaptés, de créer un environnement physique, opérationnel et humain procurant des garanties suffisantes de fiabilité et d'instaurer une régie interne propice aux fins de la Convention.

Ces engagements onéreux sont incontournables puisque la Convention force un véritable partenariat où la capacité d'une partie d'archiver utilement dépend du respect, par l'autre partie, de ses obligations. Cette dépendance est réelle et fait espérer plus d'actes volontaires que de menaces de recours en cas de défaut. Cela dit, il importera aux gestionnaires d'entreprises de fonder les investissements requis par la Convention sur de véritables obligations libellées en termes clairs et susceptibles d'être sanctionnées.

---

485 *Supra*, section 1.2.2.2.

486 *Supra*, section 1.2.2.3.

487 *Supra*, section 1.2.2.1.

488 Le C.c.Q., la *Loi type* sur le commerce électronique, le Projet de la CNUDCI de règles uniformes sur les signatures électroniques et d'autres initiatives législatives canadiennes et américaines ainsi que les contrats d'EDI reconnus à l'échelle internationale.

2.3.2 Des dispositions relatives à la conservation

Ces dispositions sont groupées sous trois rubriques, à savoir la création d'un environnement technologique fiable, l'élaboration de politiques d'archivage et le développement de mécanismes de mise en œuvre.

2.3.2.1 Un environnement technologique fiable

L'archivage électronique exige la mise en place, par chacune des parties, d'une infrastructure technologique fiable, adaptée à leur spécificité, tenant compte de l'évolution prévisible du droit et des technologies. Le choix de la technologie et des supports d'archivage est complexe et engage les parties sur une voie où l'erreur est coûteuse[489]. Des initiatives législatives en matière de commerce électronique défendent, à des degrés variables, le concept de neutralité technologique dans leur quête d'équivalents fonctionnels[490], en dépit de marchés qui présentent peu d'alternatives. D'autres États semblent commis à l'utilisation de solutions informatiques suivant certains algorithmes bien connus[491], notamment liés à la cryptographie asymétrique. Le juriste sera conscient que toutes les technologies ne peuvent satisfaire aux solutions juridiques proposées par certains ou retenues par d'autres[492], particulièrement à l'égard des concepts de signature électronique. Il retiendra donc le plus grand commun dénominateur, sachant que, pour l'heure, droit et technologie sont indissociables.

Nous avons indiqué que le document électronique doit être intelligible, fiable, accessible et reproductible[493], donc créé, conservé, reproduit ou transféré dans un environnement qui présente des garanties suffisantes de fiabilité. Outre les barrières de sécurité conçues pour prévenir la fraude ou le piratage, il importera d'établir la fiabilité inhérente de la technologie, des systèmes et du médium d'archivage choisis. Sachant que la proverbiale chaîne n'est jamais plus solide que le plus faible de ses maillons, les parties

---

489 Les informaticiens s'intéresseront aux spécifications techniques des équipements, leur capacité de stocker, la vitesse des échanges et leur compatibilité avec d'autres technologies. Les gestionnaires s'interrogeront sur leurs attributs opérationnels et leur coût. Pour le conseiller juridique d'entreprise, le défi est d'assurer l'existence, l'admissibilité et la force probante de documents électroniques au moment où ils seront offerts au tribunal, ou requis par une autorité, conformément aux exigences statutaires ou aux règles de preuve applicables.

490 Par exemple, la *Loi type* et le *Projet de Règles uniformes*, *supra*, sections 2.2.2.1 et 2.2.2.2.

491 Par exemple, le *Utah Digital Signature Act*, *supra*, section 2.2.2.7.

492 Tel celui de la signature dite sécurisée ou renforcée au cœur du *Projet de loi C-6*, précité, note 51.

493 *Loi type*, précitée, note 267, art. 10; *Projet de loi C-6*, précité, note 51, art. 37(b).

voudront maintenir ces mêmes garanties tout au long du cycle de vie du document électronique. Il leur faudra fixer la durée de conservation des documents, par catégories, et définir le périmètre de l'environnement technologique à protéger, en y incluant, le cas échéant, le tiers archiviste[494] ou d'autres intermédiaires, dont des fournisseurs d'accès à Internet[495]. La fiabilité de cet environnement n'a d'utilité que si la preuve peut en être faite par tout moyen de preuve reconnu, comprenant l'expertise, la vérification diligente et le tiers certificateur[496].

Concrètement, les parties devront procéder à l'inventaire et à la description technique de l'infrastructure technologique en place. L'acquisition et l'adaptation des systèmes et des supports d'archivage devraient être appuyées d'un rapport conjoint de l'équipe pluridisciplinaire formée à cette fin[497], sur la base des considérations commerciales, technologiques et juridiques jugées pertinentes. Le cycle de vie des documents, la possibilité de transferts ou de migrations des données ainsi que la durée de la Convention seront déterminants.

Ce rapport conjoint sera formellement ratifié dans la Convention pour servir de cahier de charges aux fins d'appels d'offres ou de devis pour travaux correctifs. Il sera à l'origine des représentations faites et des garanties données par les parties au plan technologique, particulièrement au plan de la fiabilité des systèmes de conservation. Il permettra de disposer plus aisément des différends pouvant résulter de défauts d'interopérabilité, de manquements contractuels ou de débordements budgétaires. Les contractants faisant face à des investissements différents reflétant la qualité ou la désuétude de leur infrastructure technologique, la partie confrontée à de plus importantes mises à niveau devra fonder sur ce rapport le bien-fondé de ses investissements.

---

494 *Infra*, section 2.3.2, paragraphe d).

495 L'échange continu de documents électroniques sur Internet, par le biais de fournisseurs d'accès, de routeurs ou d'autres intermédiaires constitue un véritable sas où l'information navigue sur des réseaux ouverts avec pour effet d'unir, en un seul, les environnements créés par chaque entreprise pour assurer la fiabilité des documents électroniques. Il suffit de rappeler les risques d'échanges de documents grevés de virus informatiques ou les risques d'intervention de tiers malveillants agissant sur Internet pour voir l'importance de protéger ces conduits électroniques. Cette interdépendance sert de fondement à la réciprocité des engagements évoquée précédemment.

496 *Infra*, section 2.3.2.3.

497 *Infra*, section 2.3.2.3. Une procédure analogue serait proposée pour l'obtention des garanties de sécurité d'ordre technologique.

L'inventaire, la description technique et le rapport conjoint devront être intégrés à la Convention, sous forme d'annexes, et être libellés en termes non équivoques pour dissiper toute ambiguïté quant aux obligations technologiques des parties.

2.3.2.2 Des politiques de conservation

Par delà les réalités technologiques, la Convention doit exiger l'élaboration et l'adhésion des parties à une politique d'archivage. Il suffit de vouloir cristalliser sur papier (ou sur support informatique!) une entente de principe, aussi simple soit-elle aux yeux des parties, pour qu'apparaissent la kyrielle des situations ignorées, la difficulté du choix des mots et l'enfer des détails. L'exercice est essentiel, tout comme le sont les buts recherchés. Cette politique sert en premier lieu à préciser le contenu obligationnel de la Convention de façon cohérente, pour l'ensemble des cas de figure prévisibles, à un niveau de détails utile pour les employés qui en auront la charge. Elle procure aux parties un outil référence captant la totalité des procédures administratives, des normes et des façons d'archiver qui auront droit de cité. Elle dispose à l'avance, autant que possible, des ambiguïtés et contradictions inévitables en cours d'exécution. Enfin, elle permet de bénéficier d'allégements offerts en matière de preuve pour prouver la fiabilité des systèmes d'archivage[498]. Rappelons que la preuve de l'existence et du respect d'une politique d'archivage constitue déjà, dans certaines juridictions, dont le Nouveau-Brunswick[499], une condition formelle d'admissibilité d'une reproduction électronique.

Il nous paraît utile de discuter davantage de certaines conditions qui risquent de former le cœur de toute politique d'archivage. Il s'agit de conditions relatives à la classification des documents et à la tenue de registres, à la période de conservation, au lieu d'archivage, au recours à des tiers archivistes, à la modification des documents électroniques aux fins de leur conservation et enfin, à la destruction volontaire de documents.

---

498 B. TROTTIER *loc. cit.*, note 56, p. 787, s'exprime ainsi à ce sujet, parlant de reproduction au sens des articles 2840 à 2842 C.c.Q. : « Or, la preuve de ces divers stades de conservation d'informations sera facilitée par la rédaction de politiques administratives rigoureuses, décrivant systématiquement les façons de faire du programme de numérisation et dont le dépôt devrait permettre au tribunal d'apprécier la rigueur de la gestion informationnelle de l'entreprise. »

499 *Loi sur la preuve* du Nouveau Brunswick, précitée, note 391, art. 47.1.

A) La classification des documents et la tenue de registres

La finalité de l'archivage d'un document est tributaire de sa valeur qui, pour l'entreprise, peut être d'ordre historique, légal, administratif, informatif ou technique[500]. L'entreprise veut conserver ce qui lui permet de prouver qu'elle existe et qu'elle commerce. Or, le passage d'objectifs légitimes à la gestion quotidienne de trillions d'octets nécessite un encadrement concret, donc la détermination de catégories et la confection de listes de documents électroniques à conserver. Ces outils de classification seront élaborés par les parties, conjointement, considérant les politiques d'archivage déjà en place en vue d'une transition harmonieuse. Des objectifs et un langage communs devront exister à ces fins de classification même si les parties ne veulent, ni ne doivent nécessairement archiver les mêmes documents électroniques[501].

L'expérience de la dernière décennie en matière d'EDI prouve que ce passage requiert également la tenue de registres de messages de données. La Convention stipulera l'obligation de créer, de mettre à jour et d'assurer la protection de registres des documents électroniques envoyés et reçus. Ces registres seront préparés dans le cours normal des affaires afin de bénéficier d'un traitement favorable en preuve[502]. Leur contenu devra satisfaire ou excéder des normes minimales[503], et comprendre les métadonnées permettant de déterminer l'origine et la destination du document électronique ainsi que les indications de date et d'heure de l'envoi ou de la réception[504]. Pouvant constituer des documents électroniques, leur conservation sera conforme à la politique d'archivage.

B) La période de conservation des documents électroniques

La période de conservation de certains documents est prescrite par la loi[505] et s'impose donc à l'entreprise, que ces documents soient sur support papier ou

---

500 *Supra*, section 1.1.3.

501 La mise en œuvre simultanée d'un programme de numérisation et de destruction d'archives sur support papier ajoutent à la complexité de la tâche.

502 Au Québec, voir l'art. 2870 C.c.Q.; *Loi sur la preuve* du Nouveau-Brunswick, précitée, note 391, art. 47.2.

503 Le lecteur pourra se référer en cette matière aux modèles de contrats d'EDI vus précédemment, notamment les règles de l'UNCID, art. 10.

504 Par exemple, *Loi type*, précitée, note 267, art. 10(c); *Projet de loi C-6*, précité, note 51, art. 37(c); *LUCE*, art. 9(c).

505 Voir les exigences statutaires décrites précédemment, *supra*, section 1.1.3.3.

électronique. Cette période varie en fonction de la nature ou de la finalité du document et va de quelques années à la vie entière de l'entreprise. Sauf exception, le respect de ces prescriptions exclut tout exercice discrétionnaire et l'entreprise n'a qu'à en prendre acte et à s'y conformer, en prenant soin de choisir, lorsque cela est permis, un support et une technologie compatibles avec la période de conservation prescrite.

La situation diffère en matière de conservation à des fins probatoires. La détermination de la période de conservation de chaque document ou catégorie de documents électroniques est empreinte de subjectivité. Des considérations juridiques, commerciales et de régie interne s'opposent à l'intérieur d'un processus d'évaluation de l'importance des faits et des actes juridiques prouvés par le document électronique et des risques associés à l'élimination de ce dernier. Qu'il s'agisse de la facture née de l'EDI prouvant l'achat de simples effets, du contrat de licence fondant toute l'action d'une entreprise ou de la transaction confidentielle mettant fin à un litige gênant, l'évaluation de la durée de conservation demeure une question de jugement. L'analyse en est une de coûts et de bénéfices, où les coûts d'archivage sont jugés en fonction de la valeur des informations.

Les parties ne trouveront aucune réponse magique dans les textes de référence vus précédemment[506], si ce n'est une plage allant du délai raisonnable[507] à un minimum de trois[508], de six[509] ou de dix ans[510] avec, sur les lignes de côté, des textes où l'on a préféré s'abstenir[511].

C) Le lieu d'archivage

Les lois sur les compagnies et la fiscalité demandent fréquemment que certains documents soient conservés dans des endroits spécifiques, entre autres pour qu'ils soient accessibles aux actionnaires et aux vérificateurs. Le libellé de telles dispositions dictera de la même façon le lieu d'archivage du document électronique, si l'entreprise décidait de se départir des versions sur support papier.

---

506 *Supra*, sections 1.1.3.3, 2.2.2, 2.2.3.

507 Par exemple, les *Digital Signature Guidelines de l'ABA*, art. 35, *supra*, section 2.2.3.3.

508 Par exemple UNCID, art. 10(c).

509 Par exemple, les lois sur le revenus et la fiscalité au Canada, *supra*, section 1.1.3.3c).

510 Par exemple, les *Digital Signature Administrative Rules*, *supra*, note 437.

511 *Loi type*, précitée, note 267, art. 10; *Projet de loi C-6*, précité, note 51; *LUCE*, note 347.

Le choix du lieu d'archivage obéit à d'autres impératifs. Le lieu envisagé doit permettre un accès en ligne rapide et sécuritaire, donc bénéficier d'interconnexions et de lignes de communication modernes, gérées par des fournisseurs d'accès sophistiqués et solvables. Ce lieu doit jouir de conditions atmosphériques propices à la préservation des supports. L'utilisation d'espace au siège social présentant des garanties de sécurité suffisantes peut s'avérer coûteuse et justifier la construction ou la location d'aires d'entreposage à loyer réduit loin des centres urbains. La Convention doit envisager le transfert ou la migration de données d'un lieu à l'autre, à des conditions prédéterminées. Enfin, la décision de confier la fonction d'archivage à une entité tierce comporte le choix d'un site sous la garde ou le contrôle de cette partie.

D) Le recours au tiers archiviste

Des considérations techniques et financières peuvent mener l'une ou les deux parties à recourir, dès la signature de la Convention ou en cours d'exécution, aux services de tiers archivistes. E. Caprioli définit ainsi ce tiers de confiance :

> « *Le tiers archiveur peut se définir comme une entité chargée par les utilisateurs (entreprises ou personnes physiques) ou leurs mandataires (centre de gestion agréé, expert-comptable) de recevoir, de conserver et d'assurer la gestion des enregistrements électroniques. Ainsi, il réceptionne des informations sous forme de données numériques, qu'il sera chargé de conserver, de gérer à la demande et sur l'ordre de ses clients, voire même de les présenter aux autorités administratives ou devant les tribunaux.* »[512]

Caprioli en justifie l'intervention en ces termes :

> « *L'intervention d'une tierce partie contribuera à apporter la confiance quant à la paternité et la véracité des enregistrements informatiques conservés, certes au premier chef pour le compte d'un client contre rémunération, mais aussi au service de l'intérêt général.* »[513]

L'impartition, la sous-traitance ou d'autres modes de délégation sont aujourd'hui privilégiés en raison des économies qu'ils entraînent, particulièrement pour l'exécution de tâches requérant d'importantes immobilisations, un haut niveau de spécialisation et une formation continue. Le recours au tiers archiviste est connu au plan

---

512 É. A. CAPRIOLI, *loc. cit.*, note 153, p. 53.

513 *Id.*, p. 49.

législatif[514] et la Convention devrait l'autoriser, sous certaines conditions. On exigera que l'archiviste s'engage à fournir un environnement technologique équivalent ou supérieur, offrant les mêmes garanties de fiabilité que celles exigées des parties[515]. L'archiviste sera qualifié d'agent[516] et la partie demeurera responsable, solidairement, de l'exécution conforme de la Convention[517]. Des vérifications diligentes seront prévues. Des présomptions de faute ou de responsabilité seront stipulées[518]. Des clauses d'indemnisation appropriées seront négociées. Le choix de l'archiviste sera discrétionnaire, avec droit de refus pour des motifs raisonnables, suivant les circonstances.

E) La modification des documents électroniques aux fins de leur conservation

Les informaticiens soucieux d'optimiser l'espace mémoire si précieux élaborent des méthodes de conservation convertissant de multiples façons l'expression machine du message de données. Il s'agit d'une réalité informatique, à l'origine du désormais célèbre bogue de l'an 2000, qui demeure indissociable de l'architecture des logiciels et de la recherche d'avantages concurrentiels appréciés des usagers. Ce gain d'espace, aussi rentable soit-il, n'a d'intérêt que si la fiabilité du document électronique est préservée.

Les parties devront s'intéresser de près aux règles de droit sur le sujet même si elles sont ambiguës, voire contradictoires. Au Québec, rien dans les articles 2837 à 2842 C.c.Q. n'interdit spécifiquement que l'inscription informatisée soit modifiée au plan de l'expression en langage machine durant l'archivage, pour autant que l'opération soit parfaitement réversible. Les critères d'intelligibilité et de fiabilité énoncés à l'article 2837 C.c.Q. ne s'y opposent pas, le tribunal pouvant y voir une « circonstance »[519] dont il peut

---

514 *Loi type*, précitée, note 267, art. 10(3); le *Projet de loi C-6* est silencieux à ce sujet mais n'exclut d'aucune façon le recours au tiers archiviste. Voir également le *Electric Information and Documentation Act* de la Saskatchewan, *supra*, section 2.2.2.5 et plusieurs modèles de contrats d'EDI, *supra*, section 2.2.3.1.

515 Consulter, relativement aux obligations et responsabilités de l'archiviste, É. A. CAPRIOLI, *loc. cit.*, note 153, p. 57.

516 Par exemple, NZEDIA, art. 8.1.

517 Par exemple, EIDA, art. 8.2.

518 *Id.*, art. 8.1.

519 Art. 2837 C.c.Q.

tenir compte à l'étape de l'étude des garanties de fiabilité requises[520]. Cette approche est renforcée par l'article 10 de la *Loi type* qui précise bien que le message de données doit, en principe, être conservé sous la forme dans laquelle il a été créé, envoyé ou reçu, *« ou sous une forme dont il peut être démontré qu'elle représente avec précision les informations créées, envoyées ou reçues »*. Ainsi, *« il ne serait pas approprié d'exiger que l'information soit conservée sans modification puisqu'en général, les messages sont décodés, comprimés ou convertis pour pouvoir être conservés »*[521]. Elle est également appuyée par le *Electric Information and Document Act* de la Saskatchewan qui exige que le document électronique soit exempt d'altérations, à l'exception de modifications survenant dans le cadre normal de la communication, de l'archivage ou de sa présentation, tenant compte de la finalité du document et des autres circonstances[522].

À l'inverse, cette approche contrevient aux règles de l'UNCID qui indiquent à l'article 10(c) que *« le journal des données commerciales ... doit être conservé sans modification... »*[523] Elle se heurte, en partie[524], à l'article 37(a) du *Projet de loi C-6* exigeant la conservation du document électronique *« sous la forme dans laquelle il a été fait, envoyé ou reçu ou sous une forme qui ne modifie en rien l'information qu'il contient »* ou encore, à l'article 47.2 de la *Loi sur la preuve* du Nouveau-Brunswick qui interdit *« toute altération du document électronique »*[525]. Plusieurs clauses de conservation dans les contrats d'EDI tolèrent mal ces modifications[526].

De toute évidence, l'entreprise se doit d'être prudente. Elle doit s'interroger sur la nature des modifications effectuées, l'impact que celles-ci auront sur les données relatives au contexte, à la structure et au contenu du document électronique et ultimement, si ces modifications portent préjudice à la capacité de l'entreprise de

---

520 Il suffit de rappeler la façon dont l'information circule sur les inforoutes par l'action de protocoles de communication hachant le message original en milliers d'infimes *packets* auxquels se greffent des éléments d'informations, pour comprendre que la notion de fiabilité doit composer avec un certain niveau de modifications. L'envoi de messages chiffrés et signés au moyen d'algorithmes cryptographiques constitue un autre exemple de modifications du document ou de la signature qu'il porte.

521 *Guide*, *op. cit.*, note 267, par. 73.

522 *Supra*, notes 410 et 411.

523 UNCID, art. 10(c).

524 En effet, on peut imaginer la modification du document mais non de son contenu, excluant du coup les méthodes de compression par suppression de données.

525 *Loi sur la preuve* du Nouveau Brunswick, précitée, note 391, art. 47.2.

526 Par exemple, NZEDIA, art. 7.1.

reprendre la piste de vérification et d'établir la fiabilité du document électronique. À l'heure actuelle, on ne peut dégager de consensus définitif sur la question et il paraît téméraire d'engager les parties sur une voie autorisant sans réserve des modifications dites temporaires ou réversibles du document électronique aux fins de le conserver. Une approche modulée pour refléter la valeur des documents conservés est envisageable, rappelant que la preuve du maintien de la fiabilité des informations contenues dans le document restera le critère minimal fondamental.

F) La destruction volontaire de documents

Dans les cas qui ne sont pas prohibés par la loi, l'élimination d'un document s'analyse suivant deux cas de figure distincts au plan des difficultés qu'ils posent.

Un premier scénario vise la destruction d'un document électronique au terme de son cycle de vie, tenant compte des prescriptions statutaires et de la valeur intrinsèque des informations qu'il contient. Ce scénario se résout en fonction de l'existence et du maintien ou non d'une version d'origine sur support papier. En présence de l'original papier, ce scénario pose peu de difficultés en ce sens qu'il replace l'entreprise dans la position qui aurait été la sienne n'eut été de la mise en place d'un programme de numérisation et de stockage de données. La perte est monétaire. À l'inverse, en l'absence d'un original papier, la destruction volontaire du document électronique laisse l'entreprise sans mémoire ni moyen de preuve, un risque qu'elle aura sans doute évalué à l'étape de la détermination du cycle de vie du document. La même logique s'applique lorsque le document électronique est créé simultanément à l'acte juridique ou aux faits qu'il atteste, en l'absence de tout support papier.

Un second scénario, plus délicat, vise la destruction de l'original papier reproduit sous forme électronique avant l'expiration du cycle de vie du document électronique. Les parties devront également être prudentes à ce sujet, notamment au moment de choisir le droit étatique applicable ou de convenir, comme nous le verrons[527], de règles de preuve conventionnelles autorisant la destruction d'originaux. Au Québec, par exemple, des auteurs arguent que le document électronique créé postérieurement à l'acte juridique afin de stocker les données qui en font foi ne peut être substitué à l'original, qui demeure la meilleure preuve. Si ce n'était des articles 2840 à

---

527 *Infra*, section 2.3.3.3.

2842 C.c.Q.[528], la destruction volontaire de l'original ne pourrait servir à contourner l'obstacle posé par le premier alinéa de l'article 2860 C.c.Q., la partie perdant la bonne foi exigée par le second alinéa de cet article. Il en résulte que la destruction consciente de l'original papier **hors** du cadre de l'article 2840 C.c.Q. entraîne simultanément la perte du bénéfice de l'exception à la règle de la meilleure preuve et le droit d'utiliser une reproduction ayant valeur d'original[529]. Ce résultat se comprend si l'on adhère fortement à la règle de la meilleure preuve, au point de préférer la destruction contrôlée de l'original plutôt que de bousculer la hiérarchie consacrée des moyens de preuve. Certes, l'existence d'une obligation statutaire de détruire l'original, suivant la *Loi sur la preuve* du Nouveau-Brunswick, a le mérite de résoudre la difficulté lors d'une reproduction électronique d'un original papier[530].

On comprendra la réticence des parties à investir d'importantes ressources dans un programme intégré d'archivage électronique pour ensuite conserver des « tonnes » de papier pour plaire aux juristes. La prudence dont les parties doivent faire preuve pourrait justifier une interdiction de détruire limitée à certaines catégories d'originaux sur support papier, sujet à une réévaluation de la situation suivant l'évolution des pratiques et du droit. Cette prudence mène aussi à l'imposition de conditions minimales de reproduction/destruction de documents de moindre valeur qui rejoignent ou excèdent les conditions proposées par les législations actuelles. Par exemple, la Convention devrait prévoir la présence d'une personne spécialement autorisée aux fins de la reproduction qui devra, dans un délai raisonnable, suivant la reproduction, en attester la réalisation par une déclaration assermentée mentionnant la nature du document reproduit ainsi que le lieu et la date de reproduction et en certifier l'intégrité. La tenue de registres d'affidavits de destruction serait souhaitable. Le recours aux vérifications diligentes, aux tiers spécialisés ou à la certification pourra être envisagé.

---

528 La mise en œuvre d'un programme de reproduction répondant aux critères énoncés aux articles 2840 à 2842 C.c.Q. permettrait de conférer à la reproduction la valeur de l'original, pour autant que l'original soit détruit dans le processus de reproduction.

529 Ce résultat rappelle l'importance, pour l'entreprise assujettie au droit québécois, d'adopter un programme de reproduction conforme aux articles 2840 à 2842 C.c.Q. et d'y adhérer notamment en matière de preuve préconstituée relative au processus de reproduction.

530 *Loi sur la preuve* du Nouveau Brunswick, précitée, note 391, art. 47.1.

2.3.2.3 Des mécanismes de mise en œuvre

Les parties doivent prévoir des mécanismes assurant la mise en œuvre de la Convention. En premier lieu intervient la création d'une équipe conjointe responsable de la Convention auprès de la direction des parties. En effet, l'archivage électronique soulève des questions d'ordre commercial, technologique et juridique qui ne peuvent être traitées isolément, en l'absence d'une expertise réelle dans ces domaines. L'importance des risques justifie le déploiement de ressources adéquates. Les parties voudront donc se doter d'une équipe pluridisciplinaire formée de leurs représentants et, ponctuellement, de consultants externes. Son implication sera continue et devra se manifester, entre autres, par l'exercice d'un contrôle intellectuel commençant dès l'élaboration des politiques d'archivage. Des clauses seront négociées pour régir la création de cette équipe, sa composition, son rôle, ses fonctions et responsabilités. L'équipe devra faciliter la formation d'archivistes compétents pour procéder à des reproductions de documents électroniques ou des transferts de données de façon fiable et livrer un témoignage crédible à cet égard[531].

Deuxièmement, les parties pourront stipuler une vérification périodique de l'exécution conforme de la Convention. Ces audits auront pour double objectif de donner plein effet aux engagements de réciprocité[532] et servir de moyen de preuve dans le cadre de contestations relatives aux documents électroniques archivés. L'audit témoignera du maintien des garanties de fiabilité tout au long du cycle de vie du document, nonobstant des transferts de données ou des migrations de supports. Il attestera la correction de lacunes qui auraient pu être décelées. S'agissant d'une preuve préconstituée, les parties s'assureront de la conservation utile de ces rapports de vérification et, selon les circonstances, impliqueront le conseiller juridique concernant des aspects confidentiels ou privilégiés du produit de ces vérifications.

Enfin, les parties pourront envisager l'intervention d'un tiers certificateur mandaté pour déterminer si le contenu obligationnel et les spécifications techniques de la Convention rencontrent ou excèdent les normes établies ou prévalant en matière de conservation électronique. Alors que la vérification diligente s'intéresse à l'exécution conforme, la certification interviendra en amont, à l'étape de l'élaboration de la

---

531 Au Québec, art. 2840 C.c.Q.; au Canada, *Projet de loi C-6*, précité, note 51, art. 31.1; au Nouveau Brunswick, *Loi sur la preuve* du Nouveau Brunswick, précitée, note 391, art. 47.1(4).

532 *Supra,* section 2.3.1.

Convention, puis en aval, en cours d'exécution, considérant l'évolution continue des technologies et des usages. Le certificateur permettra une mise à niveau de la Convention conclue à long terme et fournira une preuve à cet égard. La certification existe dans le cyberespace[533] et pourrait, en soi, devenir une norme. Nos commentaires concernant la préservation des rapports de certification et de l'intervention de conseillers juridiques demeurent pertinents.

2.3.3 Des dispositions relatives à la preuve

La recherche d'équivalents fonctionnels en matière d'écrit, de signature, d'original et de conditions de forme devra guider les parties[534], tant dans le cadre de leur relation d'affaires que pour faciliter l'utilisation de documents électroniques à l'encontre de tiers.

2.3.3.1 Le document électronique

Concernant le document électronique[535], les parties voudront affirmer son statut juridique et renoncer à contester sa validité, son admissibilité ou ses effets juridiques au seul motif que l'information qu'il contient est sous forme électronique. Sa force probante sera laissée à l'appréciation du juge, tenant compte de l'ensemble des circonstances, particulièrement de la fiabilité de l'environnement technologique où il a été créé, conservé ou reproduit.

Les parties reconnaîtront la valeur juridique du document électronique fiable, intelligible, accessible et reproductible pour consultation tout au long de son cycle de vie, dans le cadre de toute procédure de résolution de différends, sujet ou non, suivant les circonstances, aux règles générales de droit supplétif relatives à la preuve, à l'exception des règles discriminantes régissant, notamment, l'authentification, le ouï-dire et la meilleure preuve[536]. Les notions d'intelligibilité, de fiabilité et d'accessibilité seront

---

533 P. TRUDEL, F. ABRAN, K. BENYEKHLET, S. HEIN, *op. cit.*, note 67, pp. 3-46 et ss.

534 *Supra*, section 2.2.

535 Les documents électroniques auront préalablement été définis par les parties, par catégories, pour cadrer avec leur réalité d'affaires.

536 Nous visons ici l'exclusion des règles de preuve faisant obstacle aux principes de non discrimination et d'égalité de traitement des documents, quel que soit leur support, qui sont bien établis dans la vaste majorité des lois évoquées précédemment, sans pour autant exclure l'application de toutes les règles générales de preuve.

définies par les parties suivant des critères objectifs susceptibles d'être établis en cas de contestation. La référence à des normes reconnues sera envisagée[537].

Les parties pourront affirmer que le document électronique constitue un écrit aux fins de la preuve d'actes juridiques ou de faits matériels et renoncer aux bénéfices d'exiger un écrit sur un support particulier. Le document électronique sous forme de sortie imprimée constituera un écrit et tiendra lieu d'original si cette sortie présente des garanties de fiabilité suffisantes et que cette sortie imprimée a été utilisée dans le cours normal des affaires, suivant une pratique établie, aux fins de relater l'information enregistrée ou mise en mémoire[538]. Les documents électroniques ou « business records » établis dans le cours normal des activités de l'entreprise et ceux insérés dans un registre dont la tenue est exigée par la loi, incluant des banques de données, seront identifiés clairement pour bénéficier d'allègements en matière de preuve.

2.3.3.2 La signature électronique

Les parties pourront convenir que leur signature électronique, telle que définie, lorsque associée au document électronique, aura l'effet juridique de la signature manuscrite des parties et les liera de la même façon. Elles voudront ignorer toute neutralité technologique et opter pour une technologie fiable, éprouvée en matière d'authentification et de non-répudiation. Le recours à des normes établies est hautement préférable, sachant qu'il s'agit là d'un moyen d'appuyer l'admissibilité du document. La technologie choisie devra garantir un niveau de fiabilité suffisant, eu égard aux catégories de documents retenues, pour assurer l'identification de l'expéditeur et prouver son accord avec le contenu du document électronique. La Convention devrait être un modèle de souplesse pour reconnaître des niveaux de fiabilité en fonction de la finalité du document électronique, ouvrant du coup le recours, au besoin, à des signatures électroniques à niveau de sécurité variable. On pourra stipuler un niveau de sécurité accrue à l'étape de

---

537 Par exemple, le *Projet de loi C-6*, précité, note 51, art. 31.5, reconnaît aux parties la possibilité de présenter un élément de preuve relatif à toute norme au soutien de l'admissibilité d'un document électronique. De même, le *Guide, op. cit.*, note 267, fournit un inventaire de critères pertinents à l'établissement de la fiabilité, voir *supra*, note 288.

538 L'art. 47.1 de la *Loi sur la preuve* du Nouveau-Brunswick, précitée, note 391, précise qu'une sortie sur imprimante est admissible en preuve dans tous les cas et pour toutes les fins pour lesquelles le document original eut été admissible à condition : (1) que le document original a été copié par un procédé de prise d'images électroniques ou un procédé semblable et a été enregistré ou conservé électroniquement dans le cours d'une pratique établie afin de garder une preuve permanente du document, (2) que le document original a été détruit après avoir été copié et enregistré ou conservé conformément à l'art. 1 et (3), que la sortie sur imprimante est une copie certifiée conforme du document original.

l'identification en exigeant que certains ou la totalité des échanges soient assortis d'un certificat d'identité émanant d'une autorité de certification accréditée liant les parties à leur signature électronique[539].

2.3.3.3 L'original électronique

Les parties pourront convenir que toute reproduction sous forme électronique d'un document créé à l'origine sur support papier, et que tout document électronique résultant d'un transfert d'informations, quels que soient la technologie et le support utilisés, seront considérés de la même manière que le document d'origine et tiendront lieu d'originaux, pour autant qu'il existe une garantie de fiabilité suffisante de l'intégrité de l'information tout au long du cycle de vie du document, incluant le cycle de reproduction et de transfert, et que les conditions contractuelles prévues à cette fin, s'il en est, soient respectées.

Les parties jugeront opportun de prévoir que des modifications dans le cours normal de la reproduction, du transfert, de la communication ou de la conservation du document électronique, n'affectant en rien la fiabilité de l'information qu'il contient, n'auront pas pour effet de lui faire perdre sa qualité d'original. La Convention reconnaîtra l'usage des banques de données aux fins de la conservation d'un document électronique, ou du transfert des données qu'il contient, en spécifiant que la fiabilité du document électronique n'est pas viciée du seul fait que les données qu'il contient sont fragmentées, pour autant que ce processus de fragmentation (et de recomposition) garantisse l'intégrité de l'information et préserve les éléments de délimitation et de structure du document.

La destruction d'originaux sur support papier sera considérée avec prudence[540]. Les parties pourront dire, le cas échéant, que la mise en œuvre d'un processus destructif conformément à une procédure établie rencontrant des normes minimales reconnues[541] ne pourra constituer un motif de contestation du statut ou de la valeur juridique de la reproduction électronique. Elles pourront également recourir à la signature électronique dite sécurisée, ou à son équivalent, lorsque ce concept sera

---

539 Mentionnons, à titre illustratif, que la Directive européenne milite clairement en ce sens, *supra*, section 2.2.2.8.

540 En tout état de cause, la destruction de documents pouvant constituer une preuve pertinente dans le cadre d'un litige existant ou prévisible devra se faire en consultation avec les conseillers juridiques de l'entreprise, eu égard aux conséquences pouvant découler de la destruction volontaire d'une preuve.

541 *Supra*, section 2.2.1.3.

davantage défini[542] à l'égard des documents électroniques qui doivent porter un sceau, des affidavits ou des déclarations solennelles.

Concernant le maintien du format des échanges, les parties, confortées de normes internationales et de l'expérience en matière d'EDI, pourront convenir de conditions de forme préétablies stipulant que des modifications transitoires intervenues dans le cadre de la communication du document n'auront pas pour effet de lui faire perdre sa qualité d'original, pour autant que la fiabilité de l'information soit préservée suivant les critères évoqués plus haut en matière de modifications.

2.3.3.4 L'expédition, la réception et l'attribution du document électronique

Pour l'attribution des documents échangés, les parties pourront s'entendre pour dire que le document électronique sera réputé émaner de l'expéditeur s'il a été envoyé par l'expéditeur lui-même, par une personne autorisée à agir à cet effet en son nom ou par un système d'informations programmé par l'expéditeur pour fonctionner automatiquement[543]. S'agissant d'une présomption, la Convention pourra permettre de la repousser dans les cas où, notamment, l'expéditeur répudie le document électronique où une procédure d'attribution acceptée d'avance fait douter de l'origine du document.

La preuve du moment et du lieu d'expédition et de réception du document électronique est pertinente aux fins de la formation des contrats en ligne et de la computation de délais contractuels. Les parties pourront s'inspirer de théories de l'expédition ou de la réception qui ont vu le jour des décennies avant le commerce électronique, dans le cadre de contrats formés à distance. Au Québec, par exemple, on retient la théorie de la réception pour l'échange des consentements, statuant que le contrat est formé au moment et au lieu où l'acceptation est reçue, quel qu'ait été le moyen pour la communiquer[544]. Or, dans le cyberespace, les notions d'expédition et de réception sont à définir en ce que l'acte constitutif de l'expédition ou de la réception d'un message de données renvoie à des réalités technologiques complexes impliquant parfois des tiers, d'où l'intérêt d'y pourvoir conventionnellement. En guise d'exemple, les parties pourront juger que l'expédition intervient lorsque le document électronique entre dans un système d'informations indépendant, hors du contrôle de l'expéditeur[545]. De même, la

---

542 *Projet de loi C-6*, précité, note 51, art. 48(2).

543 Par exemple, UETA, art. 9; *Loi type*, précitée, note 267, art. 13.

544 Art. 1387 C.c.Q.

545 Par exemple, *Loi type*, précitée, note 267, art. 15.1; UETA, art. 15.1.

réception pourra intervenir lorsque le document entre dans un système d'informations désigné par la partie pour la réception ou lorsqu'il est relevé par le destinataire[546]. Alternativement, le message de données sera réputé expédié et reçu au lieu où l'expéditeur ou le destinataire a un établissement, son lieu de résidence ou encore un lieu ayant une relation étroite avec l'activité commerciale concernée, tel l'emplacement d'un système d'informations désigné[547]. On s'assurera que tout document électronique transmis soit daté et horodaté automatiquement à l'aide d'un système d'informations conçu à cette fin[548].

Dans les cas qui le requièrent, la preuve de l'accusé de réception dans un délai convenu sera établie par la Convention. La réception pourra être accusée par toute communication automatisée émanant du destinataire ou tout autre acte jugé suffisant pour indiquer à l'expéditeur que le document électronique a été reçu[549]. Le document électronique sera reçu par le destinataire lorsque l'expéditeur reçoit ou le destinataire émet l'accusé de réception. Cet accusé pourra faire preuve de la réception, sous réserve d'une preuve contraire, mais ne pourra prouver la fiabilité du document électronique à la réception, ni avoir d'effets juridiques au-delà de ce qui est prévu à la Convention[550].

2.3.4 Des dispositions finales

La Convention, comme la quasi-totalité des ententes commerciales, devra contenir certaines dispositions dites finales pour disposer de questions liées, pour la plupart, à la définition, l'application, l'interprétation ou la terminaison de la Convention. On y trouvera des clauses relatives à l'intégralité de l'entente, à la protection de renseignements personnels ou confidentiels, à la propriété intellectuelle, à la cession de droits ou encore, des clauses traitant de force majeure, de défaut, de résiliation, de responsabilité ou d'indemnisation. À cela s'ajoutera un régime relatif à la résolution des différends, comprenant le choix du droit applicable et d'un forum compétent. De telles dispositions ne sont pas spécifiques à la Convention et présentent peu de difficultés pour l'avocat d'expérience. Nous n'entendons donc pas les aborder, si ce n'est pour formuler

---

546 Par exemple, *Loi type*, précitée, note 267, art. 15.2.

547 *Id.*, art. 15.4.

548 Par exemple, CIREDIT, art. 3.

549 Par exemple, *Loi type*, précitée, note 267, art. 14.

550 Par exemple, EIDA, art. 6, UNCID, art. 6 et 7, ABA, art. 2.2, CIREDIT, art. 4, NZEDIA, art. 4, EDICA, art. 4.

des commentaires relatifs aux clauses de droit applicable et d'arbitrage qui revêtent, pour les raisons explicitées ailleurs[551], une importance particulière aux fins de la Convention.

Dans son Guide de rédaction des clauses d'arbitrage et de droit applicable dans les contrats commerciaux internationaux[552], Bienvenu aborde les principes généraux et les facteurs pertinents dans le choix du droit applicable, précisant que « soumettre un contrat à un droit dont on ignore le contenu est une attitude suicidaire »[553]. L'auteur ajoute ce qui suit :

> « *Le plus important facteur dans le choix du système juridique qui régira un contrat devrait être le degré de familiarisation des parties avec un système juridique particulier, soit parce qu'il s'agit de leur propre système, soit parce qu'il s'est développé et imposé dans le domaine particulier qui fait l'objet du contrat, par exemple le droit anglais en matière d'amirauté.* »[554]

Il précise qu'un contrat commercial international[555] est régi par la loi choisie explicitement ou implicitement par les parties, sous réserve de certaines restrictions à l'autonomie de la volonté ou, à défaut, par le système juridique désigné par un tribunal compétent suivant un critère objectif généralement fondé sur l'existence d'un lien étroit, réel ou significatif avec le contrat[556].

Les parties à la Convention voudront suivre ce conseil et veiller à ce que la loi applicable fasse place à l'autonomie de la volonté et à la réalité du commerce électronique. Il y va de la légalité de la Convention en matière de preuve[557] et de la reconnaissance du document électronique[558]. Le droit québécois est bien positionné à cet égard[559]. Les parties voudront également « stipuler leur intention de n'accorder au droit

---

551 *Supra*, section 1.2.2.1.

552 P. BIENVENU, « Guide de rédaction des clauses d'arbitrage et de droit applicable dans les contrats commerciaux internationaux », (1996) 56 *R. du B.* 39.

553 *Id.*, p. 77.

554 *Ibid.*

555 *Id.*, p. 41. Pour Pierre Bienvenu, « un contrat commercial est international lorsqu'il comporte un ou plusieurs éléments pertinents juridiquement qui le relient à plus d'un État. ». Suivant ce critère, la Convention constituera un contrat commercial international dans la vaste majorité des cas.

556 *Id.*, pp. 74-75.

557 La légalité de la Convention s'établit en regard du droit substantif applicable.

558 *Supra*, section 2.2.2.

559 *Supra*, section 1.2.2.1.

applicable qu'une vocation purement supplétive aux dispositions du contrat »[560] et voudront exclure toute possibilité de renvoi par l'exclusion des règles de conflits de lois contenues dans la loi applicable. La clause devra également désigner le droit applicable « à la Convention » et non pas uniquement « aux différends » qui pourraient en découler. Enfin, il est possible dans un bon nombre de juridictions, incluant le Québec, de n'assujettir qu'une partie seulement de la Convention à une loi donnée, par le mécanisme du « dépeçage »[561], afin de bénéficier d'un régime particulièrement bien adapté aux parties contractantes, en matière de preuve électronique par exemple.

Par ailleurs, le recours à la clause compromissoire parfaite comporte des avantages et des désavantages[562]. Ces avantages deviennent déterminants pour les parties à la Convention. Premièrement, l'arbitrage institutionnel ou *ad hoc* procure un forum confidentiel de résolution des différends. Il permet aux parties de former un tribunal neutre, spécialisé dans le domaine pertinent (le commerce électronique par exemple) et compétent pour disposer définitivement d'un différend suivant un calendrier convenu. Deuxièmement, l'arbitrage permet d'exclure le recours à de multiples tribunaux dits compétents ou au *« forum shopping »*[563] dans le cadre d'entente internationale, et ainsi gérer l'incertitude du droit dans le cyberespace et contourner les difficultés découlant de l'application de règles de droit international privé. Pour l'entreprise virtuelle, la capacité d'éviter le cirque judiciaire propre à certaines juridictions peut constituer un facteur déterminant. Enfin, l'arbitrage permet aux parties de convenir avec certitude de règles de preuve adaptées aux documents électroniques qu'elles utilisent dans le cadre de leurs échanges. Tous ces avantages militent pour l'inclusion d'une clause d'arbitrage.

La rédaction d'une telle clause devra se faire avec soin, en raison notamment des choix qui s'offrent aux parties. Au titre des éléments à considérer[564] se trouvent la portée de la clause d'arbitrage, la composition du tribunal, le lieu et la langue d'arbitrage, la qualification professionnelle des arbitres, les règles de procédure et de preuve

---

560 *Id.*, p. 78.

561 *Id.*, p. 74.

562 Au titre des désavantages, le plaideur d'expérience reconnaîtra que l'arbitrage peut être long, onéreux et mal adapté aux situations multipartites ou requérant un encadrement procédural formel ou encore exigeant des moyens extraordinaires d'administration de la preuve.

563 L'aggravation des risques liés au *forum shopping* est une réalité dans le cyberespace en raison de la multiplicité des facteurs de rattachement. Il s'agit d'un risque propre au commerce électronique, *supra*, section 1.1.1.

564 P. BIENVENU, *loc. cit.*, note 552, p. 64.

applicables, la finalité de la sentence, son homologation et son caractère obligatoire ainsi que les frais de l'arbitrage. Le recours à des clauses types d'institutions d'arbitrage est possible[565], pour autant qu'elles soient bien adaptées aux circonstances.

565 Parmi les institutions fréquemment nommées, mentionnons l'*American Arbitration Association* (AAA), la Chambre de commerce internationale (CCI), la *London Court of International Arbitration* (LCIA) et, plus près de nous, le Centre d'arbitrage commercial national et international du Québec.

CONCLUSION

Internet est né hier et dominera demain, non pas en raison du déploiement de brillantes stratégies promotionnelles mais simplement à cause de ses gènes. Internet est apparu naturellement et sa dominance toute darwinienne ne témoigne que des forces évolutives en présence. Parce que décentralisé, dématérialisé, transnational et ouvert, cet organe de communication et de commerce répond à un nouvel environnement en quête d'efficacité économique et de souplesse à l'échelle planétaire.

Or, la créature s'est imposée rapidement et porte en elle des risques, d'abord ignorés, puis jugés suffisamment sérieux pour alerter les usagers, soutenir d'importants marchés de produits de sécurité et justifier l'intervention des États. Ce ralliement et son objectif premier étaient légitimes : favoriser le commerce électronique et protéger le public par la sécurisation des échanges. Malheureusement, le succès se fait attendre alors que l'incertitude demeure la réalité du conseiller d'entreprise confronté à d'importantes difficultés juridiques.

En effet, le commerce électronique intervient par l'échange de données numériques inintelligibles, dénuées de tout substrat matériel et de structure permanente, dont l'utilisation et la conservation posent des risques. Les enjeux sont bien réels si l'on considère que ces documents dématérialisés doivent servir à l'entreprise pour prouver qu'elle existe, qu'elle commerce et qu'elle se conforme à ses obligations statutaires. Ces risques sont aggravés par l'inévitable désordre que cause le déplacement des échanges vers un monde virtuel, en continuelle transformation. Ces risques demeurent en partie indifférenciés à ce jour car la croissance d'Internet précède des réformes inévitables en matière de technologie, de commerce et de droit.

Pour l'entrepreneur, le risque est un fait quotidien dans l'établissement d'une stratégie d'affaires. Il doit cependant être géré. En réponse à l'incertitude du cyberespace, la Convention apparaît comme un outil efficace de gestion de risques juridiques liés à l'utilisation de documents électroniques. Elle constitue un moyen licite, en phase avec la réalité du commerce électronique et susceptible d'être adaptée aux besoins et aux ressources des parties contractantes. Sans être l'outil idéal que serait pour certains l'adoption à l'échelle internationale d'un régime juridique unifié et flexible relatif à la preuve et à l'archivage électronique, la Convention constitue, pour un temps, une loi négociée qui s'accepte, fonctionne et s'impose en cas de différends, pour autant que l'entreprise qui l'invoque ait bien conservé sa copie!

BIBLIOGRAPHIE

Table de jurisprudence citée

1267623 Ontario Inc. v. *Nexx Online Inc.*, [1999] O.J., n° 2246, Ontario Superior Court of Justice, 14 juin 1999;

Belland c. *R.*, (1982) 65 C.C.C. (2d) 377 (CA);

Blain c. *Tawfik*, J.E. 96-379 (C.A.), C.A. Montréal, 500-09-000165-902;

Bleau c. *Bélair, compagnie d'assurance*, C.S.Q. 505-05-000614-948, 1999-05-04;

Braintech, Inc. c. *John C. Kostiuck* [1999] B.C.J. n° 622;

British Telecommunications plc v. *One In A Million Limited*, 148 NLJ 1179;

Caisse Populaire Desjardins de St-Jacques c. *Longpré*, J.E. 92-1199 (C.Q.), C.Q. Joliette 705-02-002376-911;

CF Heros Inc. v. *Heroes Found*, 958 F Supp. 1 (D.D.C. 1996);

Condominiums Mont St-Sauveur c. *Les Constructions Serge Sauvé*, [1990] R.J.Q. 2783;

Cybersell Inc. v. *Cybersell Inc.*, 130 F. 3d 414, 419 (9th Cir. 1997);

Drouin c. Landry, [1976] C.A. 763;

DuMay (1985) Inc. c. *U.A.P.*, .C.Q. Longueuil 505-02-004177-964, 1997-02-28;

Garcia Transport Ltée c. *Cie Trust Royal*, [1992] 2 R.C.S. 499;

Hasbro Inc. v. *Clue Computing Inc.*, 994 F Supp. 34, 38 (D. Mass 1997);

Hydro-Québec c. *Benedek* [1995] R.L. 436 (C.Q.M.);

Hydro-Québec c. *Malouf,* C.Q. Montréal 500-02-014314-89, 1993-12-17;

Hydro-Québec c. *Mondor*, C.P. Joliette 705-02-000209-841, 1986-02-06;

Investors Group Inc. c. *Hudson*, J.E. 99-499 (C.S.);

Labbé v. *M.N.R.*; [1967] Tax ABC 697, 67 TDC 483;

Landerman c. *Landerman*, [1990] R.D.J. 542 (C.A.);

McCallum c. *Babineau*, [1956] B.R. 774, p.780;

McMullan c. *R.*, (1979) 47 C.C.C. (2d) 499 (CA), (1978) 42 C.C.C. (2d) 67;

BIBLIOGRAPHIE

Mousseau c. *Société de gestion Paquin Ltée*, [1994] R.J.Q. 2005 (C.S.), p. 2008, appel rejeté;

Nolin c. *Bellavance*, [1979] C.A. 168;

Otis c. *Équipements J.G.M.*, C.Q. 155-32-000132-968, 1997-09-02;

Panavision Int'l, LP v. *Toeppen*, 141 F (3d) 1315 (9th Cir. 1998);

Playboy Enterprises Inc. v. *Frena*, 839 F. Supp. 1552 (N.D. Fla. 1993);

Poulin c. *Pratt*, [1994] R.D.J. 301 (C.A.);

Productions Serpent II inc. c. *SOGIC*, J.E. 94-284 (C.S.), C.S. Montréal 500-05-013627-920;

Protection de la Jeunesse – 661, J.E. 94-307– C.Q. Montréal 500-03-001948-937;

Religious Technology Centre v. *Netcom On-Line Communication Services*, 907 F. Supp. 1361 (N.D. Cal. 1995);

Sega Enterprises Limited v. *Maphia*, 857 F. Supp. 679 (D.D. Cal. 1994);

Tessier c. *Ville de Québec*, [1979] R.P. 193 (C.S.);

Transport Dragon Limitée c. *Mauro Grillo Excavation,* C.Q Montréal 500-22-006747-979, 1997-08-07 (97BE-844);

Zellers Inc. et *Syndicat des employés et employées des magasins Zellers d'Alma et de Chicoutimi* [1998] RJDT (TA), J.E. 98T-1076;

Zippo Mfg v. *Zippo Dot Com Inc.*, 952 F Supp. 1119, 1124 (W.D. Pa 1997);

Zodiak International Productions c. *The Polish People's Republic*, [1983] 1 R.C.S. 529.

Monographies

A. GAHTAN, M. KRATZ, F. MANN, « *Internet Law, a practical guide for legal and business professionals* », Toronto, Carswell, 1998;

A. GATHAN, « *Electronic Evidence* », Toronto, Carswell, 1999;

A. LUCAS, « Le droit de l'informatique », dans *Presses Universitaires de France*, Paris, Éd. Thémis, 1994;

BIBLIOGRAPHIE

A. REDFERN, M. HUNTER, M. SMITH, « *Law and Practice of International Commercial Arbitration* », 2e éd, London, Sweet and Maxwell, 1991;

B. WRIGHT, J. WINN, « *The Law of Electronic Commerce* », 3e ed., New York, Aspen Law & Business, 1999;

Commentaires du ministre de la Justice, t. 2, Québec, Publications du Québec, 1993;

D. JOHNSTON, D. JOHNSTON, S. HANDA, « *Undertaking the Information Highway* », Toronto, Stoddart Publishing Co. Ltd., 1995;

D. JOHNSTON, S. HANDA, C. MORGAN, « *Cyber Law* », Montréal, Stoddart, 1997;

D. POULIN, « *Inforoutes et pratiques du droit: possibilités et perspectives* », Montréal, Chambre des notaires du Québec, 1996;

D. POULIN, P. TRUDEL, E. MACKAAY, « *Les autoroutes électroniques: usages, droit et promesses* ». Textes présentés lors d'un colloque tenu à Montréal le 13 mai 1994, Cowansville, Québec, Éditions Yvon Blais, 1995;

E. MACKAAY, « *Les incertitudes du droit* », Faculté de droit de l'Université de Montréal, Centre de recherche en droit public, Montréal, Éd. Thémis, 1999;

J. BELLEMARE, L. VIAU, « *Droit de la preuve pénale* », Montréal, Éd. Y. Blais, 1991;

J. C. ROYER, « *La preuve civile* », 2e éd., Cowansville, Éd. Y. Blais, 1995;

J. HAGEL III, A.G. ARMSTRONG, "*Net Gain, Expanding markets through virtual communities*". Harvard Business School Press, 1997;

J.-H. WIGMORE, « *Evidence in Trials at Common Law* », vol. 1 no 7A, Toronto, Little, Brown & Company, 1983;

J.-L. BAUDOIN, P.-G. JOBIN, « *Les Obligations* », 5e éd., Cowansville, Éd. Y. Blais, 1998;

K. BENYEKHLEF, V. GAUTRAIS, « *Échange de documents informatisés : Contrat type commenté* », mise à jour 1995;

L. DUCHARME, « *Précis de la preuve* », 5e éd., Montréal, Wilson & Lafleur Ltée, 1996;

M. MARTEL, P. MARTEL, « *La compagnie au Québec : les aspects juridiques* », vol. 1, Montréal, Wilson & Lafleur Ltée, 1996;

P. TRUDEL, F. ABRAN, K. BENYEKHLEF, S. HEIN, « *Le droit du cyberespace* », Faculté de droit de l'Université de Montréal, Centre de recherche en droit public, Montréal, Éd. Thémis, 1997;

BIBLIOGRAPHIE

P. TRUDEL, G. LEFEBVRE, S. PARISIEN, « *La preuve et la signature dans l'échange de documents informatisés au Québec* », Montréal, Les Publications du Québec, 1993;

R. MERKIN, « *Arbitration Law* », LLP, 1991;

Records Retention, Statutes and Regulations, vol. 3, Ontario, Carswell, 1999;

S. PARISIEN, P. TRUDEL, « *L'identification et la certification dans le commerce électronique- Droit, sécurité, audit et technologies* », Cowansville, Québec, Éditions Yvon Blais, 1996;

S. PARISIEN, P. TRUDEL, V. WATTIEZ-LAROSE, « *L'identification et la certification dans le commerce électronique : droit, sécurité, audit et technologies* », Cowansville, Éd. Yvon Blais, 1996;

S. PARISIEN, P. TRUDEL, V. WATTIEZ-LAROSE, « *La conservation des documents électroniques : Les phases post-transactionnelles du commerce électronique* », Faculté de droit de l'Université de Montréal, Centre de recherche en droit public, Montréal, 14 décembre 1998.

Articles et Rapports

A. ERLANDSSON, « *Electronic Record Management, a Literature Review* », Conseil national des archives, avril 1996, Études CIA 10;

A. RINALDI, « *The Net: User Guidelines and Netiquette* », disponible au site http://www.enid.org/enidscools/co/enidhigh/internet;

Avis du CAI concernant le *Projet de loi C-6* disponible au site http//www.cai.gouv.qc.ca/9981514htm ainsi que les mémoires de l'Association du Barreau canadien concernant le *Projet de loi C-6* et de l'Association du Barreau du Québec, respectivement de mars 1999 et de février 1999;

B. TROTTIER, « *L'archivage des documents sous forme électronique : aspects pratiques et légaux* », *Congrès annuel du Barreau du Québec*, 1997;

C. FABIEN, « *La communicatique et le droit de la preuve* », Actes du Colloque conjoint des Facultés de droit de l'Université de Poitiers et l'Université de Montréal, 1990;

C. KEN, « *Computer-Produced Records in Court Proceedings* », *Uniform Law Conference of Canada*, juin 1994;

Conseil international des archives, « *Guide for managing electronic records from an archival perspective*", février 1997;

BIBLIOGRAPHIE

D. MASSE, « *La preuve des inscriptions informatisées* », Montréal, 1997, disponible au site http://www.chait-amyot.ca/;

É. DUNBERRY, « *Les monnaies électroniques : un cas d'espèce* », (1997) 76 *R. du B.* 332;

É.A. CAPRIOLI, « *Les tiers de confiance dans l'archivage électronique : une institution juridique en voie de formation* », dans *Les incertitudes du droit*, Montréal, Éd. Thémis, 1999;

F. CHAMPIGNY, « *L'inscription informatisée en droit de la preuve québécois* », dans *Développements récents en preuve et procédure civile (1996)*, Cowansville, Éd. Y. Blais, 1996;

F. FROOMKIN, « *Flood Control on the Information Ocean, Living With Anonymity Digital Cash and Disputed Database*", disponible au site http://www.digicash.com;

G. LEFEBVRE, « *La preuve en matière d'échange de documents informatisés* », (1995) 74 *R. du B.* 619;

G. MASSE, « *Du témoignage apparemment admissible à titre de ouï-dire au ouï-dire apparemment admissible à titre d'écrit* », *dans Développements récents en preuve et procédure civile*, Cowansville, Éd. Y. Blais, 1996;

GREGORY ET TOLLEFSON, « *Projet de loi uniforme sur la preuve électronique* », Annexe N, *Conférence pour l'harmonisation des lois au Canada*, disponible au site http://www.law.ualberta.ca/alri/ulc;

H. MUSTILL, « *Arbitration: History and Background* », (1989) 6 *Journal of International Arbitration*;

I. KYER, « *Computer Record as Courtroom Evidence* », *Computer Law*, vol. 1, no 8, août 1984;

I.W. OUTERBRIDGE, « *The Admissibility of Computer-Produced Evidence* », *The Advocate's Society Journal*, avril 1985;

J.D. GREGORY, « *Electronic Legal Records: Pretty Good Authentification*", disponible au site http//www.callacbd.ca/summit/;

J.D. GREGORY, « *Solving Legal Issues in Electronic Commerce* », disponible au site http//www.ualberta;

J. FRÉMONT, J.P. DUCASSE, « *Les Autoroutes de l'Information : Enjeux et Défis* », Actes du Colloque tenu dans le cadre des Huitièmes Entretiens Centre Jacques Cartier –

BIBLIOGRAPHIE

Rhone – Alpes, 5 au 8 déc. 1995, Université de Montréal, Centre de recherche en droit public;

J.R. REINDERBERG, « *The Use of Technology to Assure Intenet Privacy : Adapting Labels and Filters for Data Protection*", 1997, 3 Lex Electronica disponible au site http://www.lex-informatica.org/reidenbe.html;

J.R. REIDENBERG « *L'instabilité et la concurrence des régimes réglementaires dans le cyberespace* » dans *Les incertitudes du droit*, sous la direction de E. MACKAAY, Montréal, Éd. Thémis, Faculté de droit de l'Université de Montréal;

J.R. REINDERBERG, « *Lex informatica : The Formulation of Information Policy Rules Through Technology* », (1988) 76 *Texas L. Rev.* 553;

L. DUCHARME, « *Le nouveau droit de la preuve en matière civile selon le Code civil du Québec* », dans *Réforme du Code civil*, Québec , Les Presses de l'Université Laval, 1993;

L. DUCHARME, « *Le nouveau droit de la preuve en matières civiles selon le Code Civil du Québec* », [1992] 23 *R.G.D.* 5;

L. HELM, « *Business-to-business trade set to dominate Internet* », *Financial Post*, 18 février 1999;

L. LILKOFF, « *La force probante des registres et factures de commerce* », (1967-68) *C de D* 794;

L.C. SMITH, « *The Evidence Act 1995 (cth): Should Computer Data Be Presumed Accurate? », Monash University Law Review*, vol. 22, no 1, 1996;

N. L'HEUREUX, L. LANGEVIN, « *La Pratique des cartes de paiement au Québec : l'Apport du droit comparé* »,(1990) 50 *R. du B.* 237;

P. TRUDEL, M. RACICOT, A.R. SZIBBO, M.S. HAYES, « *L'espace cybernétique n'est pas une terre sans loi: étude des questions relatives à la responsabilité à l'égard du contenu sur internet* », Ottawa, Industrie Canada, 1997;

P. BIENVENU, « *Guide de rédaction des clauses d'arbitrage et de droit applicable dans les contrats commerciaux internationaux* », (1996) 56 *R. du B.* 39;

P. TRUDEL, « *Introduction au droit du commerce électronique sur l'Internet* », (1995) 55 *R. du B.* 521;

P. TRUDEL, « *Les effets juridiques de l'autoréglementation* », (1989) 19 *R.D.U.S.*;

P.G. JOBIN. « *La rapide évolution de la lésion en droit québécois* », (1977) 29 *Rev. Int. Droit comp.* 331;

BIBLIOGRAPHIE

Rapport de la Conférence ministérielle d'Ottawa du 7 au 9 octobre 1998, *Un Monde sans frontières : Concrétiser le potentiel du commerce électronique mondial*, OCDE, SG/EC (98) 14/Rev6, p. 4 et les Annexes 1 et 2;

Rapport de la délégation canadienne à la trente-quatrième session du Groupe de travail de la CNUDCI sur le commerce électronique et les documents préparatoires disponibles au site http://www.canada.justice.gc.ca/Commerce/ un99gau_fr.html;

Rapport des sondeurs ScienceTech Communications, « *Perspectives sur le commerce électronique et les Politiques publiques* », MIQ-98, réalisé en octobre 1998;

Résumé de synthèse du Comité de la Politique de l'Information, de l'Informatique et des Communications (PIIC) de l'Organisation de Coopération et de Développement Économique (OCDE) intitulé « *The Economic and Social Impacts of Electronic Commerce: Preliminary Findings and Research Agenda*", disponible au site http://www.oecd.org//subject/e_commerce/summary.htm préparé en vue de la Conférence ministérielle d'Ottawa des 7 au 9 octobre 1998;

« Summary of Electronic Commerce and Digital signature legislation » disponible au site http://www.mbc.com/ecommerce/legis;

« Challenges of the Internet for Agency, Distribution and Franchising Agreements », *International Bar Association*, vol. 27, no 4, juin 1999;

Documents de consultation et les comptes rendus de réunions annuelles de la CHLC en matière de preuve électronique disponibles au site http://www.law.ualberta.ca/alri/ulc;

Glossaire de l'ingénierie documentaire, Rapport synthèse du Chantier en ingénierie documentaire intitulé *La gestion des documents adaptés à l'inforoute gouvernementale,* janvier 1999.