

Université de Montréal

Nature et impacts juridiques de la certification
dans le commerce électronique sur Internet

par

Bernard Brun

Faculté de droit

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

Mars 2000

© Bernard Brun, 2000



E-1184-11 on 6

AZBD
U54E
2000
V.025

10/10/00 10:30 AM (UTC)

10/10/00 10:30 AM (UTC)

10/10/00 10:30 AM (UTC)

10/10/00 10:30 AM (UTC)



10/10/00 10:30 AM (UTC)

10/10/00 10:30 AM (UTC)

Identification du jury

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :

Nature et impacts juridiques de la certification
dans le commerce électronique sur Internet

présenté par :

Bernard Brun

a été évalué par un jury composé des personnes suivantes :

Président-rapporteur: Karim Benyekhlef

Directeur de recherche: Pierre Trudel

Membre du jury: Pierre Noreau

Mémoire accepté le : ..1er septembre 2000.....

Sommaire

Le sujet sur lequel porte la présente étude est inspiré de la problématique à la base du développement du commerce électronique : la confiance.

En effet, l'accroissement exponentiel du nombre d'internautes et des sites Web commerciaux pose un sérieux problème à ce niveau. Ces sites présentent au public une information et des services divers mais peu vérifiables. Ainsi, le principal obstacle au développement du commerce électronique avec les particuliers est le manque de confiance qu'inspire les lieux visités. En effet, comment savoir si l'entreprise existe, quelles sont ses politiques concernant la sécurité ou la gestion des renseignements personnels, etc...

La vérification et la certification des sites apparaît comme une solution de plus en plus attrayante et utilisée pour ajouter cet élément de confiance. Déjà, de nombreux sceaux de qualité sont apparus sur les sites commerciaux. Certains sceaux portent sur la confidentialité tandis que d'autres ciblent la protection des consommateurs. La certification peut provenir de la compagnie même, d'un tiers certificateur ou d'un organisme public. Ces éléments constituent des balises et repères importants pour le consommateur sur Internet.

Toutefois, les incidences légales sont multiples et certains concepts demeurent flous. Pour apporter une réponse à ces questions, nous définiront le concept de certification des sites Web et ses enjeux dont plus particulièrement la problématique de la confiance des consommateurs. Les différents objets de la certification seront analysés, tant au niveau de l'entité, du contenu du site que de la dimension transactionnelle de celui-ci.

Les processus possibles et les impacts de la certification occupent la seconde partie du travail. Il s'agit d'examiner successivement les étapes menant à la certification, soit

l'établissement des standards, de l'évaluation de l'entité et de la certification elle-même. L'analyse des impacts de la certification, tant sur le plan de la portée, de la responsabilité légale et des effets sur la concurrence de la certification constitue quant à eux, l'aboutissement de la recherche, soit de savoir quel est l'impact juridique d'un tel mécanisme.

Le but de la recherche est de permettre au lecteur de mieux cerner ce phénomène de l'utilisation de la certification sur Internet avec ses avantages et ses limites. Certes, cet outil peut s'avérer très utile pour bâtir la confiance des consommateurs, promouvoir l'essor du commerce électronique et constituer une forme d'autoréglementation. Toutefois, mal utilisé ou mal encadré, il peut engendrer l'effet inverse et détruire cette confiance si fragile à construire dans un environnement dématérialisé.

TABLE DES MATIÈRES

INTRODUCTION	1
PARTIE I – OBJECTIF DE LA CERTIFICATION	4
A. NATURE ET ENJEUX DE LA CERTIFICATION	4
1. DÉFINITION DE LA CERTIFICATION.....	4
2. CONCEPTS CONNEXES.....	9
2.1 Normalisation et standardisation	9
2.2 Accréditation	10
2.3 Certification et audit.....	11
3. ENJEUX DE LA CERTIFICATION.....	12
3.1 Contexte particulier du commerce par Internet.....	13
3.2 La problématique de la confiance	13
3.3 Enjeux pour les consommateurs	16
3.4 Enjeux pour les entreprises	17
3.5 Enjeux pour les autorités publiques	18
B. DIMENSION JURIDIQUE DE LA CERTIFICATION	20
1. L'ENTITÉ CERTIFIÉE	21
1.1 Existence de l'entité.....	21
1.2 Capacité de contracter	22
1.3 Droit et juridiction applicable.....	23
2. LES ÉLÉMENTS CONSTITUTIFS ET LE FONCTIONNEMENT DU SITE WEB	25
2.1 Noms de domaine	25
2.2 Sécurité du site	26
2.3 Les liens.....	28
2.4 Les clauses légales et règles d'utilisation du site.....	29
3. LES BIENS ET SERVICES OFFERTS.....	30
3.1 Information sur le site.....	30
3.2 Respect des règles concernant la protection des consommateurs.....	31
3.3 Respect de la propriété intellectuelle.....	32
4. LES TRANSACTIONS EN LIGNE.....	34
4.1 Intégrité de la communication.....	34
4.2 La protection des renseignements personnels	35
4.3 Authentification de l'interlocuteur et communication du consentement	37
4.4 Le mécanisme de paiement.....	38
PARTIE II – PROCESSUS ET IMPACTS JURIDIQUES	43
A. LE PROCESSUS DE CERTIFICATION	43
1. L'ÉTABLISSEMENT DE STANDARDS.....	44
1.1 Rôle et évolution des standards.....	44

1.2 Les niveaux des standards	45
1.3 Standard de facto et standard officiel.....	46
2. ÉVALUATION DE L'ENTITÉ.....	47
2.1 L'audit interne.....	48
2.2 La déclaration volontaire.....	49
2.3 L'audit externe.....	50
3. LA CERTIFICATION.....	51
3.1 Décision du certificateur.....	51
3.2 Les marques de certification.....	52
3.3 Le suivi de la certification.....	53
3.4 Des exemples de certification de sites Web.....	54
3.4.1 TRUSTe.....	55
3.4.2 Better Business Bureau.....	59
3.4.3 Webtrust.....	62
B. IMPACTS DE LA CERTIFICATION	65
1. LA PORTÉE DE LA CERTIFICATION.....	65
1.1 Le type de certification.....	66
1.2 Les standards utilisés.....	67
1.3 Le mode d'évaluation.....	67
1.4 Le traitement de l'information.....	68
1.5 Le mécanisme contractuel.....	69
1.6 Le statut du certificateur.....	70
1.7 La reconnaissance.....	72
2. LES RESPONSABILITÉS SOUS-JACENTES.....	74
2.1 Nature de la relation entre le certificateur et le candidat.....	75
2.2 Responsabilité face au certifié.....	76
2.2.1 Le refus de certification.....	77
2.2.2 Le retrait de certification.....	78
2.3 Nature de la relation entre le certificateur et le tiers.....	79
2.4 La responsabilité face aux tiers.....	80
2.5 La résolution des conflits.....	83
3. LE DROIT DE LA CONCURRENCE.....	86
3.1 Effets de la certification sur la concurrence.....	86
3.2 L'impact des standards de facto.....	88
3.3 L'imposition d'un standard officiel.....	91
CONCLUSION	93
BIBLIOGRAPHIE.....	97
INDEX DES TEXTES LÉGISLATIFS CITÉS	109
ANNEXE A.....	110
ANNEXE B.....	113
ANNEXE C.....	115

INTRODUCTION

Au cours des dernières années, nous avons vu le rythme des développements technologiques s'accroître, notamment sur le plan des moyens de communication. Cette situation a pour effet direct de faciliter les échanges et, notamment, de stimuler et d'accroître considérablement le nombre d'échanges commerciaux.

Auparavant, et encore aujourd'hui, la plupart des échanges mettent les personnes en présence physique l'une de l'autre. Cette situation donne accès à des éléments objectifs concernant l'éventuel partenaire et permet ainsi de s'évaluer mutuellement. Ce contact est nécessaire afin de créer entre eux le lien de confiance indispensable au succès de leur relation.

La tendance naturelle de mettre à profit les nouvelles technologies disponibles dont notamment les technologies de l'information crée un paradoxe surprenant en matière de contact et de création d'un lien de confiance. D'un côté, si les technologies de l'information facilitent les communications, elles ont toutefois pour conséquence, à la fois utile et néfaste, de ne plus requérir la présence physique des protagonistes.

Le contact est à la base de l'échange. Ce contact peut se faire sans aucun intermédiaire par le biais de sites Internet. Ces sites présentent au public une information et des services divers, mais peu vérifiables. De plus, la facilité à créer des illusions est considérable.

Les consommateurs acceptent de visiter les lieux en raison du fait qu'ils présentent une information intéressante et variée. Cependant, la confiance demeure une lacune importante dans une optique de transaction.

Ce manque de confiance constitue à ce jour le principal obstacle au développement du commerce électronique avec les particuliers. En effet, comment savoir si l'entreprise existe, quelle juridiction est applicable, quelles sont ses politiques

concernant la sécurité ou la gestion des renseignements personnels, quelles sont ses pratiques commerciales, bref, quelle sera la situation si une difficulté se présente dans le cadre de la transaction ?

Internet est un milieu que plusieurs présentent comme un « monde virtuel ». Cette qualification est juste dans le sens que les éléments physiques qui ont servi de point de repère aux consommateurs ne peuvent plus répondre à cet objectif sur ce réseau informatique. Nous en tirons une conclusion toute simple : les consommateurs ont besoin de nouveaux repères car ceux-ci nous apparaissent essentiels.

C'est dans ce cadre qu'on parle de plus en plus de standardisation et de certification. Ces deux concepts se veulent de nature objective. Leur but est de rendre possible l'évaluation d'une personne, d'une entreprise, d'un produit ou d'un service au moyen de critères préétablis.

En quelque sorte, l'évaluation ne se fait plus entre deux parties en présence l'une de l'autre, mais par l'intermédiaire d'un tiers indépendant.

La vérification et la certification des sites apparaissent comme une solution de plus en plus utilisée pour ajouter cet élément de confiance¹. Déjà, de nombreux sceaux de qualité sont apparus sur les sites commerciaux. Certains sceaux portent sur la confidentialité tandis que d'autres ciblent la protection des consommateurs. La certification peut provenir de la compagnie même, d'un tiers certificateur ou d'un organisme public. Ces éléments constituent des balises et repères importants pour le consommateur qui navigue sur le réseau Internet.

Les incidences légales sont multiples et les concepts méritent d'être précisés. Notre étude consiste donc à définir la certification, ses enjeux et ses implications légales

¹ « La certification représente l'un des développements les plus importants des comportements économiques des dernières décennies. », Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997 à la page 3-46. Aussi, selon une étude de BBBOnline, 84% des personnes s'estimeraient rassurés par une certification. Voir à ce sujet : Thierry Trompette, « Une nouvelle mission : la certification des sites Web de commerce électronique », (1999) 4 Les Cahiers de l'Audit 34.

dans la perspective de mieux cerner le rôle et la responsabilité des acteurs. Nous pourrions ainsi découvrir si la certification est réellement une nécessité, un outil ou simplement un caprice du développement du commerce sur Internet. De plus, il y a lieu d'étudier si un type de certification est à préconiser.

Nous aborderons donc plus particulièrement la problématique de la confiance des consommateurs, les différents objets de la certification, les processus possibles (de l'établissement des standards à leur évaluation qui mèneront éventuellement à la certification) et nous terminerons par les impacts de la certification.

Partie I – Objectif de la certification

A. Nature et enjeux de la certification

La nature et les objectifs de la certification sont encore confus aux yeux de plusieurs. Pour en étudier correctement l'utilisation et la portée, il est important de bien définir le cadre de la certification, notamment en établissant en quoi elle consiste et en la distinguant des divers concepts qui s'en rapprochent ou la complètent.

Les enjeux auxquels s'attaque la certification dans le cadre du commerce électronique doivent également être identifiés et discutés. Ils constituent la justification de l'utilisation de ce mécanisme pour le commerce sur Internet auxquels se greffent les autres éléments de la recherche.

1. Définition de la certification

La certification en matière commerciale est un concept relativement nouveau dont la signification peut varier selon le domaine dans lequel on se trouve. Ce mot, proche parent de « certificat », existe depuis longtemps, mais s'est acquis une nouvelle renommée avec l'ouverture des marchés. Tout comme son cousin, il provient du terme latin « certus », qui signifie : décidé, résolu, arrêté, fixé, déterminé, précis, convenu, certain, sûr, clair, manifeste, fidèle.

La certification de métier dans les corps professionnels ou encore de chèques ou effets de commerce certifiés dans le milieu financier est connu depuis longtemps. Dans le milieu commercial, la première utilisation visait la certification de produits.

Dans son sens générique, les dictionnaires donnent plusieurs sens à la certification qui varie de l'assurance² à l'attestation, la licence ou même la garantie³.

² Dictionnaire Universel Francophone, Édition Hachet/Edicef, 1997 <http://www.francophonie.hachet-livre.fr>.

De notre côté, aux fins de la présent étude, nous nous référons à une définition qui se veut un peu plus précise, qui se rapproche davantage de ses racines latines et qui se lit comme suit :

« La certification est une procédure par laquelle une tierce partie donne une assurance écrite qu'un produit, un service, un système qualité, un organisme est conforme à des exigences spécifiées. »⁴

Cette définition conserve néanmoins une portée générale. Dans le domaine de l'électronique et des technologies de l'information, la notion de certification a été souvent assimilée uniquement au concept de sécurité⁵.

La certification est d'abord et avant tout un outil nous donnant une mesure qui se veut objective suivant des critères déterminés. Elle permet ainsi la comparaison entre différents produits ou services, ce qui lui a valu une analogie avec la balance comme outil d'analyse comparative⁶.

Son apparition est intimement liée au phénomène de l'ouverture et à la mondialisation des marchés. Pour s'adapter à cette nouvelle réalité, le concept de qualité a pris une importance particulière dans les entreprises. Ce concept s'est d'abord penché sur les questions d'hygiène et de sécurité des produits⁷.

Par la suite, des difficultés sont apparues de plus en plus manifestes au niveau des échanges. Celles-ci ont amené un questionnement au niveau de la nécessité d'une compatibilité dont la réponse devait d'abord s'exprimer sous la forme d'une standardisation ou d'une normalisation.

³ Merriam-Webster Dictionary, <http://www.m-w.com/dictionary.htm> (consulté le 22-11-1999).

⁴ Alain Couret, Jacques Igalens et Hervé Penan, *La Certification*, Presses Universitaires de France, Paris, 1995, Collection Que sais-je ?, numéro 3006, page 9. On retrouve une définition similaire dans Rae, Andrew, K., Hans-Ludwig Hausen, Philippe Robert, *Software Evaluation for Certification, Principles, Practice and Legal Liability*, (1995), McGraw Hill Book Company, England, à la page 2.

⁵ Thierry Piette-Coudol, « *Certification électronique : pratique et modélisation* », <http://www.e-betobe.com/texteece.htm> (consulté le 13-11-1999).

⁶ Jean-Marie Ponthier, « La certification outil de la modernité normative », 30 (1996) *Dalloz-Sirey*, c. 355-360., page 355.

La certification s'inscrit dans la suite logique de la normalisation. Elle est une étape ultérieure de ce processus. Une fois les standards établis, la certification donne la confirmation du respect de ceux-ci par un organisme indépendant. Les marques de certification sont quant à elles la façon d'en publiciser la certification⁸.

La certification peut par ailleurs couvrir différents éléments et être de portée variable. À titre d'exemple, nous sommes plus familiers avec la certification comptable ou fiscale. Il s'agit essentiellement d'une certification des comptes selon les méthodes comptables reconnues⁹. Les comptables ont d'ailleurs profité de leur familiarité avec le milieu de la certification en devenant les acteurs les plus dynamiques du développement de ce phénomène sur Internet¹⁰. Une certification peut également s'adresser à la dimension technique d'un produit ou service, c'est-à-dire porter sur des spécifications techniques de ceux-ci.

Affirmative
do-tesse

Plus rare est toutefois la certification de nature juridique. En réalité, ce type d'approche n'entre pas vraiment dans la conception que les juristes ont de leur travail. Le terme certification étant une assurance de conformité à certaines règles, la certification légale consisterait alors en une assurance de la conformité à une ou à l'ensemble des règles de droit.

Traditionnellement, parmi les actes qui sont de leur ressort exclusif¹¹, les conseillers juridiques émettent des avis juridiques. Ceux-ci sont présentés comme des opinions et non des assurances. Des réserves non équivoques sont d'ailleurs prudemment placées à ce sujet sur les textes. La distinction entre l'obligation de moyen et l'obligation de résultat en tire là toute son importance.

⁷ Geneviève Iacono, « La certification d'assurance qualité : De nouvelles questions pour le Droit ? », (1994) Revue Internationale de Droit Économique 63, p. 63 .

⁸ Voir partie II A paragraphe 3.2.

⁹ Alain Couret, Jacques Igalens et Hervé Penan, *La Certification*, Presses Universitaires de France, Paris, 1995, Collection Que sais-je ?, numéro 3006, section sur la certification des comptes.

¹⁰ Citons ici l'exemple de l'organisme de certification Webtrust dont la mécanique est gérée par l'association des comptables.

¹¹ Article 128 de la *Loi sur le Barreau*, L.R.Q., c. B-1.

Les juristes sont pleinement conscients que le droit n'est pas une science exacte. Il existe toujours une part variable d'incertitude dans les opinions émises. La venue d'une procédure de certification juridique risque donc de recevoir un accueil inquiet de la communauté juridique.

À ce jour, de nombreuses firmes d'avocats proposent des « audits juridiques » des sites Web¹². Il s'agit de la vérification des divers aspects d'un site ayant une dimension légale. La vérification se solde par une opinion, mais en aucun cas par une certification. La différence essentielle entre l'opinion juridique et une éventuelle certification se situe dans le fait que l'opinion est préparée à la demande du client et lui est destinée exclusivement sauf exception. En revanche, la certification, même si elle bénéficie à l'entreprise, est d'abord émise à l'attention du tiers, en l'occurrence le consommateur.

Malgré le choc dans les mœurs légales que peut représenter la certification juridique d'un site Web, c'est pourtant de ce côté que se dirige la demande des entreprises. Il ne s'agit plus simplement d'effectuer une vérification et d'émettre une opinion, mais de certifier la conformité à certaines règles puisque c'est précisément l'impossibilité d'avoir de telles assurances qui fait actuellement défaut sur Internet.

Le niveau d'une certification peut également être variable. Sur Internet, on a en effet vu apparaître une première forme de certification, soit la certification d'existence. La certification de conformité est celle qui tente actuellement de se faire valoir et qui subira sans doute le plus de développement dans les prochaines années.

¹² Ces firmes, américaines en majorité, exposent une listes d'éléments à vérifier sur un site Web et proposent leurs services pour un audit juridique. Voir notamment : Rochelle S. Blaustein, « *Does Your Website Need A Legal Audit ?* », <http://www.patentplus.com/webaudit.html> (Dernière modification le 21 novembre 1998 ; consulté le 24 août 1999); Stephen C. Brandt, « *Legal Audit Checklist* », Stafford Frey Cooper, <http://www.buildyourbusiness.com/> (consulté le 24 août 1999); Gary Dunn « *Legal Audit for Websites* », November/December 1997, Computer & Technology Law, <http://www.cc.ubc.ca/ccandc/nov-dec97/audit.html> (consulté le 24 août 1999); Nicole A. Wong et James F. Brelsford, « *Conducting Website Legal Audits* » : a U.S. perspective, <http://www.perkinscoie.com/webrelease/webaudits.html> (consulté le 24 août 1999); Beck & Arad LLP, " Legal SiteCheck™ ", <http://www.legalsitecheck.com> (©1998, consulté le 14 août 1999).

Finalement, certains se sont penchés longuement sur la qualification de la certification à ce niveau pour en conclure qu'il s'agit du « cas typique de l'acte complexe »¹³. Cette affirmation mérite quelques commentaires.

D'abord, il est important de bien situer le contexte de la certification, à savoir si elle survient entre personnes privées ou si elle implique l'intervention du pouvoir public et possède un cadre réglementaire. Les deux situations sont possibles et très différentes. Le cadre réglementaire d'une certification donne à l'acte un caractère public.

Nous nous intéressons toutefois ici davantage à la certification issue d'organismes privés. Dans le domaine privé, le mécanisme menant à la certification comporte une relation consensuelle entre le candidat et le certificateur. L'étape ultime quant à elle, soit celle de l'attribution ou non de la certification, peut apparaître comme un acte unilatéral de la part du certificateur. Ainsi, certains ont affirmé que l'action de certifier comme tel doit à notre avis être considérée comme un acte unilatéral¹⁴. Il faut être prudent avec une telle affirmation. Bien que la décision de certifier ou non le candidat relève du certificateur, il faut considérer le tout dans son ensemble contractuel. De plus, les processus et mécanismes utilisés varient de manière importante entre divers programmes ce qui a un impact important sur le mode d'attribution de la certification.

Si la structure utilisée est de nature à avoir un impact sur la qualification de la relation entre les parties, elle sera certainement de nature contractuelle entre parties privées..

¹³ Geneviève Iacono, « *La certification d'assurance qualité : De nouvelles questions pour le Droit ?* », (1994) *Revue Internationale de Droit Économique* 63, p. 72.

¹⁴ Geneviève Iacono, « *La certification d'assurance qualité : De nouvelles questions pour le Droit ?* », (1994) *Revue Internationale de Droit Économique* 63, p. 72.

2. Concepts connexes

La certification côtoie de nombreux autres concepts qui s'en rapprochent ou qui, parfois, peuvent en faire partie. Nous tenterons ici d'établir les différences existant entre la certification et certains de ces concepts.

2.1 Normalisation et standardisation

La normalisation et la standardisation sont des concepts voisins.

La normalisation est présentée comme l'établissement et la mise en application d'un ensemble de règles et de spécifications ayant pour objet de simplifier, d'unifier et de rationaliser les produits industriels, les unités de mesure, les symboles, etc.¹⁵ La standardisation, quant à elle, est l'unification, l'uniformisation de tous les éléments d'une production¹⁶.

La certification n'est pas complètement étrangère à ces concepts puisque ce sont des standards ou des normes sur lesquels se basera l'organisme certificateur pour conclure ou non à une certification. Comme l'explique le professeur Couret, l'information normative constitue un référentiel privilégié de la certification¹⁷.

L'établissement de standards est d'une importance capitale puisqu'il permet aux entreprises de s'ouvrir à de nouveaux marchés en répondant aux exigences de base de ceux-ci. La certification en est un élément complémentaire qui vient confirmer la

¹⁵ Dictionnaire Universel Francophone Édition Hachette/Édicef, 1997 <http://www.francophonie.hachet-livre.fr>

¹⁶ Voir à ce sujet : Bureau de normalisation du Québec (BNQ), <http://www.criq.qc.ca/bnq> ; Le Conseil Canadien des Normes (CCN), <http://www.scc.ca> ; Federal Electronic Commerce Program Office, <http://www.ec.fed.gov/> ; L'association canadienne de normalisation (CSA), <http://www.csa.ca> ; L'association française de normalisation (AFNOR), <http://www.afnor.fr> ; L'association française pour l'assurance de la qualité (AFAQ), <http://click.rever.fr/afaq/> ; L'organisation internationale de normalisation (ISO), <http://www.iso.ch> ; Secretariat for Federal EDI, <http://snad.ncsl.nist.gov/fededi/> (standards pour EDI).

¹⁷ Alain Couret, Jacques Igalens et Hervé Penan, *La Certification*, Presses Universitaires de France, Paris, 1995, Collection Que sais-je ?, numéro 3006, page 91.

conformité à ces standards, standards qui peuvent être officiels ou avoir été développés *de facto* par un secteur donné¹⁸.

2.2 Accréditation

Dans son sens littéral, « accréditer » est le geste de donner du crédit à quelqu'un¹⁹. La définition générale présente l'accréditation comme étant le fait de reconnaître officiellement la qualité de quelqu'un ou quelque chose. Il n'y a cependant pas nécessairement là une référence de conformité à des standards précis.

Dans plusieurs cas, le terme « accréditation » est toutefois utilisé indifféremment du concept de certification²⁰. Cette situation se présente souvent dans les textes des auteurs américains. La définition suivante en témoigne de façon éloquente :

« Accreditation can be defined as the formal expression by a private body of an authoritative opinion concerning the acceptability, under objective quality standards fairly applied, of the services rendered by a particular institutional provider. »²¹

On remarque toutefois que définie de cette façon, l'accréditation sous-entend la présence d'une autorité déléguée à un organisme privé et, de manière incidente, la participation du pouvoir public. Cet élément est distinctif de la certification. Aux États-Unis, l'accréditation est fréquemment utilisée dans les milieux de la santé²² et de l'éducation²³.

¹⁸ Kees Stuurman, « Legal aspects of standardization and certification in information technology and telecommunication : an overview », dans Kaspersen, HWK et A. Oskamp, *Amongst friends in computer law : a collection of essays in remembrance of Guy Vanderberghe*, 1996, Kluwer, page 76.

¹⁹ Dictionnaire Larousse.

²⁰ Par exemple, l'Internet Consumer Protection Agency (ICPA) fait référence sur son site à une procédure d'accréditation mise en place pour rassurer les consommateurs. Voir à ce sujet : Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, aux pages 3-48 et 20-12.

²¹ Clark C. Havighurst, « *The Place Of Private Accrediting Among The Instruments Of Government* » (1994) 57 *Law and Contemporary problems*, 1, à la page 2. Voir également la définition dans : Eleanor D. Kinney, « *Private Accreditation As A Substitute For Direct Government Regulation In Public Health Insurance Programs : When Is It Appropriate ?* », (1994) 57 *Law and Contemporary problems*, 47, à la page 49. Voir également les définitions respectives de l'accréditation et de la certification dans : Clark C. Havighurst et Peter M. Brody, « *Accrediting and the Sherman Act* », (1994) 57 *Law and Contemporary Problems*, 199, la page 199 note 2.

²² Michael, J. Astrue, « *Health care reform and the constitutional limits on private accreditation as an alternative to direct government regulation* », 57 *Law and Contemporary Problems*, 75 ; Timothy-Stoltzfus Jost, « *Medicare And The Joint*

Aux fins de la présente étude, nous emploierons le terme accréditation comme la reconnaissance d'un produit ou un individu par une personne en autorité qui, dans le cas de ce dernier, peut lui permettre de poser des gestes donnés ou de se qualifier pour avoir accès à des programmes particuliers.

Nous garderons néanmoins à l'esprit que le concept se rapproche beaucoup de la certification en ce qu'il nécessite une évaluation et fait habituellement référence à des standards.

2.3 Certification et audit

Une étape intermédiaire survient entre l'élaboration de standards et la certification quant à la conformité à ceux-ci. C'est celle de l'évaluation de l'entreprise ou de ses produits et services.

Le mécanisme d'évaluation le plus connu est sans doute l'audit. L'audit n'établit pas les standards ni ne certifie de conformité à quelque norme que ce soit. De même, il doit être distingué de l'attestation ou de l'assurance. Nous présentons l'audit comme une procédure de vérification systématique. Elle est effectuée en vue d'obtenir et évaluer objectivement une preuve, dans le but de d'établir l'exactitude de certaines affirmations entre elles et les conséquences économiques de celles-ci²⁴.

Comme nous le verrons plus loin, ce mode d'évaluation peut être effectué de différentes manières et couvrir des champs particuliers²⁵. De même, son étendue

Commission On Accreditation Of Healthcare Organizations », (1994) 57 Law and Contemporary Problems, 15 ; Eleanor D. Kinney, « *Private Accreditation As A Substitute For Direct Government Regulation In Public Health Insurance Programs : When Is It Appropriate ?* », (1994) 57 Law and Contemporary problems, 47.

²³ Matthew, W. Finkin, « *The Unfolding Tendency In The Federal Relationship To Private Accreditation In Higher Education* », (1994) 57 Law and Contemporary Problems, 89.

²⁴ Voir à ce sujet: William F. Messier, *Auditing, a Systematic Approach*, (1997) McGraw-Hill, États-Unis.

²⁵ Il existe différentes formes d'audit. Le plus communément utilisé est l'audit des états financiers. Toutefois, il existe des audits de conformité, que ce soit en rapport à des politiques internes, à la réglementation, etc... ou encore des audits opérationnels. William F. Messier, *Auditing, a Systematic Approach*, (1997) McGraw-Hill, États-Unis, aux page 11 et 12.

peut varier. L'évaluation peut porter soit sur les procédures de l'entreprise de façon générale²⁶, soit sur les processus au niveau de la qualité²⁷ ou encore être orientée sur un secteur spécifique de l'entreprise²⁸.

Certaines d'entre elles sont simples alors que d'autres s'avèrent fort complexes. La qualité de l'évaluation aura un impact important sur la qualité de la certification qui en découle.

3. Enjeux de la certification

La procédure de certification nous semble destinée à jouer un rôle primordial dans le développement du commerce électronique.

Bien entendu, l'assurance de la conformité à certaines caractéristiques est en effet nécessaire pour s'assurer d'une compatibilité et d'un échange possible. Les enjeux vont aujourd'hui au delà de la simple compatibilité dans le cadre de transactions commerciales sur Internet. Dans ce réseau qu'aucune autorité centrale ne contrôle ou ne régit, la certification est de nature à apporter une solution des plus intéressantes.

²⁶ Alvin A. Arens, James K. Loebbecke, « Auditing, an Integrated Approach », (1997), 7^e Edition, Prentice Hall, Upper Saddle River ; Etienne Barbier, « L'audit interne, permanence et actualité », (1996), 3^e Edition, Les Éditions d'Organisation, France ; Larry F. Konrath, « Auditing, concept and application, a risk analysis approach », (1993), 2nd Edition, West Publishing Company ; William F. Messier, « Auditing, a Systematic Approach », (1997) McGraw-Hill, USA. ; Jack C. Robertson, Timothy J. Louwers, « Auditing », (1999), 9^e Edition, McGraw-Hill, USA. ; Lawrence B. Sawyer, Mortimer A. Dittenhofer, « Sawyer's internal auditing, the practice of modern internal auditing », (1998), 4^e Edition, The Institute of Internal Auditor, Alta Monte Springs, USA.

²⁷ Charles A. Mills, « The Quality Audit, a management evaluation tool », (1992), ASQC Quality Press, Milwaukee, USA. ; Janet L. Smith, « The Quality Audit Handbook », (1997), ASQC Quality Press, Milwaukee, USA.

²⁸ On en retrouve fréquemment au niveau des logiciels et des technologies de l'information Barry E. Cushing, Marshall B. Romney, « Accounting Information Systems », (1993), 6^e Edition, Addison-Wesley Publishing Company, USA. ; Frederick Gallegos, Dana R. Richardson, A. Faye Borthick, « Audit and Control of Information Systems », (1987), South Western Publishing Company, USA. ; Ulric G. Gélinas, Steve G. Sutton, Allan E. Oram, « Accounting Information Systems », (1998), 4^e Edition, South Western College Publishing, USA. ; Darrill Ince, « Software quality assurance - a student introduction », (1996), McGraw-Hill Book Company, USA. ; William C. Mair, Donald R. Wood, Keagle W. Davis, « Computer Control and Audit », (1976), USA. ; Norman G. McIntosh, « The social software of accounting and information systems », (1986), John Wiley & Sons, USA.

3.1 Contexte particulier du commerce par Internet

La principale caractéristique d'Internet est le fait qu'il s'agit d'un réseau ouvert. Un réseau ouvert n'a pas de point central qui permet un contrôle des échanges qui s'y effectuent²⁹. En conséquence, toutes sortes d'information peuvent s'y retrouver, variant du meilleur jusqu'au pire.

Cette caractéristique de décentralisation a d'abord favorisé l'essor du réseau Internet. Désormais, elle risque d'avoir un effet contraire dans le cadre du développement du commerce électronique sur ce réseau. En effet, l'absence d'un point central permettant de contrôler les échanges et la qualité de ceux-ci, engendre un manque de confiance des divers intervenants qui met en péril le développement de cette façon de faire le commerce.

L'apparition de la certification comme instrument visant à faciliter le commerce sur Internet est, somme toute, récente. Peu d'analyse existe sur le sujet, encore moins dans le domaine juridique. Nous aurons donc recours fréquemment à l'utilisation d'analogies pour appuyer nos propos.

3.2 La problématique de la confiance

Cette problématique n'est pas nouvelle. Elle a surgi dès les premiers échanges sur le réseau.

La confiance l'élément essentiel autour duquel gravite toute relation commerciale. Elle est cependant difficile à établir en matière de commerce électronique³⁰. Ainsi, la fonction commerciale qui s'est récemment développée sur le réseau a accentué la sensibilité à ce problème.

²⁹ Arnaud Dufour, *Internet*, 2^{ième} édition, Presses Universitaires de France, Paris, 1996, Collection Que sais-je ?, numéro 3073.

³⁰ Voir à ce sujet: David Kosiur, « *Understanding Electronic Commerce* », (1997), Microsoft Press, Redmond, USA.

D'un côté, les technologies de l'information permettent des échanges plus rapides, plus précis en éliminant toute barrière géographique. Paradoxalement, cette situation supprime également la relation en tête-à-tête et crée des doutes sur l'identité et les qualités de l'interlocuteur.

Dans un cadre commercial, ces doutes sont extrêmement néfastes à l'initiation et à la conclusion des transactions. Bien que la mise en place de systèmes cryptographiques et autres soit de nature à en rassurer plusieurs au niveau de la sécurité des échanges et de l'existence de l'intervenant, de nombreux doutes ou un manque de compréhension subsistent quant à la qualité de ceux-ci et leur capacité de remplir leurs obligations. Or, ces éléments sont essentiels à l'émergence d'un sentiment de confiance³¹.

Avant l'essor exponentiel du réseau Internet, cette question de confiance a été soulevée de nombreuses fois en ce qui a trait aux échanges au sein de la communauté économique européenne, puis particulièrement dans le contexte du commerce électronique³². Là encore, la certification a été perçue comme un élément crucial pour favoriser les transactions dans un système ouvert puisque celle-ci ajoute l'élément de confiance jusque-là manquant³³.

Au Canada, le ministre fédéral de l'Industrie soulignait dès avril 1998 les multiples défis du commerce électronique et le fait que ceux-ci ont tous un élément simple en commun : la confiance³⁴. Récemment, deux facteurs étaient présentés comme essentiels à la croissance du commerce électronique sur Internet. Le premier, de nature purement matérielle, est l'accès à celui-ci tandis que le second est l'élément de confiance. On y souligne d'ailleurs que « tant les gouvernements que les secteurs

³¹ « *A question of trust* », Computer Weekly, 10 juillet 1997, page VII.

³² Stéphane Lefer, « *Sécurité et confiance : maître mot du commerce électronique* », Lamy Droit de l'informatique, janvier 1998, n° 1999, à la page 1. L'auteur y cite notamment une communication de la Commission Européenne du 8 octobre 1997 intitulée « Assurer la sécurité et la confiance dans la communication électronique ».

³³ Kees Stuurman, « Legal aspects of standardization and certification in information technology and telecommunication : an overview », dans Kaspersen, HWK et A. Oskamp, *Amongst friends in computer law : a collection of essays in remembrance of Guy Vanderberghe*, 1996, Kluwer, page 80.

privés doivent se préoccuper de susciter la confiance à l'égard du cybercommerce sur le plan national et international»³⁵. Cette problématique de la confiance, reconnue depuis un certain temps déjà, a attiré l'attention d'associations de professionnels et d'organismes privés qui tentent d'intervenir à différents niveaux³⁶.

Une étude américaine a estimé que les points de départ pour gagner la confiance des consommateurs sur Internet sont la mise en place d'une marque reconnue jumelée avec un site Web aisément navigable³⁷. Si la navigation du site est un élément relevant des concepteurs du site, la présence d'une marque reconnue, quant à elle, peut poser des difficultés pour la plupart des entreprises. Or, la certification peut être l'élément permettant de rencontrer cette condition.

La certification apparaît comme l'une des meilleures avenues pour bâtir ce sentiment de confiance³⁸. Dans la mesure où elle constitue en soi une marque reconnue, celle-ci rassure alors le tiers quant à la conformité d'un site à certaines exigences, que ce soit au niveau des pratiques commerciales, de la confidentialité ou de la sécurité des échanges³⁹. Elle nous apparaît également mieux adaptée à la réalité commerciale que l'idée d'attribuer des cotes aux sites Web⁴⁰.

³⁴ John Manley, ministre de l'Industrie, allocution devant la Commission ministérielle du sommet sur le commerce électronique, Ottawa, 30 avril 1998.

³⁵ John Manley, ministre de l'Industrie, Dialogue mondial des entreprises sur le commerce électronique, 13 septembre 1999, Paris, France.

³⁶ ADDSecure.Net inc., <http://www.addsecure.net> ; BBBOnline, <http://www.bbbonline.com/> ; Check-marks , <http://www.check-mark.com> ; European Information Technology Security Evaluation Criteria (ITSEC), <http://www.itsec.gov.uk> ; ICSA (NCSA) Firewall Certification, <http://www.icsa.net> ; TRUSTe, <http://www.truste.org/> ; US GOLD.gov, <http://www.usgold.gov/certification.html> ; WebAssured.com (anciennement le Web Assurance Bureau) <http://www.WebAssured.com> ; Webtrust, <http://www.cica.ca/new/index/f-wt-in.htm> ; Legal Site check www.legalsitecheck.com.

³⁷ Cheskin Research and Studio Archetype/Sapient, *Commerce Trust Study*, Janvier 1999 ; « *Gaining trust from online consumers (A survey on what online customers expect from a commerce site)* », Infoworld, 1^{er} février 1999, vol. 21, p. 41.

³⁸ La certification n'est cependant pas un remède miracle. Elle constitue davantage un additif pour ajouter l'élément de confiance. Comme l'exprime David Kosiur, même en présence de celle-ci, les commerçants sur Internet auront de la difficulté à établir le même niveau de confiance que celui dont jouissent les banques. David Kosiur, " *Understanding Electronic Commerce* ", (1997), Microsoft Press, Redmond, États-Unis, aux pages 258 et 259.

³⁹ John Fontana, « *Certification plans to help Web confidence* », Communications Week, 5 août 1996, n° 622.

⁴⁰ James E. Gaskin, *Corporate Politics and the Internet*, (1997), Prentice Hall Printers, Upper Saddle River, États-Unis, chapitre 11.

3.3 Enjeux pour les consommateurs

Le commerce sur Internet ouvre au consommateur des avenues des plus intéressantes. Il lui offre de nouvelles perspectives. Le consommateur voit ses horizons s'élargir puisque le nombre de commerçants se multiplie de même que les offres de ceux-ci. D'un autre côté, Internet donne toujours cette perception d'incontrôlable et d'inconnu.

En conséquence, le premier enjeu des consommateurs est d'obtenir de meilleures assurances concernant la qualité des produits et services offerts. Or, la certification peut répondre à cet objectif puisqu'elle constitue une forme d'assurance en regard de la conformité à certains standards. Il s'assure ainsi que son interlocuteur ou les produits auxquels il s'intéresse, répondent à des standards bien définis. Dans certains cas, la certification pourra permettre au consommateur d'obtenir une certaine forme de garantie.

Outre l'assurance, la certification a la faculté d'améliorer la perception par le consommateur des transactions commerciales qui se déroulent sur Internet. C'est grâce à cette assurance et à l'amélioration de la perception, que la certification peut apporter au consommateur un certain niveau de confiance dans ce nouveau mode d'établissement de relations contractuelles.

Finalement, il faut souligner que la certification permet au consommateur d'obtenir une meilleure information sur les produits et services recherchés en plus des preuves objectives quant au respect de certains standards. En effet, la certification comportera un lot d'informations utiles à l'internaute sur le site consulté.

3.4 Enjeux pour les entreprises

Si les enjeux pour le consommateur peuvent se résumer au concept de « mieux acheter », l'enjeu principal des entreprises est celui de « mieux vendre »⁴¹ et par le fait même de vendre plus.

Cet enjeu se traduira d'abord par le défi de bâtir la confiance des consommateurs pour stimuler son commerce. Il s'agit alors d'exigences nouvelles puisqu'on demande des preuves factuelles de la qualité dans un milieu qualifié souvent de virtuel. C'est là que la certification peut s'avérer d'une aide appréciable, en apportant au consommateur une source d'information extérieure à l'entreprise même.

Les enjeux pour les entreprises ne se limitent pas là. La certification ouvre de nouvelles avenues aux entreprises. En plus de bâtir la confiance du consommateur, les entreprises ou les secteurs d'activité les plus dynamiques pourront y voir une forme d'autoréglementation en établissant leurs propres standards⁴². Il s'agit alors de démontrer la capacité d'une industrie à s'autoréglementer et ainsi éviter l'intervention étatique⁴³.

De plus, ces standards pourront ainsi être développés et même appartenir aux entreprises d'un secteur donné qui y auront donné naissance. De cette façon, le respect de standards et la certification ouvrent également la voie à de nouveaux marchés pour les entreprises. Les plus agressives voudront conserver la propriété des standards développés pour se conférer un avantage commercial sur leurs

⁴¹ Alain Couret, Jacques Igalens et Hervé Penan, *La Certification*, Presses Universitaires de France, Paris, 1995, Collection Que sais-je ?, numéro 3006.

⁴² « A closely related objective of most programs is the political one of preventing or assuaging public concerns that might lead government to regulate the field or to regulate it more aggressively. », Clark C. Havighurst, « *The Place Of Private Accrediting Among The Instruments Of Government* » (1994) 57 *Law and Contemporary problems*, 1, à la page 3. Pour une discussion de la question de l'autoréglementation dans le Cyberspace, voir : Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, aux pages 3-34 et suivantes.

⁴³ L'autoréglementation du commerce électronique semble chère au monde des affaires. On va même jusqu'à affirmer que celle-ci est de nature à conforter la confiance des consommateurs. Michel Dolbec, « Vibrant plaidoyer de Jean Monty en faveur de l'autoréglementation du commerce électronique », *La Presse*, Montréal, 14 septembre 1999, à la page C3. En revanche, les consommateurs recherchent certaines garanties de l'État. Marie-Andrée Amiot, « Les magasiniers internautes québécois veulent la protection de l'État », *La Presse*, Montréal, 14 septembre 1999, à la page C3.

concurrents. Cela leur sera possible dans la mesure où le standard développé aura une reconnaissance universelle.

On constate que l'enjeu pour les entreprises de stimuler son commerce ne se limite pas simplement à gagner la confiance du consommateur, mais peut même lui permettre de s'autoréglementer et de s'approprier des parts de marché importantes.

3.5 Enjeux pour les autorités publiques

Le commerce électronique avec les consommateurs n'est pas un nouveau type de commerce. Certes, il s'agit d'un nouveau moyen d'effectuer le commerce. De leur côté, les gouvernements ont toujours été intéressés à l'essor du commerce qui stimulera l'économie de l'État. Cet intérêt est manifeste si on en croit les efforts considérables déployés pour favoriser le commerce sur Internet⁴⁴.

C'est ainsi que les autorités gouvernementales canadiennes ne se privent pas pour donner leurs conseils aux internautes et aux commerçants sur Internet. À ce niveau, nous remarquons d'une part des recommandations à l'intention des commerçants pour les inciter à procéder à la certification de leur site Web⁴⁵. De l'autre, les consommateurs sont avisés de rechercher la présence de certificats ou de sceaux de qualité sur les sites commerciaux qu'ils visitent⁴⁶. L'importance de la certification dans le développement du commerce électronique semble établie dans l'esprit du gouvernement.

⁴⁴ Pour une discussion sur le sujet, voir: Organisation de coopération et de développement économique (OCDE), « *Le commerce électronique, opportunités et défis pour le gouvernement* », (1997), France.

⁴⁵ « Une façon de rassurer les clients est de vous faire agréer par une tierce partie digne de foi. On voit apparaître de plus en plus de programmes d'approbation de sites Internet. L'approbation va d'une simple vérification de la présence de votre commerce à l'adresse indiquée, à des services complets de vérification. », Bureau de la consommation, Industrie Canada, « Votre commerce dans Internet, Gagner la confiance des consommateurs » <http://strategis.ic.gc.ca/SSGF/ca01186f.html#Certifying>, (Diffusé le 1999-11-08, Consulté le 1999-11-22).

⁴⁶ « À mesure que croît le commerce dans Internet, certains organismes commencent à offrir des cotes de confiance aux commerces en direct et à les agréer. Les programmes d'approbation vont de la simple vérification de l'adresse où prétend se situer l'entreprise et peuvent aller jusqu'à des services de vérification exhaustifs. Visitez le site Web de l'organisme pour voir ce qui est garanti ou ce que signifie vraiment le certificat d'approbation. », Industrie Canada, « Magasiner dans Internet, Renseignez-vous », <http://strategis.ic.gc.ca/SSGF/ca01187f.html>, (Diffusé le 1999-11-08, Consulté le 1999-11-22).

Mis à part l'enjeu du développement du commerce, il faut garder à l'esprit que la certification demeure fondamentalement un outil de contrôle. Cet instrument est d'ailleurs abondamment utilisé par le gouvernement aux États-Unis où le rôle du certificateur est fréquemment joué par des organismes privés⁴⁷.

Dans le cas du réseau Internet, malgré le fait qu'il s'agisse d'un réseau ouvert, il n'en demeure pas moins que l'élaboration de standards et l'instauration de la certification constituent un mode de contrôle de ce nouveau moyen de commercer, et ce, même si ce rôle de certificateur est rempli par des organismes privés. Actuellement, les autorités publiques affirment ne pas vouloir réglementer Internet⁴⁸. Nul n'ignore toutefois que cette position est dictée par la difficulté de mettre en place une réglementation efficace doublée du désir de ne pas nuire au développement du commerce sur Internet.

Néanmoins, la mise en place d'un mécanisme de certification, indépendamment du fait qu'il provienne du secteur public ou privé, constitue un premier pas en matière de contrôle du commerce sur Internet qui pourra mener, éventuellement, vers une certaine réglementation. Lorsque les moyens d'intervention seront plus accessibles, il y a tout lieu de croire que les gouvernements ne résisteront pas à l'attrait de dicter leurs règles dans ce nouvel environnement, surtout en matière fiscale.

Finalement, toujours dans l'optique de contrôle, la certification peut jouer un rôle intéressant en matière de protection du consommateur. Les gouvernements ont certaines responsabilités envers les contribuables à cet égard. Dans un système ouvert tel qu'Internet, la certification peut être un moyen pour les autorités publiques de répondre à cet enjeu.

⁴⁷ Clark C. Havighurst, « *The Place Of Private Accrediting Among The Instruments Of Government* » (1994) 57 *Law and Contemporary problems*, 1.

⁴⁸ Par exemple, le Conseil de la Radiodiffusion et des Télécommunications du Canada a annoncé en mai dernier son intention de ne pas intervenir à ce stade. Voir : « Le CRTC ne réglementera pas Internet », communiqué de presse du 17 mai 1999 (Consulté le 20 mai 1999).

Jusqu'à ce jour, la certification des sites Web sur Internet est une activité prise en charge par le secteur privé. Néanmoins, la certification intéresse l'État puisqu'elle comporte des enjeux importants pour les autorités gouvernementales, que ce soit en rapport au développement du commerce sur Internet, au contrôle de celui-ci et à la protection des consommateurs.

En conséquence, la tentation de faire de la certification des sites Web un acte public supervisé par l'État se manifesterait peut-être. Dans un tel cas, celle-ci se heurterait sans doute à la structure internationale du réseau et aux organismes déjà en place. Il nous apparaît toutefois qu'à ce stade, l'enjeu demeure de stimuler la croissance du commerce.

B. Dimension juridique de la certification

L'implantation d'un site Web de nature commerciale et plus encore, s'il se situe dans le créneau transactionnel, expose l'entité concernée à de nombreux risques de nature légale, notamment en raison du fait qu'Internet procure une exposition instantanée et internationale au site⁴⁹. C'est d'ailleurs l'argument soulevé fréquemment par les firmes d'avocats pour justifier leur intervention en ce domaine⁵⁰.

En réalité, bien avant de parler de certification, la plupart de ces éléments devraient, à notre avis, avoir été pris en considération au moment de développer le site. La plupart de ceux-ci pourront d'ailleurs se retrouver dans le contrat de développement du site Web, lequel aura avantage à adresser la plupart de ces éléments⁵¹.

Au stade de la certification, l'attention sera portée à l'évaluation de certains ou de l'ensemble de ces éléments, selon le type de certification qui sera en cause. La

⁴⁹ John Angel, « *Legal risks of providing services on the Internet* », (1996) *Communications Law*, vol. 1, n°3, 1996, p. 105.

⁵⁰ Voir à ce sujet : <http://www.legalsitecheck.com>.

⁵¹ Voir à ce sujet : Michael D. Scott, « *Website development agreement* », <http://www.perkinscoie.com/webrelease/webdevagmt.htm> ; Valérie Sédallian, « *Création d'un site sur Internet : Aspects juridiques* », <http://62.161.196.163/ij/sitejuridique.html>; l'article Build a safer Website, <http://www.netlaw.com/safer>.

dimension juridique du fonctionnement d'un site Web est très importante, bien plus que le consommateur ne le soupçonne. En conséquence, la certification devrait couvrir ces divers points qui chevauchent des éléments techniques.

Nous avons classé les éléments de nature juridique de la certification des sites Web en quatre grandes catégories. La première concerne l'entité qui demande la certification au niveau de son existence, de sa capacité et de la juridiction qui lui est applicable. La seconde catégorie vise le contenu et le mécanisme de fonctionnement du site Web, à l'exclusion des objets qui touchent directement aux biens et services offerts qui, quant à eux, font l'objet d'une troisième catégorie. Enfin, la dernière catégorie regroupe les facteurs affectant directement les transactions en ligne.

1. L'entité certifiée

Il est utile de se rappeler que l'entité concernée est au centre du mécanisme de certification. C'est elle qui en effectue la demande et si une première étape doit être franchie, c'est d'abord et avant tout de permettre de mieux la connaître et de mieux la cerner.

1.1 Existence de l'entité

Le problème de l'existence même d'une entreprise prend tout son sens dans le monde virtuel. En effet, mis à part une reconnaissance universelle dont jouissent certaines entreprises majeures, l'internaute ne peut se permettre de présumer de la réalité de ce qu'on lui affiche.

C'est d'ailleurs cet élément qui a amené la première vague d'entreprises de certification spécialisées dans l'identité des intervenants et l'authentification des

transactions sur le Web. Dès lors, il était question du rôle des autorités de certification de bâtir la confiance dans le commerce électronique⁵².

Depuis, celles-ci se sont multipliées à un rythme effarant, et ce, dans un grand nombre de juridictions⁵³. Ce premier élément, fondamental en soi, a pour simple mission de permettre à l'internaute de connaître l'identité d'une entreprise réelle qui se trouve derrière la réalité virtuelle du site Web.

1.2 Capacité de contracter

Cette question est sans objet en regard de la plupart des sites que l'on retrouve sur le réseau Internet. En revanche, elle revêt une importance de premier plan dans la perspective de transactions.

Dans le cadre de transactions commerciales, la capacité de contracter de son partenaire est habituellement présumée. Sur Internet, une telle attitude devient particulièrement risquée. C'est l'exemple du mineur qui vient automatiquement à l'esprit lorsqu'il est question de capacité à contracter. Or, de nombreuses autres restrictions peuvent exister en matière de capacité à contracter. Les risques se situent à plusieurs autres niveaux.

Les technologies de l'information facilitent les communications et, en ce sens, favorisent les rapprochements. Néanmoins, elles ne pallient pas l'absence de contact physique qui rend l'évaluation de la capacité de l'interlocuteur plus difficile et donc le risque plus réel.

Par ailleurs, comme le commerce prend une dimension internationale sur Internet, la capacité de contracter peut facilement être affectée par la législation nationale d'une entreprise. Car, si les règles relatives à la protection des mineurs et des majeurs

⁵² Jimmy Lewis, « *Certifying Authorities Must Build Trust* », PC Week, 29 juin 1998, vol. 15, n° 26, page 107.

inaptes ne s'appliquent pas aux personnes morales, des restrictions de nature territoriale, soit la prohibition de commerce entre certains états ou encore des restrictions de nature réglementaire peuvent être en cause. Notamment, dans les secteurs d'activité très réglementés, l'obtention de permis préalables peut poser des difficultés.

La vérification de la capacité de l'interlocuteur et des limites à celle-ci s'il y a lieu sont par conséquent un élément important à certifier.

1.3 Droit et juridiction applicable

Voilà un élément qui suscite de nombreuses interrogations chez les internautes. À quelle juridiction le site est-il soumis ? Lors d'une transaction, quel est le droit applicable ? Et en cas de litige, quel tribunal sera compétent pour entendre les parties et rendre une décision exécutable ?

Ces questions sont fondamentales pour le visiteur d'un site car si le droit applicable et la juridiction diffèrent de ceux du consommateur, il pourra en pratique être dans l'impossibilité de faire valoir ses droits s'il s'estime lésé ou détenir un recours simplement illusoire en raison des coûts de celui-ci par rapport à la valeur de la transaction.

Or, s'il est vrai de dire qu'Internet abolit les distances et supprime les frontières, en revanche, il constitue un irritant important à la question de juridiction applicable. En effet, il est très difficile, et parfois même impossible pour un visiteur de déterminer celle-ci⁵⁴.

⁵³ Annexe A (liste des autorités de certification).

⁵⁴ Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, à la page 4-33.

Sans aller jusqu'à prétendre qu'aucune juridiction n'est applicable⁵⁵, nous devons néanmoins constater qu'il existera fréquemment des conflits de juridiction entre les intervenants.

« En tout état de cause, l'application des principes de rattachement dans le contexte des environnements électroniques semble davantage destinée à faire apparaître une certaine concurrence de revendication de juridiction, plutôt que d'enrayer ce mécanisme de revendication. Ainsi, la question des conflits de juridiction doit-elle être analysée. »⁵⁶

En cas de litige, chaque partie désirera voir le problème traité sur son territoire et selon ses règles. C'est, dans l'esprit de plusieurs, la meilleure assurance d'obtenir satisfaction. À tout le moins est-ce essentiel pour maintenir les coûts à un niveau acceptable. Il est donc important que cette question soit réglée lors du premier contact.

À ce niveau, il nous semble que la meilleure avenue soit la détermination de la juridiction applicable par contrat, avant ou au moment de la transaction⁵⁷. La certification des aspects juridiques pourra aborder cet aspect de la détermination de la juridiction.

⁵⁵ Certains auteurs vont même jusqu'à qualifier Internet de milieu « sans juridiction ». David G. Post, « *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace* », 1995 Journal Online L. article 3.

⁵⁶ Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, à la page 4-35.

⁵⁷ « La possibilité pour les individus de déterminer, dans un contrat, la juridiction compétente à régler leurs litiges et les normes de fond qui régiront leurs rapports présente de nombreux avantages, par rapport aux mécanismes traditionnels de règlement des différends, lorsque des conflits se développent dans les espaces électroniques. [...] Devant les problèmes de juridiction soulevés par les environnements électroniques, le contrat semble être une panacée. », Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, à la page 4-53.

2. Les éléments constitutifs et le fonctionnement du site Web

Il s'agit ici essentiellement d'éléments de nature juridique qui devraient normalement faire l'objet d'une étude préalable et d'une attention particulière lors de la création du site. Une entente claire à ce sujet est de mise⁵⁸.

La création d'un site Web commercial est souvent confiée à des experts. Il s'agit de firmes informatiques spécialisées ou encore ayant développé une expertise dans ce type de développement informatique. Ainsi, la plupart des éléments couverts sont habituellement des éléments de nature technique. Toutefois, de nombreux éléments des sites Web ont une incidence juridique importante⁵⁹.

Ainsi, même s'il est vrai que la création et le fonctionnement d'un site relèvent d'abord du domaine technique, les réalités légales ne doivent pas pour autant être oubliées. Les entreprises ont intérêt à veiller aux aspects légaux dès le début des démarches de création du site pour les guider lors de décisions importantes, notamment au niveau du choix d'un nom de domaine, des normes applicables en termes de sécurité du site et de protection des renseignements personnels, relativement aux liens et aux règles d'utilisation du site⁶⁰.

2.1 Noms de domaine

Les noms de domaine ont déjà engendré un nombre impressionnant de conflits. L'origine de ces conflits est le fait que les noms de domaines sont un concept juridique différent de celui des marques de commerce. Ils ne sont donc pas réglementés de la même manière malgré le fait qu'ils soient appelés à cohabiter

⁵⁸ Michael D. Scott, « *Website development agreement* », <http://www.perkinscoie.com/webrelease/webdevagmt.htm> (Dernière modification le 15 juin 1999, consulté le 14 août 1999).

⁵⁹ Carole A. Kunze, « *Website Legal Issues* », (1998), *Santa Clara Computer and High Technology Law Journal*, vol. 14, p. 477.

⁶⁰ Valérie Sédallian, « *Création d'un site sur Internet : Aspects juridiques* », <http://62.161.196.163/lij/sitejuridique.html> (décembre 1998).

souvent avec les marques de commerce. Précisons d'abord ce qu'est un nom de domaine.

Chaque site Web occupe un espace différent sur Internet. On appelle cet espace un domaine. Chaque domaine a une adresse spécifique⁶¹. Le nom de domaine est une composante de l'adresse pour en faciliter le repérage.

Or, les marques de commerce et dénominations sociales d'entreprise sont fréquemment reprises ou intégrées dans le second niveau des noms de domaine.

En effet, la cohabitation des marques de commerce et des noms de domaine est difficile puisque plusieurs entités peuvent détenir la même marque de commerce dans le monde, ce qui crée des conflits lors de l'utilisation de cette marque dans le second niveau des noms de domaine. Cette problématique a d'ailleurs fait l'objet de nombreuses études légales⁶².

Il nous apparaît donc opportun que le nom de domaine utilisé par l'entité fasse l'objet d'une vérification pour démontrer, à tout le moins, qu'il n'entre pas en conflit avec une marque de commerce existante.

2.2 Sécurité du site

La question de la sécurité est un élément crucial pour accroître la confiance des consommateurs⁶³. La simple idée qu'un intrus puisse réussir à s'introduire sur un site pour y voler ou modifier de l'information est de nature à affoler les consommateurs potentiels⁶⁴.

⁶¹ Communément appelée « U.R.L. » (Uniform Resource Locator).

⁶² Annexe B (bibliographie sur noms de domaine).

⁶³ Stéphane Lefer, « *Sécurité et confiance : maître mot du commerce électronique* », Lamy Droit de l'informatique, janvier 1998, n° 1999, à la page 1.

⁶⁴ Ce fut par exemple le cas du site d'Air Canada où un individu a pu avoir accès à la liste des membres du programme Aéroplan. Les conséquences peuvent être très néfastes pour une entreprise. On cherche alors à effacer toute trace de cet événement. (<http://www.aircanada.ca/francais/aeroplan>).

Cette inquiétude, légitime en soi, prend des proportions importantes dans un environnement ouvert tel que Internet. Le nombre de piratages⁶⁵, tenté ou réussi, a suivi la croissance du commerce électronique. De plus, la sensibilité du public fait en sorte qu'ils font l'objet d'une couverture médiatique accrue. La question de la sécurité constitue dès lors l'une des préoccupations incontournables de l'entreprise qui désire assurer sa présence à long terme sur Internet⁶⁶.

Bien entendu, les normes de sécurité devront être proportionnées à la nature de l'activité commerciale exercée par l'entreprise. Par exemple, une entreprise oeuvrant dans le milieu financier et désirant effectuer des transactions financières importantes sur Internet devra soumettre son site à des normes de sécurité du plus haut niveau.

En revanche, l'entreprise dont les activités se limitent à l'échange de renseignements ou à des transactions de faible valeur pourra répondre à des normes moins strictes. Toutefois, peu importe le montant des transactions, certaines normes devront être adoptées et respectées puisque le dommage potentiel ne se limite pas à l'interception du message, mais également à l'usage de l'information appropriée, lequel peut être important indépendamment du montant de la transaction.

Les solutions en matière de sécurité des sites Web sont essentiellement techniques. Elles devront néanmoins être examinées sous l'aspect juridique. De plus, la sécurité d'un site nous apparaît comme l'un des premiers éléments qui devrait faire l'objet d'une certification. Par ailleurs, cette question ne se limite pas à l'aspect strictement « Internet », mais également à tout le processus d'affaires de l'entreprise. En effet, il ne sert à rien de placer une porte blindée sur un mur de bois...

⁶⁵ Communément appelé par le biais de leur expression anglaise « hacking ».

⁶⁶ Pour illustrer cette importance, soulignons que dans un ouvrage récent dédié à l'établissement de la présence d'une entreprise sur Internet, la préoccupation de sécurité constitue un thème de chacun des seize chapitres: Martin A. Schulman, Rick Smith, *The Internet Strategic Plan, A Step-by Step Guide to Connecting Your Company*, Wiley Computer Publishing, (1997), États-Unis.

2.3 Les liens

Un des grands attraits du Web est le fait de permettre aux internautes de naviguer d'un site à l'autre. Cette navigation s'effectue au moyen d'hyperliens. Avec le temps, diverses techniques sont apparues sur les sites Internet.

Si les hyperliens posent peu de difficultés aux organismes sans but lucratif, il en est tout autrement pour les sites Web de nature commerciale. En effet, une entité aura avantage à s'assurer d'une autorisation, expresse ou tacite, avant de poser un hyperlien sur son site.

La destination du lien de même que la façon dont il fonctionne peut donner lieu à des différends. Ainsi, les liens approfondis⁶⁷ qui court-circuitent la page d'accueil du site destinataire ont déjà été la source de divers litiges⁶⁸.

Dans la même lignée, certains sites recourent à la technique du cadrage⁶⁹ pour garder leur clientèle captive. Cette méthode permet à un internaute d'utiliser un hyperlien sans quitter le site où il se trouve.⁷⁰

Finalement, il faut être prudent quant à l'utilisation d'une image, un logo ou une marque de commerce comme hyperlien qui peuvent également donner naissance à des conséquences légales non désirées⁷¹.

⁶⁷ Cette méthode appelée en anglais « deep linking » a fait naître certains litiges en raison du fait que l'internaute navigant au moyen de ces liens se retrouve projeté « profondément » dans le site où mène le lien, court-circuitant de ce fait la page d'accueil et la publicité qui s'y trouvent qui peut donner lieu à un dommage économique au site destinataire.

⁶⁸ Citons notamment les célèbres affaires de *Shetland Times Ltd. v. Dr Jonathan Wills and Zetnews Ltd.*, (Lord Hamilton, J., Court of Sessions, Edinbourg, Écosse, 1996-10-24 et *Ticketmaster Corporation v. Microsoft Corporation*, Civ. 97-3055 DDP, Californie, 1997-04-12.

⁶⁹ Cette autre méthode, appelée en anglais « framing », est encore plus contestée du fait qu'elle a pour conséquence de donner l'impression à l'internaute qu'il est toujours sur le site original ou encore que les deux sites n'en forment qu'un.

⁷⁰ Dans une décision récente portant sur cette question, la Cour fédérale du Canada a octroyé une injonction pour faire cesser ce genre d'utilisation des hyperliens puisqu'elle estimait que l'utilisation porte l'internaute à croire que l'information présentée fait partie du même site. Voir : *Imax Corp. v. Showmax Inc.*, Cour fédérale, le 18 janvier 2000, disponible à : <http://www.fja.gc.ca/en/cf/2000/orig/html/2000fca25888.o.en.html>

⁷¹ Alan Gahtan, Martin P.J. Kratz, J. Fraser Mann, *Internet Law, A Practical Guide For Legal And Business Professional*, 1998, Carswell, Canada, à la page 209.

Dans tous ces cas, il y a la problématique du consentement de l'entité vers laquelle pointe le lien mais également un site commercial devrait être sensible à la responsabilité qu'il peut encourir du fait de donner l'impression que cette information provient de son site ou simplement pour y avoir donné accès.

2.4 Les clauses légales et règles d'utilisation du site

Tous les sites sur Internet ont avantage à disposer d'une section, plus ou moins élaborée selon le cas, dans laquelle les règles d'utilisation du site sont clairement énoncées. Dans certains cas, comme pour les sites Web commerciaux, des clauses légales plus complexes pourront venir s'y ajouter.

Il est encore étonnant de constater le nombre de sites Web de nature commerciale qui ne disposent d'aucune section de ce genre. Il s'agit pourtant là d'un élément de base dont l'entreprise devrait se munir et auquel les nouveaux visiteurs devraient automatiquement avoir accès.

Or, cette section doit être rédigée en termes compréhensibles et accessibles par l'internaute, où qu'il se trouve sur le site. C'est à cet endroit qu'on informera l'internaute des règles générales que l'entité entend voir appliquées dans le cadre de l'utilisation du site⁷².

L'essentiel de la participation des conseillers juridiques à la création d'un site est souvent concentré à cet endroit. De plus, les notes légales se limitent souvent au thème de l'exclusion de la responsabilité alors qu'elles pourraient informer davantage l'internaute.

⁷² Pour une étude de cette question de même que des modèles de notes légales, voir : Gahtan, Alan, Kratz, Martin P.J., Mann, J. Fraser, *Internet Law, A Practical Guide For Legal And Business Professional*, 1998, Carswell, Canada, à la page 87.

À défaut d'être rédigée par des conseillers juridiques, cette section du site devrait faire l'objet d'une vérification légale et, idéalement, faire partie de la certification du site.

3. Les biens et services offerts

Un site Web commercial se caractérisera par le fait d'aller au-delà de l'information et d'offrir également des biens et/ou services.

3.1 Information sur le site

L'objectif ultime de l'entreprise est d'effectuer des transactions. Toutefois, cet objectif sera toujours précédé d'une étape préliminaire de contact avec l'internaute, qui sera de nature informative.

Ce premier contact est très important pour la suite des événements. C'est là que la première impression se forge. Le premier contact étant une étape nécessaire, les commerçants ont entrepris de la rentabiliser.

Les entreprises sont en effet conscientes de la possibilité d'offrir directement au consommateur non seulement des biens, mais également une information précise et quasi globale sur ses biens et services sans avoir à supporter une large équipe de service à la clientèle. Le client peut désormais chercher son information de façon autonome. Ainsi, on retrouve une foule d'informations sur les sites Web de nature commerciale.

L'information sur le site devra néanmoins faire l'objet de vérifications et de mises à jour constantes. L'entité aura notamment avantage à indiquer le caractère temporaire de ces informations et le fait que celles-ci peuvent être modifiées en tout temps.

Par ailleurs, l'information que l'on retrouve sur les sites ne provient pas nécessairement de l'entreprise elle-même. Il peut s'agir d'informations recueillies ou même achetées auprès de partenaires spécialisés dans la communication et la distribution d'informations. En théorie, une entreprise ne devrait pas être responsable d'information dont elle n'est pas l'auteur. Toutefois, en devenant le messager, elle se place dans une situation qui pourrait lui causer des difficultés.

L'entreprise doit donc être prudente lorsqu'elle affiche sur son site une information dont elle n'est pas l'auteur. C'est d'abord et avant tout dans le contrat entre la source de l'information et l'entreprise que se retrouvera la protection dont l'entreprise a besoin, à savoir une clause selon laquelle la source de l'information se tient responsable et s'engage à tenir son partenaire indemne de toute réclamation en rapport avec celle-ci. Face à l'internaute, l'entreprise aura avantage à indiquer la source de l'information et d'inclure une clause appropriée aux notes légales affichées sur le site.

Dans le cas d'entreprises utilisant fréquemment de l'information provenant de tiers, des normes et des standards relativement à l'information diffusée pourront être élaborés et faire l'objet d'une vérification ultérieure par un tiers. Le rôle du juriste ne serait pas de certifier la qualité de l'information, mais plutôt d'assister l'entreprise dans l'élaboration de ces normes.

3.2 Respect des règles concernant la protection des consommateurs.

Il n'est pas facile d'importer toutes les règles concernant la protection des consommateurs dans le domaine des transactions sur Internet. La qualification fréquente d'Internet comme un « monde sans loi » donne la perception que les règles concernant la protection des consommateurs ne s'y appliquent pas.

Bien que cela soit faux, l'entreprise qui désire bâtir la confiance avec le consommateur devra adopter une attitude proactive pour démontrer le respect de ces règles dans le cadre du commerce sur Internet. La divulgation de ses pratiques commerciales sur le site constitue un bon exemple.

Mieux encore, un programme de certification adéquat de ses pratiques auquel s'ajoute un sceau démontrant la vérification et le respect de celles-ci pourra rassurer les consommateurs.⁷³

3.3 Respect de la propriété intellectuelle

La problématique du respect de la propriété intellectuelle est omniprésente sur Internet⁷⁴. Les sites Web n'y font pas exception. La propriété intellectuelle revêt diverses formes ayant chacune leurs caractéristiques propres. Nous pensons au droit d'auteur, aux marques de commerce, brevets, dessins industriels et topographie.

Au Canada, chacune de ces formes fait l'objet d'une protection en vertu d'une loi distincte⁷⁵. Sur le plan international, de nombreux traités internationaux portent sur les questions de propriété intellectuelle.

La plupart des litiges au niveau des marques de commerce sont en rapport avec l'enregistrement d'un nom de domaine. Toutefois, les risques potentiels ne s'arrêtent pas là.

Pour le droit d'auteur, les violations potentielles sont nombreuses à l'intérieur d'un site. En effet, le droit d'auteur est une question beaucoup plus délicate lorsqu'elle est

⁷³ Au Québec, le gouvernement n'a pas adopté de position claire à ce sujet. Le seul écho des médias fait mention d'un mécanisme de loi d'adhésion. Il s'agirait d'une loi établissant des normes facultatives, lesquelles deviendrait impératives pour les entités y ayant adhéré.

⁷⁴ Jacques Labrèche, « *Inforoute et propriété intellectuelle* », <http://www.robic.ca/publications/1997> (consulté le 1999-11-21) Donald M. Cameron, Tom S. Onyshko, W. David Castell, « *IP on the I-Way* », *Canadian Intellectual Property Review* (1996-1997) 13 C.I.P.R., 311.

mise dans le contexte de l'Internet. Il est important de rappeler que le droit d'auteur sur une oeuvre est défini comme suit dans la loi canadienne:

« Le droit d'auteur sur l'oeuvre comporte le droit exclusif de produire ou reproduire la totalité ou une partie importante de l'oeuvre, sous une forme matérielle quelconque, d'en exécuter ou d'en représenter la totalité ou une partie importante en public et, si l'oeuvre n'est pas publiée, d'en publier la totalité ou une partie importante;

(...) »⁷⁶

(notre soulignement)

Or, au niveau de la reproduction, l'aspect technologique d'Internet pose un défi important étant donné la facilité d'effectuer des copies de presque tout ce qui figure sur le réseau⁷⁷. De plus, la doctrine de l'utilisation équitable n'est pas applicable aux sites commerciaux en raison du but et du type d'utilisation effectuée, soit une utilisation commerciale⁷⁸. Seuls les engins de recherche semblent bénéficier d'une exception à cet égard⁷⁹.

Une certification de nature juridique quant au respect des règles en matière de propriété intellectuelle est un autre élément à considérer. Elle se situe tant au niveau de l'information, des documents que des logiciels disponibles sur le site. Pour l'entreprise, il ne s'agit toutefois pas d'un lourd fardeau supplémentaire, mais davantage de la continuité de l'application de ses normes sur son site Web.

⁷⁵ Voir à ce sujet: *Loi sur les brevets*, L.R.C., chapitre P-4; *Loi sur le droit d'auteur*, L.R.C. chapitre C-42; *Loi sur les marques de commerce*, L.R.C., chapitre T-13; *Loi sur les dessins industriels*, L.R.C. chapitre I-9; *Loi sur les topographies de circuits intégrés*, L.C. 1990, chapitre 37.

⁷⁶ *Loi sur le droit d'auteur*, L.R.C., chapitre C-46, art. 3(1).

⁷⁷ François Painchaud, « *La propriété intellectuelle sur Internet: le policier à cheval et le voleur en formule 1?* » <http://www.robic.ca/publications/179.htm>. (consulté le 1999-11-21).

⁷⁸ Sheldon Burnshtein, « *Surfing the internet : copyright issues in Canada* », *Santa Clara Computer & High Technology Law Journal*, 1997, Volume 13, 385.

⁷⁹ Daniel Ovanezian, « *Internet research Engine Copying : Fair Use Defense to copyright Infringement* », *Computer & High Technology Law Journal*, 1997, Volume 14, 267.

4. Les transactions en ligne

La transaction constitue l'étape ultime du magasinage de l'internaute. Cependant, c'est là où la plupart font demi-tour et rebroussement chemin. L'entreprise qui désire effectuer des transactions commerciales sur Internet doit donc porter une attention particulière à la présentation de cette étape.

Le concept de transaction est pris ici dans son sens large. Il ne se limite pas uniquement à l'achat ou à l'échange d'une somme d'argent, mais comprend toute communication entre l'internaute et le site Web.

Ces besoins sont traités ensemble en raison du fait qu'ils font appel au concept d'infrastructure à clé publique⁸⁰.

4.1 Intégrité de la communication

Dans la continuité de la notion de sécurité abordée précédemment, nous nous penchons ici sur la sécurité, non plus au niveau du site, mais au niveau de la communication qui s'établit entre l'entreprise et le consommateur.

Avant d'effectuer une transaction, le client devra être rassuré quant à la sécurité et à l'intégrité de la communication qui s'établit avec le commerçant⁸¹.

⁸⁰ Le chiffrement, une méthode qui permet de préserver la confidentialité des réseaux, des bases de données et des fichiers à l'aide d'algorithmes mathématiques. Le codage obtenu exige une clé secrète. Le destinataire se sert de cette clé pour décoder les caractères et reconstituer le message. Plus la clé compte de chiffres, meilleure est la protection. L'avantage du chiffrement à clé publique réside dans le fait qu'il utilise deux clés algorithmiques : une clé publique pour coder les données et une clé privée pour les décoder.

⁸¹ Mark A. Kellner, « *Net transaction security : a state of mind* », Communication Week, 19 février 1996, n° 597, page 1 à 7.

4.2 La protection des renseignements personnels

La question de la protection des renseignements personnels se situe dans le même girond que les questions de sécurité du site et d'intégrité de la communication. Il s'agit là d'une préoccupation très importante des consommateurs qui constitue jusqu'à un certain point une limite à la liberté de commerce⁸².

Pour les entreprises, elle peut être traitée comme une extension aux échanges sur Internet des normes internes applicables à la protection des renseignements personnels. Dans ce contexte, il s'agit de déterminer quelle est la politique de l'entreprise à ce niveau et quelles sont ses règles relativement à la constitution de dossiers, à la cueillette d'informations ainsi qu'à la conservation de ceux-ci.

Sur Internet, la question de la cueillette et de l'utilisation de renseignements personnels est d'autant plus sensible qu'elle se fait sur support informatique, parfois sans que le consommateur ne s'en aperçoive et permet l'élaboration de profils de consommation⁸³. Le traitement des données transactionnelles doit donc faire l'objet d'une attention particulière.

Étant donné le caractère ouvert et international de l'Internet, on prône également une grande participation du secteur commercial lui-même en matière d'autorégulation. Au Canada, l'Association canadienne de normalisation (C.S.A.) a été en mesure d'élaborer des normes acceptées par des organisations importantes dans le milieu commercial⁸⁴. De même sont apparues des normes sectorielles comme celles adoptées par l'Association des banquiers canadiens (A.B.C.) ou encore l'Association canadienne des compagnies d'assurance de personnes (A.C.C.A.P.).

⁸² Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, à la page 11-42.

⁸³ Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, à la page 11-43 à 11-46.

⁸⁴ Voir: Rapport du groupe de travail sur le commerce électronique, « La protection des renseignements personnels - pour une économie et une société de l'information au Canada » janvier 1998, aux pages 9 et suivantes.

À notre avis, les entreprises canadiennes auront tout avantage à modeler leur pratique sur ces normes⁸⁵ ou, mieux encore, sur celles qui semblent en voie d'être adoptées par le gouvernement fédéral⁸⁶. Celles-ci comportent d'ailleurs de grandes similarités avec la *Loi sur la protection des renseignements personnels dans le secteur privé* adoptée et entrée en vigueur au Québec en 1994⁸⁷. Les entreprises québécoises peuvent donc continuer d'appliquer les règles déjà édictées dans cette loi⁸⁸.

Si l'entrée en vigueur de la *Loi sur la protection des renseignements personnels dans le secteur privé* a créé un certain remous au Québec, on doit néanmoins constater son effet bénéfique sur la protection des droits des consommateurs. En revanche, lorsqu'on parle du réseau Internet, le problème prend immédiatement une dimension internationale. La première constatation est alors le problème de sanction. Or, il est bien connu que ce problème de sanction peut rendre une loi stérile. C'est pourquoi le recours à la certification semble indiqué.

Néanmoins, dans un milieu difficile à régler comme Internet, un mécanisme de certification offre certaines garanties quant au respect de normes déterminées. Or, jusqu'à présent, les organismes de certification ne font qu'exiger l'existence et la publication d'une politique en matière de protection des renseignements personnels sans que son respect ou sa mise en application ne soit abordé⁸⁹.

⁸⁵ Nous partageons l'avis émis par le professeur Trudel à ce sujet dans son ouvrage : Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, à la page 11-70.

⁸⁶ Voir le Projet de loi fédéral C-6, *Loi sur la protection des renseignements personnels et les documents électroniques* (anciennement Projet de loi C-54, *Loi sur la protection des renseignements personnels et documents électroniques*, première session, 36e législature, 46-47 Élisabeth II, 1997-1998). Par ailleurs, le Bureau de la consommation du ministère de l'Industrie recommande aux commerçants le respect de certaines normes non légales développées par divers organismes comme l'explique cet extrait : « Le meilleur exemple à suivre est le Code type sur la protection des renseignements personnels de CSA (Association canadienne de normalisation) », <http://strategis.ic.gc.ca/SSGF/ca01186f.html#Protecting> (Diffusé 1999-11-09, consulté le 1999-11-22).

⁸⁷ *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q. chapitre P39.1.

⁸⁸ Il est à noter que la *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1 a pour objet d'établir des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise (article 1 de la loi). Elle n'exige toutefois pas l'adoption d'une politique d'entreprise en cette matière bien que ce soit fortement recommandable. Soulignons par ailleurs que le projet de loi fédéral devrait s'appliquer à toutes les provinces mais crée une exception pour le Québec qui a déjà mis en place son mécanisme de protection de la vie privée.

⁸⁹ Voir par exemple les exigences en matière de certification de l'organisme TRUSTe et celle du « Privacy Label » de l'organisme BBBOnline, dont les sceaux visent précisément la protection de la vie privée.

4.3 Authentification de l'interlocuteur et communication du consentement

Mais le défi ne se limite pas là. Il faudra de plus que les parties soient en mesure d'authentifier les messages émis comme provenant de l'autre partie. Une partie de la confiance porte sur l'identification et la non-répudiation des actes.

Le cyberspace comporte certaines limites inhérentes à sa forme immatérielle. En revanche, ces contraintes en font un terrain fertile aux nouvelles idées. Les intervenants ne manquent d'ailleurs pas de faire appel à leur imagination lorsque vient le temps de pallier des problèmes physiques, tels l'authentification de l'interlocuteur et l'échange des consentements.

Dans le monde physique, la signature manuscrite joue habituellement ce rôle de marque de consentement. Dans le cyberspace, cette solution n'est toutefois pas envisageable. Bien que la signature manuscrite soit perçue comme le moyen nécessaire de marquer son consentement, il ne s'agit cependant pas de la seule avenue possible.

D'abord, en termes de signature, soulignons que le Code civil énonce une définition large de la signature en ces termes :

« La signature consiste en 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. »⁹⁰

On constate donc que d'autres mécanismes que la signature manuscrite pourront répondre à cette définition. Par ailleurs la signature, indépendamment de sa forme, n'est qu'un moyen de prouver le consentement. Rien n'empêche toutefois le recours à d'autres méthodes.

⁹⁰ Article 2827 du *Code civil du Québec*.

Dès lors, tout moyen démontrant l'identité de la personne et sa volonté à contracter peut être valide. Ainsi, pour une personne, toute autre marque ou geste offrant des garanties suffisantes pourra être considéré à ce titre⁹¹.

Le fait de recourir à une technique différente à la signature manuscrite aura tout de même avantage à bénéficier d'une vérification pour s'assurer que le mécanisme utilisé constitue une manifestation suffisante du consentement. Elle sera de nature à rassurer tant l'entreprise que le consommateur.

4.4 Le mécanisme de paiement

Puisqu'il est question ici des relations entre une entreprise et un consommateur, le paiement dont il est question constitue en fait le versement d'une somme d'argent à l'entreprise⁹².

Certains ont vu dans le paiement électronique une révolution du paiement ou des mécanismes de paiement. Or, le paiement électronique n'est en soi que le résultat inéluctable d'une évolution technologique constante, laquelle s'est accentuée au cours des dernières années dans le cadre de la croissance explosive du réseau Internet. Néanmoins, il faut garder à l'esprit qu'aucun des mécanismes de paiement traditionnels, qui comportent chacun leur lot de particularités, n'est parfaitement adapté à une utilisation dans l'environnement du cyberspace.

Pris dans son sens large, le paiement électronique fait partie de notre vie quotidienne depuis de nombreuses années déjà. Dans son sens restrictif, il fait une apparition qui

⁹¹ Pour une étude plus détaillée de la question, voir : Pierre Trudel, Guy Lefebvre et Serge Parisien, *La preuve et la signature dans l'échange de documents informatisés au Québec*, Québec, Les Publications du Québec, 1993. En droit américain, voir: Henry H. Perritt, *Law and the Information Super Highway*, (1996), Wiley Law Publications, John Wiley & Sons inc., États-Unis.

⁹² Le *Code civil du Québec* comporte quant à lui une définition de l'obligation à son article 1553 qui se lit comme suit: « Par paiement on entend non seulement le versement d'une somme d'argent pour acquitter une obligation, mais aussi l'exécution même de ce qui est l'objet de l'obligation. »

engendre la naissance de divers mécanismes de paiement sur Internet. En effet, bien qu'elles doivent être prises avec une certaine réserve, les données et projections statistiques recueillies auprès de divers organismes prévoient unanimement une progression très importante du commerce électronique et, de façon incidente, du paiement sur Internet⁹³.

Deux grandes catégories de mécanismes de paiement doivent être distinguées. La première se base sur l'utilisation et l'adaptation des techniques actuelles de paiement au réseau Internet. Ainsi, certains systèmes proposent un paiement par carte de crédit, par chèque électronique ou encore par virement de fonds. En raison des particularités d'Internet, certains de ces systèmes ont recours à un intermédiaire. Ce dernier aura toujours pour rôle de répondre à la question de sécurité de la transaction. La seconde catégorie vise les nouveaux mécanismes de paiement. Certains systèmes proposent la création de nouveaux mécanismes de paiement proprement électronique, mais qui ne seront pas nécessairement uniques à Internet. Ces systèmes ont recours à ce qu'il convient de qualifier de monnaie électronique. Ce système a principalement l'avantage (ou le désavantage) d'assurer la confidentialité de l'identité de la personne effectuant la transaction.

Il ne faut toutefois pas confondre commerce et paiement malgré l'étroite association qui existe entre ces deux notions. En effet, on constate que moins de la moitié des personnes ayant placé une commande sur Internet effectuent systématiquement le paiement de ce produit sur le réseau. Cette proportion a néanmoins tendance à augmenter et il y a tout lieu de croire que cette tendance se maintiendra au fur et à mesure que la confiance des consommateurs s'établira⁹⁴.

Les perspectives à moyen terme sont à l'apparition d'une certaine standardisation des mécanismes de paiement sur Internet. De façon inhérente, le commerce qui s'y fait est de nature internationale. Ainsi, la préoccupation d'une acceptation globale par les

⁹³ Les projections quantitatives relativement au chiffre des affaires transigées sur Internet en l'an 2002 varient de 268 milliards à un trillion. (Newsbite: 268 milliards, Infoworld: 333 milliards, CNN: 400 milliards et TechServer: un trillion).

commerçants revêt un aspect essentiel pour les consommateurs. Déjà, on assiste à la disparition de divers joueurs en faveur des plus grosses organisations que favorise le libéralisme économique sur ce réseau.

Le consommateur y trouve actuellement son compte par la recherche de la suppression des intermédiaires commerciaux. Simplification et accélération du processus de paiement sont à l'ordre du jour. La sécurité est somme toute bien assurée par tous les mécanismes proposés. Néanmoins, le consommateur n'en est pas nécessairement informé lorsqu'il fait affaires avec ce dernier. Il faut d'abord que les normes soient étendues à tous et connues du public pour obtenir l'effet escompté.

Avec à l'esprit le fait que le véritable défi du commerce électronique est d'acquérir la confiance des consommateurs, on ne peut que conclure que la confiance en matière de transaction électronique transite d'abord avec le mécanisme de paiement. Avant de s'aventurer sur ce terrain, le consommateur désirera se faire rassurer quant aux mécanismes employés⁹⁵.

La certification au niveau du mécanisme de paiement vise à informer et donner cette confiance au consommateur pour qu'il puisse conclure une transaction. L'objet de la certification devra donc couvrir les aspects de sécurité du mécanisme (intégrité de la communication et protection des renseignements transmis) autant que l'effet libérateur du paiement.

Il ne s'agit là que d'un bref survol et d'une liste non exhaustive des divers éléments pouvant faire l'objet de la certification juridique des sites Web commerciaux.

⁹⁵ Voir à ce sujet : Bernard Brun, « Les mécanismes de paiement sur Internet », Juriscom.net, 20 octobre 1999, <http://www.juriscom.net/universite/doctrine/article5.htm> ; Roger Clarke, « Introduction to Electronic Payment Mechanisms », Australian National University, 24 mai 1998, <http://www.anu.edu.au/people/Roger.Clarke/EC/EPMIntro.html> ; Andreas Furche, Graham Wrigton, *Computer Money: A Systematic Overview of Electronic Payment Systems*, Les Éditions Morgan-Kaufman, 1997 ; Alain Plamondon, « Le paiement électronique sur Internet, Recensement et analyse », Août 1996, <http://www.rambit.qc.ca/plamondon/ecashind.htm> ; Greg TUCKER, « Electronic Payment system », Law Institute Journal, janvier 1997 ; David WARD, « Electronic Payment Systems for the Internet », 11-03-1996, http://members.ecom.net/~davidward/eps/elec_pay.html.

Plusieurs d'entre eux se chevauchent et chacun peut susciter des difficultés considérables à l'entreprise qui n'y prend garde.

De plus, discuter de certification dans le domaine juridique suscite un questionnement évident. En effet, si l'activité juridique se situe parfois dans le champ de la prévention, l'emploi du terme certification en fera sursauter plus d'un. Sa connotation d'assurance et même de garantie va à l'encontre de la conception d'opinion et d'obligation de moyen du conseiller juridique. De plus, le droit n'étant pas une science exacte, qui pourrait donc s'aventurer dans un processus de certification de nature juridique ?

Par ailleurs, l'opinion rendue par le conseiller juridique est habituellement conçue pour un usage privé par le client. Au contraire, la certification se destine directement au tiers et, par conséquent, à un usage externe. En effet, le but n'est pas de rassurer l'entreprise, mais le consommateur qui veut effectuer des transactions sur Internet.

Malgré ces inquiétudes, nous sommes d'avis que la dimension juridique d'un site Web peut faire l'objet d'une certification. Le concept de certification doit être distingué de celui de garantie⁹⁶. Le champ et la portée de celui-ci devront être clairement établis.

Les dimensions juridiques du fonctionnement d'un site Web sont nombreuses et se situent au centre des préoccupations des internautes. Pour qu'une certification soit d'une utilité quelconque aux visiteurs d'un site, celle-ci doit couvrir les aspects essentiels de son fonctionnement⁹⁷, y compris les aspects juridiques.

⁹⁶ « It must not be thought that a product can be subjected to some mechanistic process of evaluation which will then be transformed into an unconditional guarantee against every eventuality. » Andrew K. Rae, Hans-Ludwig Hausen, Philippe Robert, *Software Evaluation for Certification, Principles, Practice and Legal Liability*, (1995), McGraw Hill Book Company, England.

⁹⁷ « To be of any real value, the evaluation and certification of a product needs to cover all the essential attributes which make the product satisfying its specified requirements and fitness for purpose in an operational environment. », Andrew K. Rae, Hans-Ludwig Hausen, Philippe Robert, *Software Evaluation for Certification, Principles, Practice and Legal Liability*, (1995), McGraw Hill Book Company, England, page 4.

Or, seuls les juristes sont en position de rendre un avis quant au respect de ces aspects⁹⁸. Le rôle de ceux-ci aura donc avantage à être revu pour faire face à ce nouveau besoin. Les éléments techniques étant également omniprésents, le modèle de certification idéal se verrait comme une certification plus globale dont les aspects juridiques feront partie intégrante.

⁹⁸ Il est à noter que plusieurs autres professions s'immiscent dans l'évaluation d'éléments spécifiques au domaine juridique. La justification vient du fait qu'elles affirment que l'auditeur n'agit pas comme un expert du domaine, mais uniquement pour évaluer si les risques sont maîtrisés. Nous ne partageons pas cette opinion et à notre avis, un tel travail est du ressort des experts en ce domaine, soit les juristes. Voir à ce sujet : Etienne, Barbier *L'audit interne, permanence et actualité*, (1996), 3^e Edition, Les Éditions d'Organisation, France, pages 43-44.

Partie II – Processus et impacts juridiques

Nous nous attarderons ici davantage au processus de la certification, c'est-à-dire aux diverses étapes à franchir pour en arriver finalement à la certification d'un site. Nous étudierons par la suite les impacts de cette certification sur les diverses parties en présence.

A. Le processus de certification

Le processus de certification se divise en trois grandes étapes, soit : l'établissement de standards, l'évaluation de l'entité et finalement la décision d'accorder ou non la certification⁹⁹.

Le point de départ du processus est la demande de certification déposée par une entité et l'identification précise de son objet. La demande de la part du candidat doit comporter un certain nombre de renseignements, notamment quant à la portée recherchée de la certification.

Il est important de garder à l'esprit qu'une certification n'est rien d'autre qu'une déclaration de conformité en rapport à des paramètres déterminés. Ainsi, une certification pourra se limiter à la dimension sécuritaire d'un site tout comme certaines certifications existantes visent les questions de confidentialité. De même, nous pourrions entrevoir la possibilité d'une certification de la dimension juridique du fonctionnement d'un site Web.

⁹⁹ Il s'agit là d'étapes purement procédurales et générales. Sur le plan technique, les étapes sont plus nombreuses comme le rapporte : Jonathan T. Howe et Leland J. Badger, « *The Antitrust Challenge To Non-Profit Certification Organizations : Conflicts of Interest and a Practical Rule of Reason Approach to Certification Programs as Industry-Wide Builders of Competition and Efficiency* », (1982) 60 Washington University Law Quarterly 357, à la page 364. Voir également : Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberespace*, Montréal, Les Éditions Thémis, 1997, à la page 3-46.

1. L'établissement de standards

L'établissement de standards joue un rôle primordial dans la certification. En fait, il faut garder à l'esprit que la certification est le complément de l'élaboration et la mise en place de standards. Ce sont par ailleurs ces standards qui déterminent le niveau et la portée de la certification.

1.1 Rôle et évolution des standards

La nécessité de régir, soit officiellement soit officieusement, un secteur d'activité engendre l'apparition de standards. L'ouverture et l'élargissement des marchés apportent de plus le besoin d'assurer les comparaisons et l'interchangeabilité entre les produits et les services.

Les premiers éléments à avoir attiré l'attention à ce niveau se rattachaient, soit à des préoccupations de santé ou encore de sécurité¹⁰⁰. Il s'agissait alors davantage de qualité que de compatibilité. Toutefois, si le standard de qualité diffère en nature de celui portant sur la compatibilité, dans les faits, ceux-ci se fondront fréquemment en une seule norme. Ceci est particulièrement le cas dans le domaine de l'informatique et des technologies de l'information¹⁰¹.

Aujourd'hui, la standardisation est vue d'abord et avant tout comme un élément essentiel pour assurer la survie d'une entreprise dans un marché ouvert. En effet, des concepts comme compatibilité et intercommunication prennent alors une importance majeure¹⁰².

¹⁰⁰ Geneviève Iacono, « *La certification d'assurance qualité : De nouvelles questions pour le Droit ?* », (1994) *Revue Internationale de Droit Économique* 63, p. 63

¹⁰¹ Clark C. Havighurst, « *The Place Of Private Accrediting Among The Instruments Of Government* » (1994) 57 *Law and Contemporary problems*, 1, à la page 2.

¹⁰² Kees Stuurman, « *Legal Aspects Of Standardization And Certification In Information Technology And Telecommunication : An Overview* », dans Kaspersen, HWK et A. Oskamp, *Amongst Friends in Computer Law : a Collection of Essays in remembrance of Guy Vanderberghe*, 1990, Kluwer Law and Taxation Publishers, Deventer, Hollande, page 75.

La mise en place de standards est de nature à faciliter l'ouverture de marché. En ce sens, l'application de standards peut être utilisée pour la caractérisation des produits¹⁰³. Quant au concept de qualité, l'établissement de standards à ce niveau diffère, mais n'est pas toujours

Au niveau de l'Internet, le commerce électronique apparaît pour certains comme étant en grande partie conduit par les standards du marché¹⁰⁴.

Enfin, le rôle des organismes de standardisation peut être très variable. Pour certains, leur rôle devrait se limiter aux aspects de compatibilité des technologies sous-tendant le commerce électronique en laissant au marché le soin de déterminer le reste. À notre avis, sans qu'il soit question de réglementer Internet de quelque façon que ce soit, il nous apparaît utile et profitable aux entreprises que des standards existent et puissent donc être reconnus tant au niveau des pratiques commerciales que des technologies.

1.2 Les niveaux des standards

La certification peut être de portée variée selon les paramètres qu'elle utilise. L'un de ces paramètres est le niveau des standards utilisés.

Ceux-ci peuvent varier de la simple reconnaissance de l'existence d'une pratique dans l'entreprise, de la qualité ou de la conformité de celle-ci ou de ses produits pour aller de façon ultime jusqu'aux standards du plus haut niveau, c'est-à-dire ceux se rapportant aux performances.

¹⁰³ Marcus Maher, « *An Analysis of Internet Standardization* », 3 Va. J.L. & Tech. 5 (Spring 1998) http://scs.student.virginia.edu/~vjolt/graphics/vol3/home_art5.html An analysis of Internet standardization, « *An Analysis of Internet Standardization* », 3 Va. J.L. & Tech. 5 (Spring 1998) http://scs.student.virginia.edu/~vjolt/graphics/vol3/home_art5.html An analysis of Internet standardization, paragraphe 18.

¹⁰⁴ Marcus Maher, « *An Analysis of Internet Standardization* », 3 Va. J.L. & Tech. 5 (Spring 1998) http://scs.student.virginia.edu/~vjolt/graphics/vol3/home_art5.html An analysis of Internet standardization, « *An Analysis of Internet Standardization* », 3 Va. J.L. & Tech. 5 (Spring 1998) http://scs.student.virginia.edu/~vjolt/graphics/vol3/home_art5.html An analysis of Internet standardization, paragraphe 65.

Le standard est un élément clé de l'attribution de la certification. Or, dans le cas d'organismes de certification privés, il existe peu de contrainte dans l'élaboration de standards. Mis à part la prohibition de certains motifs de discrimination¹⁰⁵ dans les relations privées, le contenu des standards est laissé à l'entière discrétion du certificateur¹⁰⁶. Une certaine uniformité est cependant requise dans le but de faciliter la compréhension et la reconnaissance de la certification.

Tel que mentionné précédemment, la portée de la certification qui en découle aura une relation directe avec le niveau des standards utilisés.

1.3 Standard *de facto* et standard officiel

L'élaboration de standards peut donner lieu à des difficultés insoupçonnées. On peut imaginer qu'il est simple d'élaborer des normes pour un secteur d'activité pour ensuite laisser à la discrétion des entreprises de les appliquer ou non.

Cependant, certaines industries verront un avantage à développer leurs propres standards. Dans le cadre de grandes entreprises, on pourra même assister au développement de standards internes. Il sera alors question de standards *de facto*¹⁰⁷. Or, les entreprises ayant développé elles-mêmes leurs standards pourront revendiquer des droits d'auteur sur ceux-ci, ce qui pourrait engendrer certaines limites à l'accessibilité et à l'applicabilité de ces standards par leurs concurrents.

On imagine aisément qu'un standard *de facto* reconnu par les consommateurs mais non accessible à l'ensemble des entreprises d'un secteur d'activité sera néfaste pour

¹⁰⁵ Article 10 de la *Charte des droits et libertés de la personne*, L.R.Q., c. C-12.

¹⁰⁶ Cette problématique a été abordée dans le cadre d'une étude sur le système d'accréditation des institutions d'enseignement supérieur aux États-Unis dans Matthew, W. Finkin, "*The Unfolding Tendency In The Federal Relationship To Private Accreditation In Higher Education*", (1994) 57 *Law and Contemporary Problems*, 89.

¹⁰⁷ Kees Stuurman, « *Legal Aspects Of Standardization And Certification In Information Technology And Telecommunication : An Overview* », dans Kaspersen, HWK et A. Oskamp, *Amongst Friends in Computer Law : a Collection of Essays in remembrance of Guy Vanderberghe*, 1990, Kluwer Law and Taxation Publishers, Deventer, Hollande, page 76.

ceux qui en sont privés. Dans une telle situation, les standards auront plutôt l'effet inverse de fermeture de marché pour protéger le secteur d'activité de certaines industries. Ce genre de situation a d'ailleurs donné lieu à des débats devant les tribunaux¹⁰⁸.

En revanche, la présence de standards officiels, dans le sens d'accessible à tous, poursuivra davantage l'objectif de l'ouverture des marchés. Il est difficile de croire qu'un organisme privé pourra atteindre cet objectif. De plus, l'emploi de l'expression « standard officiel » apporte une dimension étatique, un caractère public aux standards. Il existe déjà des situations où des organismes privés sont chargés de certification ou d'accréditation dans un domaine public¹⁰⁹.

Toutefois, la mise en place de standards publics donnera lieu à une intervention sans doute peu souhaitée qui risque peut-être d'avoir des conséquences plus néfastes que positives. Contrairement à un domaine public où le gouvernement détermine les critères et délègue son pouvoir d'évaluation¹¹⁰, le milieu du commerce sur Internet n'a peut-être pas besoin d'une telle intervention.

2. Évaluation de l'entité

L'évaluation de l'entité constitue la seconde étape du processus de certification. Celle-ci peut se dérouler de différentes façons. La méthode employée aura un impact direct sur la valeur de la certification. Notons qu'il s'agit de la phase contractuelle de ce processus, laquelle nécessite une participation active des parties.

¹⁰⁸ *Lotus Development corporation vs. Paperback Software International and Stevenson Software Ltd*, US District Court of Massachusset, Juge Robert E. Keeton, 28 juin 1990.

¹⁰⁹ Par exemple dans le milieu de la santé. Voir à ce sujet : Timothy-Stoltzfus Jost, « *Medicare And The Joint Commission On Accreditation Of Healthcare Organizations* », (1994) 57 *Law and Contemporary Problems*, 15.

¹¹⁰ Eleanor D. Kinney, « *Private Accreditation As A Substitute For Direct Government Regulation In Public Health Insurance Programs : When Is It Appropriate ?* », (1994) 57 *Law and Contemporary problems*, 47.

À ce niveau, il est important de mentionner que l'évaluation d'une entité dans le but d'obtenir la certification nécessite en principe l'implication d'un tiers indépendant¹¹¹. Cette implication pourra se situer à différents niveaux.

Dans ce contexte, on parle beaucoup d'audit. Si les références habituelles portant sur l'audit réfèrent à la vérification de compte, l'audit peut néanmoins porter sur un ensemble d'éléments. C'est dans ce sens large que nous y référons.

Tout comme la certification, l'audit peut être de différents types, selon qu'il vise la régularité, la conformité ou encore l'efficacité¹¹². Elle peut viser également divers objets, certains relevant du domaine juridique¹¹³.

2.1 L'audit interne

L'audit interne est d'abord et avant tout une méthode de contrôle interne à l'entreprise. Il vise à vérifier que les conditions nécessaires à assurer l'équilibre interne de l'entreprise sont réunies¹¹⁴. Une telle méthode implique que l'entreprise concernée effectue elle-même les vérifications avec des moyens qu'elle se donne et qu'elle juge appropriés.

Parfois, l'audit interne débouche directement et sans l'intervention d'un tiers extérieur sur l'émission d'un sceau ou d'un certificat à l'intention des tiers. Une telle procédure peut être qualifiée d'autocertification. Toutefois, il est à notre avis incorrect de parler de certification dans un tel cas en raison de l'absence

¹¹¹ Alain Couret, Jacques Igalens et Hervé Penan, *La Certification*, Presses Universitaires de France, Paris, 1995, Collection Que sais-je ?, numéro 3006, page 5. Voir également : Rae, Andrew, K., Hans-Ludwig Hausen, Philippe Robert, *Software Evaluation for Certification, Principles, Practice and Legal Liability*, (1995), McGraw Hill Book Company, England, à la page 2 : « certification involves some form of independent assessment. ».

¹¹² Etienne Barbier, *L'audit interne, permanence et actualité*, (1996), 3^e Edition, Les Éditions d'Organisation, France, à la page 27.

¹¹³ Il est à noter que plusieurs autres professions s'immiscent dans l'évaluation spécifique au domaine juridique. Elles se justifient en affirmant que l'auditeur n'agit pas comme un expert du domaine, mais uniquement pour évaluer si les risques sont maîtrisés. Nous ne partageons pas cette opinion et à notre avis, un tel travail doit être confié à des juristes. Voir à ce sujet : Etienne Barbier, *L'audit interne, permanence et actualité*, (1996), 3^e Edition, Les Éditions d'Organisation, France, pages 43-44.

d'intervention externe. Le résultat consiste davantage en une sorte de garantie ou une marque de conformité interne ou encore à un secteur d'activité¹¹⁵.

Tel que nous l'avons mentionné précédemment, pour être en présence de certification, nous sommes d'avis que le processus requiert la participation d'un tiers externe indépendant. Il y a donc l'alternative de communiquer avec un tiers certificateur et lui transmettre les résultats de l'audit. Ce dernier étudiera alors l'évaluation effectuée et sera en mesure de décider d'émettre ou non la certification.

La valeur d'une telle certification en est cependant affectée. Bien que les résultats de la vérification soient transmis au certificateur, ce dernier ne joue alors qu'un rôle très limité dans l'évaluation. En effet, il ne participe ni à la détermination de l'objet de l'évaluation, ni à l'évaluation elle-même. La certification qui en résulte est somme toute de valeur très limitée.

Une meilleure solution pour l'entreprise est de se soumettre, soit à un audit externe, soit de répondre aux questions posées par le tiers certificateur.

2.2 La déclaration volontaire

La déclaration volontaire est la méthode la plus fréquemment employée pour l'émission de certificat et de sceau sur Internet. En effet, il n'y a pas que les entreprises et les consommateurs qui ne soient pas en présence l'un de l'autre lors de leurs relations dans le cyberspace. Dans la plupart des cas, l'entité qui recherche la certification et celle qui l'octroie ne se rencontreront jamais physiquement.

¹¹⁴ Etienne Barbier, *L'audit interne, permanence et actualité*, (1996), 3^e Edition, Les Éditions d'Organisation, France, à la page 24.

¹¹⁵ On cite à ce niveau l'exemple de la marque « Woolmark » que l'on retrouve sur les produits de laine vierge dans : Alain Couret, Jacques Igalens et Hervé Penan, *La Certification*, Presses Universitaires de France, Paris, 1995, Collection Que sais-je ?, numéro 3006, page 10.

L'évaluation se fait alors au moyen de questionnaires détaillés auxquels doit répondre l'entreprise par le biais de personnes compétentes dûment autorisées. Dans un tel cas, il y a réellement une évaluation de l'entité concernée par un tiers et le certificateur joue un rôle en ce sens. Toutefois, il y a peu de contrôle sur la qualité des réponses obtenues par ce moyen.

La qualité de la certification qui en résulte dépendra en grande partie de la qualité des formulaires d'évaluation et de l'analyse des réponses données par le certificateur.

2.3 L'audit externe

L'audit externe est la forme la plus poussée d'évaluation. C'est aussi la plus coûteuse et c'est pourquoi elle est encore peu employée dans le cadre du commerce sur Internet.

En matière d'audit externe, les auditeurs se chargent d'évaluer le candidat selon la nature de la certification recherchée. Cette évaluation est fréquemment longue et coûteuse. Selon la procédure utilisée, elle peut déboucher sur l'émission d'un rapport et parfois, sur un audit complémentaire.¹¹⁶ Elle offre cependant des garanties maximales de fiabilité et le niveau de certification le plus élevé.

Malheureusement, force nous est de constater que les personnes qui se réfèrent à la certification pour bâtir un lien de confiance ne sont jamais informées du mode d'évaluation utilisé. En général, c'est la réputation du certificateur qui joue le plus grand rôle à cet égard.

¹¹⁶ Geneviève Iacono, « *La certification d'assurance qualité : De nouvelles questions pour le Droit ?* », (1994) *Revue Internationale de Droit Économique* 63, p. 72.

3. La certification

La décision d'accorder ou non la certification est l'aboutissement du processus. Elle ne met cependant pas un terme au rôle du certificateur car un suivi de celle-ci doit par la suite être effectué.

3.1 Décision du certificateur

Le premier élément à souligner est que le certificateur n'a pas d'obligation initiale d'accorder ou non la certification. Cette décision se base sur l'analyse effectuée. En ce sens, nous partageons donc l'avis exprimé à ce sujet :

« il faut bien avoir présent à l'esprit que l'entreprise candidate à la certification, ne peut être considérée comme coauteur du contenu de l'acte. »¹¹⁷

Bien que l'étape de la certification par un organisme privé comporte les caractéristiques d'un acte unilatéral¹¹⁸, il n'en demeure pas moins qu'il s'inscrit dans un cadre contractuel précis.

En effet, le certificateur ne jouit pas d'un pouvoir arbitraire. Comme la certification est une reconnaissance de conformité relativement à des paramètres déterminés, le certificateur doit se baser sur ces critères pour déterminer s'il octroie ou non la certification, d'autant plus qu'il a lui-même élaboré ces critères et qu'il jouit d'une grande latitude quant à la portée de ceux-ci.

¹¹⁷ Geneviève Iacono, « *La certification d'assurance qualité : De nouvelles questions pour le Droit ?* », (1994) *Revue Internationale de Droit Économique* 63, p. 74.

¹¹⁸ Geneviève Iacono, « *La certification d'assurance qualité : De nouvelles questions pour le Droit ?* », (1994) *Revue Internationale de Droit Économique* 63, p. 76.

3.2 Les marques de certification

On perçoit les marques de certification d'abord comme étant une façon de publiciser la certification acquise. C'est en ce sens qu'on la compare souvent à un diplôme¹¹⁹.

Deux marques de certification sont utilisées fréquemment. Il s'agit du sceau et du certificat.

Le sceau rappelle d'habitude les anciens cachets de cire dont étaient marqués certains actes pour les rendre authentiques. Aujourd'hui, il prend un sens plus général mais conserve la notion d'empreinte. C'est donc une marque confirmant la certification mais ne donnant aucun détail sur celle-ci, mis à part l'identité du certificateur.

Le sceau demeure toutefois très populaire. Il semble que les internautes soient de nature assez visuels. Ainsi, le sceau a l'avantage d'être plus remarquable qu'un certificat disponible au moyen d'un hyperlien.

En revanche, le certificat se veut une marque plus complète. Il s'agit encore une fois d'une attestation confirmant la certification. Cependant, elle (devra ou donnera) des détails sur la nature de la certification, à savoir les critères et paramètres dont la certification atteste la conformité¹²⁰.

Le certificat fournit donc une information plus complète mais se doit en revanche d'être précis en reprenant le plus fidèlement possible les paramètres sur lesquels se fonde la certification. En effet, le consommateur sera justifié de se fier et de se rapporter au contenu du certificat.

¹¹⁹ Geneviève Iacono, « *La certification d'assurance qualité : De nouvelles questions pour le Droit ?* », (1994) *Revue Internationale de Droit Économique* 63, p. 70.

¹²⁰ La loi française, 78-23 du 10 janvier 1978 sur la protection et l'information des consommateurs de produits et de services (dite loi Scrivener) contient une définition du certificat en matière de certification. L'extrait pertinent de l'article 22 paragraphe 1 se lit comme suit : « Constitue un certificat de qualification, quelle que soit la dénomination qui lui est donnée, toute inscription, tout signe distinctif, tout document ou titre joint tendant à attester, à des fins commerciales, qu'un produit [...] présente certaines caractéristiques spécifiques ayant fait l'objet d'un contrôle par un

Sur Internet, il est intéressant de constater que l'utilisation du sceau et du certificat peuvent être conjugués. En effet, seul le sceau apparaîtra sur une page certifiée. Toutefois, le sceau lui-même constituera un hyperlien permettant à l'internaute d'avoir accès à toute l'information contenue au certificat.

Par ailleurs, les organismes de certification verront à protéger les sceaux et certificats qu'ils émettent et à en garder le contrôle. Cette protection sera d'abord et avant tout basée sur les règles en matière de marque de commerce. Ainsi, une marque de certification pourra être enregistrée comme marque de commerce et bénéficier de la protection qui s'y rattache¹²¹.

Une mise en garde est cependant requise contre le danger de la multiplication du nombre de sceaux. En effet, on voit de plus en plus apparaître des sigles et sceaux de classification ou de qualité sur les sites Web. Leur graphisme se veut le plus attrayant ou encore le plus frappant possible, ce qui n'est pas nécessairement en proportion avec leur valeur. De plus, plus le nombre de ceux-ci augmente, plus il est difficile de distinguer les véritables sceaux de qualité des instruments purement publicitaires. Il peut alors en résulter davantage de confusion que d'information au consommateur¹²².

3.3 Le suivi de la certification

Rien ne garantit qu'une fois la certification accordée, les mêmes standards continueront d'être maintenus par l'entité certifiée. Ainsi, l'évaluation est un processus récurant car un suivi est nécessaire auprès de cette dernière. Ce suivi

organisme distinct du fabricant, de l'importateur ou du vendeur. », tiré de : <http://www.admi.net/jo/loi78-23.html> (consulté le 30-11-1999).

¹²¹ Kees Stuurman, « *Legal Aspects Of Standardization And Certification In Information Technology And Telecommunication : An Overview* », dans Kaspersen, HWK et A. Oskamp, *Amongst Friends in Computer Law : a Collection of Essays in remembrance of Guy Vanderberghe*, 1990, Kluwer Law and Taxation Publishers, Deventer, Hollande, page 85.

¹²² Clark C. Havighurst, « *The Place Of Private Accrediting Among The Instruments Of Government* » (1994) 57 *Law and Contemporary problems*, 1, à la page 10.

pourra être très différent selon les cas. Le délai du suivi, le niveau d'évaluation pourra différer substantiellement selon le secteur d'activité concerné. Ainsi, dans les milieux financiers, un suivi devra être effectué entre 30 jours et 90 jours.

En réalité, le suivi n'est autre chose qu'une réévaluation. En conséquence, l'entité certifiée qui échoue à cette réévaluation est susceptible de perdre le sceau et le certificat qui lui ont été conférés.

Il faut souligner que l'établissement d'une durée fixe à la certification et la réévaluation de l'entité revêtent une importance particulière sur Internet. En effet, le support informatique facilite beaucoup la modification d'un site Web. Et de fait, les sites sont pour la plupart en mouvement et en construction perpétuelle. On peut les comparer à une image vidéo tandis que la certification, de son côté, est de la nature d'une photographie, donnant l'état de la réalité à un moment précis. En ce sens, la certification devient rapidement obsolète, d'où la nécessité de la mettre à jour régulièrement.

3.4 Des exemples de certification de sites Web

Le premier type de certification qui est apparu sur Internet ne vise pas les sites comme tels, mais adresse une question particulière : l'existence de l'entité. Ainsi sont nées les autorités de certification. Aujourd'hui, les entreprises et organismes qui se sont constitués comme autorité de certification sont très nombreux et présents dans plusieurs pays¹²³.

Ces organismes ne vérifient en rien le contenu du site ni les biens et services offerts. Ils ne s'attardent qu'à un seul aspect, soit celui de confirmer ou encore de permettre aux parties de s'assurer de l'identité réelle du correspondant. Comme ce mécanisme d'identification fait appel à des concepts de cryptographie, par extension, il permet

¹²³ Voir la liste à l'annexe « A ».

parfois à ces entités d'échanger des messages sécurisés et même signés au moyen de la technique de cryptographie asymétrique.

Puis, la certification des sites Web est apparue comme un besoin. Même à ce niveau, plusieurs organismes se limitent à la certification d'un ou plusieurs objets. Ainsi, certains se spécialisent sur la certification des sites qui rencontrent des spécifications minimales en matière de sécurité¹²⁴. Par ailleurs, on ne peut passer sous silence l'apparition et la disparition rapide de nouvelles entreprises dans ce domaine¹²⁵.

Pour les fins des présentes, nous nous attarderons à trois organismes offrant des services de certification qui nous apparaissent actuellement comme les acteurs majeurs à ce niveau. Ils offrent chacun des types différents de certification qui se rattachent au contenu du site. Il s'agit de : TRUSTe, WebTrust et le Better Business Bureau.

3.4.1 TRUSTe

TRUSTe¹²⁶, de son nom complet Trusted Universal Standards in Electronic Transactions a été constitué aux États-Unis en 1996¹²⁷. Commandité par une cinquantaine d'entreprises majeures dans le domaine de l'Internet et des technologies de l'information¹²⁸, le programme de certification développé par TRUSTe est orienté exclusivement à la protection des renseignements personnels.

¹²⁴ Voir à ce sujet : Dan Costa, « *NCSA Launches Secure Website certification* », Computer Shopper, novembre 1996, vol. 16, n° 11, p. 84 ; Gary H. Anthes, « *Look for the NCSA label* », Computer World, 5 août 1996, vol. 30, n° 32, page 57 ; ICSA (NCSA) Firewall Certification, <http://www.icsa.net>. Note : NCSA est la National Computer Security Association.

¹²⁵ Certains organismes disparaissent, d'autres changent de vocation. Ainsi, des exemples cités récemment ne sont plus applicables. C'est le cas des exemples de l'Internet Consumer Protection Agency (<http://www.glen-net.ca/icpa>) et de l'Ombudsman (<http://www.ombudsman.com/#1>), cités dans : Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, aux pages 3-48 et 3-49.

¹²⁶ <http://www.TRUSTe.org>. Voir également le site <http://www.TRUSTe.com> qui donne la liste des participants au programme.

¹²⁷ Voir à ce sujet : Esther Shein, « *You can eTRUST us* », PC Week, 16 décembre 1996, vol. 13, n° 50, page E-1 ; Elizabeth Wasserman, " *Getting A Website Seal Of Approval* ", San Jose Mercury News, 16 octobre 1996, page 1A. Il est à noter que le programme s'appelait à l'origine « eTRUST ».

¹²⁸ La liste des commanditaires se retrouve à : http://www.TRUSTe.org/about/about_sponsors.html

Bien que l'organisme se penche principalement sur le besoin des consommateurs américains, le programme de certification est tout de même offert à tous les sites Web dans le monde.

Les objectifs poursuivis par l'organisme sont multiples. Bien qu'on tente de les résumer au noble fait d'établir la confiance dans le commerce électronique¹²⁹, ceux-ci dépassent l'objectif de la confiance pour atteindre des besoins plus corporatistes.

Le premier d'entre eux est de donner au consommateur le contrôle sur l'information personnelle qui le concerne et qu'il peut être amené à divulguer sur Internet. Le second est de fournir un encadrement standardisé aux éditeurs de sites Web tout en leur procurant des solutions satisfaisantes sur le plan commercial.

Le dernier but poursuivi, bien qu'il ne soit pas mis en évidence, est de démontrer aux gouvernements que l'industrie oeuvrant sur Internet a la volonté et la capacité de s'autoréglementer convenablement.

La mécanique de la certification offerte par TRUSTe gravite autour d'un contrat de licence¹³⁰. TRUSTe offre une marque de certification générale dont les critères d'obtention et d'utilisation sont décrits au contrat de licence. Un programme complémentaire à ce dernier s'adresse spécifiquement au site destiné aux enfants de moins de 13 ans.

On exige différents éléments de la part de l'entité qui recherche la certification. Le premier élément est, si ce n'est déjà fait, l'adoption et la mise en place d'une politique d'entreprise en matière de protection des renseignements personnels. Les éléments devant être couverts par cette politique sont détaillés au contrat de licence. Ils concernent essentiellement des règles concernant la cueillette, la constitution de dossiers et l'utilisation de l'information confidentielle. On y retrouve de nombreux

¹²⁹ « eTRUST, an initiative to establish trust and confidence in electronic commerce », dans : Shein, Esther, « *You can eTRUST us* », PC Week, 16 décembre 1996, vol. 13, n° 50, page E-1.

éléments en commun avec la *Loi sur la protection des renseignements personnels dans le secteur privé*¹³¹.

Ainsi, l'information confidentielle est définie de façon très large comme toute information de nature personnelle pouvant être utilisée pour identifier, contacter ou localiser une personne.

L'évaluation initiale à laquelle TRUSTe procède s'effectue au moyen de questionnaires élaborés auxquels l'entité concernée doit répondre. Y sont abordées la collecte et l'utilisation de l'information personnelle dans son sens large. L'entité doit identifier quel type d'information elle recueille des internautes, qui la recueille, comment elle sera utilisée et avec qui elle sera partagée. On y aborde également les choix offerts à l'utilisateur et on exige de l'entité de donner un droit de retrait à la personne concernée. La conservation de l'information recueillie fait l'objet d'une série de questions portant tant sur la sécurité, la confidentialité que la non altération de celle-ci.

L'évaluation initiale de l'entité se limite donc à un formulaire¹³². Une fois celui-ci rempli, il est simplement examiné par TRUSTe, qui émet alors le sceau. Les frais imposés ne peuvent être qualifiés de frais de certification puisqu'ils sont clairement indiqués comme étant des frais de licence pour l'utilisation du sceau. Or, cette licence est d'un coût variable selon les revenus annuels bruts de l'entreprise concernée¹³³. Ainsi, le sceau remis fait l'objet d'un contrat de licence. Aux termes de ce contrat, TRUSTe accorde une licence non exclusive et universelle à l'entité concernée. Il est cependant clairement stipulé que TRUSTe demeure le seul et unique propriétaire de toutes les marques de commerce et marques de certification¹³⁴.

¹³⁰ Nous référons ici à la version 5.01 de l'entente de licence TRUSTe (elle est datée du 19 août 1999), disponible sur le site <http://www.TRUSTe.org>.

¹³¹ L.R.Q. chapitre P-39.1.

¹³² À l'origine, le système prévoyait un audit externe par des entreprises comptables majeures. Esther Shein, « *You can eTRUST us* », PC Week, 16 décembre 1996, vol. 13, n° 50, page E-1.

¹³³ Ces frais varient de 299\$ à 4 999\$, selon les revenus annuels de l'entreprise (article 6 du contrat de licence).

¹³⁴ Article 3 b) de l'entente de licence TRUSTe, version 5.01.

Il est intéressant de constater que TRUSTe offre sa marque de certification telle quelle et stipule expressément dans son contrat de licence n'offrir aucune garantie de quelque nature que ce soit. On y stipule expressément que le licencié défendra, indemnisera et tiendra TRUSTe indemne de tout dommage, responsabilité, frais ou dépense qu'il pourrait encourir suite à la réclamation d'un tiers relativement au site du licencié¹³⁵. Il s'agit en fait de la clause standard visant à exclure toute responsabilité face aux tiers.

De son côté, le licencié s'engage aux termes du contrat à afficher la marque de certification dans les endroits appropriés de son site tel que la page d'accueil, la page de menu ou encore la première page où débute la collecte d'information personnelle¹³⁶.

Une fois la certification mise en place, TRUSTe doit assurer un certain suivi au niveau des organismes certifiés. À ce sujet, on indique simplement qu'une réévaluation périodique à laquelle le licencié acquiesce peut avoir lieu¹³⁷. Aucune information supplémentaire n'est donnée quant à la qualité, la portée et la fréquence de cette réévaluation.

Pour le consommateur, un dispositif pour la réception des plaintes a été mis en place. Celui-ci s'intitule «Watchdog». Toutefois, avant de pouvoir rapporter la plainte à TRUSTe, le consommateur doit vérifier au préalable si celle-ci cadre dans l'objet de la certification, à savoir la protection des renseignements personnels, et dans l'affirmative, la plainte doit avoir été adressée dans un premier temps à l'entité concernée qui a alors l'occasion d'y répondre directement. Ainsi, c'est uniquement dans les cas où l'entité concernée ne fournit pas de réponse ou encore fournit une réponse insatisfaisante que l'organisme de certification sera saisi de la plainte.

¹³⁵ Article 3 d) du contrat de licence.

¹³⁶ Article 2 e) schedule A, du contrat 5.01.

¹³⁷ Article 5, schedule A, Licence agreement version 5.01.

Le mécanisme de résolution des plaintes s'exerce là encore par étapes puisque TRUSTe contacte dans un premier temps l'entité concernée pour résoudre les différents points. C'est seulement si cette démarche échoue et que TRUSTe estime que l'entité est en bris de contrat qu'elle procédera à la résiliation de la licence. À la lecture du contrat de licence, on constate toutefois que ce type de résiliation doit être précédé d'un avis écrit de 30 jours au licencié concerné, ce qui crée de nouveaux délais¹³⁸. Enfin, il est intéressant de noter le fait que dans des cas extrêmes, TRUSTe pourrait référer le cas à l'agence gouvernementale appropriée.

Dans une perspective d'autoréglementation, l'avantage principal d'un organisme tel TRUSTe comparativement à une loi gouvernementale est l'évaluation préalable de l'entité. De plus, le caractère contractuel de la licence lui permet d'avoir une portée extraterritoriale. En revanche, il nous semble que la portée de l'évaluation, le suivi de celle-ci et le mécanisme de résolution des plaintes soit faible.

3.4.2 Better Business Bureau¹³⁹

Le Better Business Bureau, un organisme américain, a développé deux types de certifications sur Internet. Il existe un programme portant sur la protection des renseignements confidentiels et l'autre sur la fiabilité du site.

Le programme sur la protection des renseignements personnels est très récent puisqu'il a été lancé en mars 1999¹⁴⁰. Il offre un sceau de certification confirmant que le site a été vérifié relativement à ces pratiques en matière de manipulation de l'information. Ces pratiques incluent la mise en place d'une politique de protection des renseignements personnels, la révision de celle-ci par une organisation de confiance et finalement un mécanisme de résolution des litiges.

¹³⁸ Article 5 a) du Licence agreement, version 5.01.

¹³⁹ <http://www.bbbonline.org>.

¹⁴⁰ « BBBOOnline's NEW PRIVACY SEAL PROGRAM OPENS FOR BUSINESS: Helps Websites Assure Visitors that their privacy is respected », BBBOOnline, communiqué du 17 mars 1999.

Le programme de fiabilité, quant à lui, a démarré en avril 1997 dans le but d'identifier les entreprises qui démontrent une certaine fiabilité sur le marché de l'Internet¹⁴¹.

Programme de protection des renseignements personnels

Le programme de certification en matière de protection des renseignements personnels de BBBOnline se rapproche beaucoup de celui offert par TRUSTe. Encore une fois, on note un programme complémentaire pour les sites destinés aux enfants.

L'entité qui désire obtenir le sceau de certification doit être partie à une entente de participation avec BBBOnline. Encore une fois, l'évaluation de l'entité et du site se fait au moyen d'un questionnaire qui est complété et retourné avec le paiement des frais afférents¹⁴².

Dans l'entente, on retrouve des clauses au même effet en ce qui a trait à la propriété du sceau¹⁴³. BBBOnline se réserve ainsi le droit d'effectuer des vérifications sur une base aléatoire.

Le contrat est accordé pour une période initiale de un (1) an. De plus, l'organisme se réserve le droit de suspendre l'entité certifiée du programme à son entière discrétion si elle évalue que celle-ci ne se conforme pas aux termes de l'entente.

Par la suite, l'entente peut être terminée si le licencié fait défaut d'en appeler de la suspension ou encore si BBBOnline rejette cet appel¹⁴⁴. Le texte de l'entente contient néanmoins une stipulation très claire à l'effet que les sceaux sont émis tels

¹⁴¹ Miguel Helft, « *Commerce on the Net : whom do you trust ?* », Los Angeles Times, 10 mars 1997, vol. 116, page D-1, colonne 4.

¹⁴² Dans le cas du programme de protection des renseignements personnels de BBBOnline, les frais annuels varient de 150\$ à 3 000\$ selon les revenus totaux de l'entreprise.

¹⁴³ BBBOnline Privacy Program Participation Agreement, revised on August 31, 1999, art. 3.

¹⁴⁴ BBBOnline Privacy Program Participation Agreement, revised on August 31, 1999, art. 4, par. c) et d).

quels sans garantie d'aucune sorte. De plus, le licencié s'engage ici encore à indemniser et tenir indemne BBBOnline relativement à toute réclamation, perte, poursuite, dommages ou dépenses encourues dans le cadre d'une poursuite¹⁴⁵. Il est à noter que ces (problèmes) de sceaux, bien qu'établis aux États-Unis et régis par les lois de l'état de la Virginie, ne sont disponibles qu'au Canada et aux États-Unis.

Une procédure de résolution des conflits a également été élaborée par BBBOnline. Celui-ci offre un processus de résolution des conflits effectué par le Privacy Policy Review Service du BBBOnline. Il s'agit de modes alternatifs de résolution des conflits entre les individus. Il faut remarquer que dans le cadre d'une telle procédure, le plaignant peut demander d'avoir accès à l'information, de voir celle-ci corrigée s'il y a lieu mais en aucun cas le service de l'organisme de certification ne peut accorder de dommages monétaires ou de la même nature. Un droit d'appel à un autre comité est également prévu au programme. Les règles de procédures en sont clairement établies et prévoient même la publication des décisions quatre fois par année.

Le programme de fiabilité

Le programme de certification relativement à la fiabilité des entreprises vise à donner une certaine assurance relativement au commerce sur Internet.

Si sa mission est d'aider les internautes à trouver des entreprises dignes de confiance sur Internet, le programme a également pour but d'éviter la réglementation étatique sur Internet.

Pour obtenir le sceau, les entreprises doivent devenir membres d'un bureau local du Better Business Bureau. Comme exigence première, l'organisme exige que l'entreprise concernée soit en affaires depuis un minimum d'un an.

¹⁴⁵ BBBOnline Privacy Program Participation Agreement, revised on August 31, 1999, art. 7.

Outre l'inscription auprès d'un bureau local du Better Business Bureau, l'entreprise doit signer une entente d'arbitrage qui le liera en cas de différend avec ses clients.

Il est toutefois souligné que malgré son appellation de sceau de fiabilité, l'organisme de certification ne garantit pas la satisfaction des clients et n'endosse pas les compagnies ou leurs produits. L'organisme se contente de certifier l'existence d'une compagnie bien établie et qui s'engage à un mode de résolution neutre des conflits pouvant survenir avec ses clients.

3.4.3 Webtrust

Le sceau Webtrust poursuit le même objectif que ses concurrents, soit celui d'apporter la confiance d'un commerce électronique sur Internet. Le programme est cependant quelque peu différent et se distingue des sceaux développés par TRUSTe et BBBOnline.

En effet, le programme Webtrust a été développé par l'Institut des comptables agréés au Canada et aux États-Unis. Le programme fut lancé en 1997 par l'AICPA¹⁴⁶ et l'ICCA¹⁴⁷.

Essentiellement, le programme Webtrust se distingue des autres programmes puisqu'il est endossé par un ordre professionnel et qu'un audit complet du site Web concerné doit être effectué par un comptable reconnu ayant reçu une formation spécifique à cet égard. C'est une fois que le professionnel a émis son rapport confirmant que le site rencontre les principes et critères développés par Webtrust que le sceau sera émis.

¹⁴⁶ American Institute of certified public accountants, www.cpaonline.com.

¹⁴⁷ Institut canadien des comptables agréés, www.cica.ca.

Le sceau Webtrust est donc présenté lui-même comme étant la représentation symbolique du rapport effectué.

Les principes sur lesquels se base la vérification sont :

- la divulgation des pratiques commerciales;
- l'intégrité des transactions;
- la protection de l'information personnelle.

Un document est régulièrement mis à jour expliquant en détail ces principes et critères du programme WebTrust pour le commerce électronique entre entreprises et consommateurs¹⁴⁸.

Dans le cas du programme WebTrust, le sceau affiché sur le site informe donc le consommateur que ce site a été évalué par un comptable reconnu ayant reçu une formation spécifique à cet effet. Les promoteurs du programme font donc valoir que les comptables agréés sont des professionnels reconnus particulièrement dans le domaine de la vérification et de l'assurance de conformité. Bien que l'entité désirant obtenir la certification doive remplir un questionnaire, il n'en demeure pas moins qu'un comptable doit se rendre auprès de l'entreprise et effectuer une vérification complète de celle-ci en fonction des principes et critères de WebTrust.

Ainsi, la compagnie ne paie pas un droit de licence pour l'affichage d'un sceau mais paie uniquement les services du professionnel qui procède à l'audit.

C'est uniquement sur réception d'un rapport reconnu que l'entité concernée pourra bénéficier du sceau sur son site Web. Par ailleurs, l'entreprise devra se requalifier sur une base périodique d'au plus 90 jours. La période de requalification dépendra notamment de la nature et de la complexité de ses activités, de la fréquence des

¹⁴⁸ Voir à ce sujet le Webtrust™ Principles and Criteria for Business-to-Consumer Electronic Commerce, version 2.0, 1^{er} septembre 1999, disponible à <http://www.cica.ca/cica/cicawebsite.nsf/Public/SPASWebTrust>.

changements significatifs apportés à son site et de l'opinion du comptable chargé de la vérification¹⁴⁹.

L'internaute a accès au rapport du comptable puisque le sceau WebTrust constitue un hyperlien vers ce rapport. La compagnie Verisign¹⁵⁰ apporte son expertise dans le but d'assurer l'authenticité du certificat apposé sur le site. Contrairement aux deux problèmes précédents, on note cependant que le programme WebTrust ne prévoit aucun mécanisme pour recueillir les plaintes. Bien qu'un arbitrage soit possible entre l'entreprise et le consommateur et que WebTrust ait prévu un ensemble de règles à cet effet, les parties doivent d'abord convenir de s'y soumettre¹⁵¹. De plus, les participants au programme de certification insistent sur le fait qu'il ne donne aucune garantie au consommateur quant à la qualité des produits. Les seuls éléments qui sont examinés sont les pratiques commerciales de l'entreprise, l'intégrité des transactions et la protection des renseignements personnels. La protection du consommateur en regard de la certification est donc uniquement garantie par le fait que le travail a été effectué par un professionnel membre d'un ordre et disposant normalement à cet effet d'une assurance responsabilité.

Nous avons ici fait un bref survol de trois types de certification disponibles pour les sites Web commerciaux. Tous trois poursuivent la même finalité, à savoir de combattre les craintes et les inhibitions que les consommateurs ressentent face au fait d'effectuer des transactions commerciales sur Internet tout en démontrant par la même occasion la capacité de l'industrie de s'autoréglementer.

D'emblée, il est important de remarquer que ces trois programmes ont été lancés récemment puisque le plus ancien d'entre eux, TRUSTe, a démarré en 1996. Par ailleurs, aucun de ces programmes n'a réussi à ce jour à s'élever au niveau de standard (de fait) dans l'industrie.

¹⁴⁹ WebTrust principles and criterias, version 2.0, page 11.

¹⁵⁰ <http://www.verisign.com>.

¹⁵¹ WebTrust principles and criterias, version 2.0, page 63.

À ce niveau, il semble que les coûts reliés au programme WebTrust lui ait fait perdre du terrain face à ses concurrents. Bien que moins populaire, nous sommes d'avis que ce programme offre les meilleures garanties au consommateur puisqu'il est le seul à offrir une évaluation du site par un expert indépendant. De plus, l'entité certifiée paie pour une évaluation effectuée par un professionnel et non pas pour un droit de licence pour l'utilisation d'un sceau.

Bien entendu, il est beaucoup plus facile et moins dispendieux pour une entreprise de se procurer un sceau émis par TRUSTe ou BBBOnline. Le consommateur, quant à lui, ne saisit pas toujours l'implication ou la valeur des sceaux qui sont affichés sur les sites. Il y a donc lieu de s'interroger quant à savoir si c'est la simple présence d'un sceau affiché sur un site qui permet d'apporter cet élément de confiance qui manque encore lors des relations commerciales sur Internet. Il faut toutefois être conscient qu'à moyen ou long terme, une procédure moins stricte risque d'avoir un effet contraire à celui de bâtir la confiance si les internautes constatent que la certification octroyée trop facilement n'a aucune signification réelle.

B. Impacts de la certification

Si le but premier de la certification est d'assurer le tiers de la conformité d'un produit ou service à des critères déterminés, les impacts de ce geste sont quant à eux multiples, tant au niveau de la portée de la certification, de la responsabilité des divers intervenants et de ses impacts en matière de concurrence.

1. La portée de la certification

Comme nous l'avons expliqué tout au long de cette recherche, la certification n'est pas une assurance de portée absolue et encore moins une garantie. Elle a ses limites

et sa portée sera déterminée en fonction de divers éléments. De même, sa valeur sera proportionnelle à sa portée.

1.1 Le type de certification

La certification n'exige pas une évaluation absolue de tous les aspects d'un bien ou d'un service. Il existe plusieurs types de certification et toutes n'ont pas la même portée¹⁵². En fonction de ses objectifs et objets, la portée de la certification pourra être très limitée ou couvrir un large spectre¹⁵³.

Ainsi, à titre d'exemple, un type de certification peut ne s'attarder qu'à l'aspect sécuritaire d'un produit. D'autres iront plus loin en certifiant certaines spécifications d'un produit ou de processus d'entreprise. Enfin, sur le plus haut échelon, on retrouvera la certification de qualité. Bien qu'il ne s'agisse pas d'une garantie de satisfaction, on vise alors à certifier non plus la conformité à des spécifications mais un certain niveau de qualité. Il faut être conscient qu'il n'existe pas de cloison étanche entre les différents types de certification.

En matière de certification de sites Web commerciaux, la portée de la certification s'étudiera d'abord relativement aux objets couverts par la certification. À notre avis, le type de certification devrait être déterminé en fonction de la mission du site¹⁵⁴. Le rythme, le volume, le montant et la nature des transactions sont des facteurs à considérer.

Nous avons vu que les certifications offertes par plusieurs organismes se limitent à l'identification de l'entité commerciale dans le cadre des échanges. Celles qui nous intéressent plus et qui visent directement le site Web s'attarderont habituellement à

¹⁵² Voir à ce sujet : Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, à la page 3-47 et Alain Couret, Jacques Igalens et Hervé Penan, *La Certification*, Presses Universitaires de France, Paris, 1995, Collection Que sais-je ?, numéro 3006, page 86.

¹⁵³ Andrew K. Rae, Hans-Ludwig Hausen, Philippe Robert, *Software Evaluation for Certification, Principles, Practice and Legal Liability*, (1995), McGraw Hill Book Company, England, page 2.

¹⁵⁴ L'analogie avec les logiciels nous apparaît appropriée. Andrew K. Rae, Hans-Ludwig Hausen, Philippe Robert, *Software Evaluation for Certification, Principles, Practice and Legal Liability*, (1995), McGraw Hill Book Company, England, à la page 8.

la dimension sécuritaire du site et à la protection des renseignements personnels. Très peu vont au-delà de ces éléments jusqu'à certifier les pratiques commerciales de l'entreprise.

1.2 Les standards utilisés

Une fois établi le champ que couvre la certification visée, le niveau et la précision du standard appliqué auront un impact majeur sur la valeur de la certification qui en découle.

Or, en matière privée comme c'est actuellement le cas de la certification sur Internet, l'établissement des standards est laissé entièrement à la discrétion de l'organisme de certification.

Certains organismes exigeront ainsi la mise en place de normes dans l'entreprise sans en préciser la portée ou en évaluer la pertinence. C'est le cas par exemple lorsque l'existence d'une politique portant sur la protection des renseignements personnels est exigée sans que la portée de celle-ci ne soit précisée¹⁵⁵.

1.3 Le mode d'évaluation

Le mode d'évaluation de l'entité désirant obtenir la certification revêt une grande importance. Comme cette évaluation peut se faire au moyen de déclarations volontaires, de formulaires à remplir ou d'un audit de l'entreprise, le résultat final en matière de vérification pourra être très variable¹⁵⁶.

¹⁵⁵ Ceci est le cas de l'organisme TRUSTe qui exige l'existence et la mise en place sur le site d'une politique de confidentialité des renseignements recueillis sans en établir de portée obligatoire.

¹⁵⁶ Voir à ce sujet : Andrew K. Rae, Hans-Ludwig Hausen, Philippe Robert, *Software Evaluation for Certification, Principles, Practice and Legal Liability*, (1995), McGraw Hill Book Company, England, aux pages 20 et suivantes.

À ce sujet, un audit externe effectué par un tiers indépendant offre une meilleure garantie quant à la valeur du résultat final obtenu. Les risques de mission, ou carrément de fausse déclaration ou fraude de la part de l'entité cherchant à obtenir la certification en sont grandement amoindris.

En effet, si la certification apporte un certain avantage commercial à une entreprise, certaines d'entre elles seront peut-être tentées d'améliorer leur portrait dans le but d'obtenir un sceau pouvant être apposé sur leur site.

1.4 Le traitement de l'information

Une grande quantité d'information est recueillie dans le cadre du processus de certification. Celle-ci engendre à son tour de nouvelles informations lors de son traitement. Comme la certification vise des éléments clés d'une entreprise, l'information en question en est une de nature à avoir un impact sérieux sur les affaires de la candidate¹⁵⁷.

La question se pose donc quant à la manipulation et à l'utilisation de cette information recueillie et créée. Dans un contexte de certification privée, au cours duquel un organisme privé effectue l'évaluation de la candidate en conformité d'un contrat, il appert que l'information devrait être traitée de façon confidentielle. Pour l'organisme de certification, cette information n'est autre chose que des renseignements concernant un client, recueillis pour le traitement de son dossier.

Toutefois, si cette information est utile à l'organisme de certification pour décider d'accorder ou non celle-ci, elle semble tout aussi pertinente pour le tiers à qui l'on demande de faire confiance à la certification¹⁵⁸.

¹⁵⁷ Timothy-Stoltzfus Jost « *Confidentiality and Disclosure in Accreditation* », (1994) 57 *Law and Contemporary Problems*, 171.

¹⁵⁸ Timothy-Stoltzfus Jost, « *Confidentiality and Disclosure in Accreditation* », (1994) 57 *Law and Contemporary Problems*, 171, à la page 181.

Par ailleurs, notons que si l'information en question met à jour un risque pour le consommateur, il peut être du devoir de l'organisme de communiquer cette information, à défaut de quoi elle risque une part de responsabilité dans le dommage subi¹⁵⁹.

Il semble que sur un plan historique, ce type d'information ait été traité généralement de façon confidentielle en matière d'accréditation. Cette attitude reposait sur le fait que le processus visait d'abord et avant tout l'amélioration de l'entité¹⁶⁰. Tel n'est cependant pas la visée de la certification des sites Web.

Par ailleurs, les candidats à la certification ont sans doute intérêt à ce que certains types d'information demeurent confidentiels. Il s'agit d'établir un juste équilibre entre les deux. Somme toute, la divulgation, ou à tout le moins l'accessibilité à cette information, est de nature à augmenter la valeur de la certification octroyée.

1.5 Le mécanisme contractuel

Dans le cadre d'un processus de certification, divers mécanismes contractuels peuvent être employés.

Habituellement, l'entente prévoira le niveau de standard utilisé, le mode d'évaluation et la latitude dont disposent les certificateurs pour émettre ou non la certification.

Or, nous avons vu que certaines certifications constituent en fait des contrats de licence qui octroient un droit d'utilisation du sceau suivant certaines conditions.

¹⁵⁹ « [...] those who already possess risk information are under a duty to communicate it nonnegligently to strangers who, if so informed, could avoid harm to themselves. » Peter H. Schuck, « *Tort Liability To Those Injured By Negligent Accreditation Decisions* », (1994) 57 *Law and Contemporary Problems*, 185, à la page 196.

¹⁶⁰ Timothy-Stoltzfus Jost, « *Confidentiality and Disclosure in Accreditation* », (1994) 57 *Law and Contemporary Problems*, 171, à la page 171.

Dans d'autres cas, les dispositions contractuelles se limiteront à la partie concernant l'évaluation de l'entité ou, plus particulièrement, l'audit externe.

Si ces mécanismes semblent s'équivaloir en termes de résultats, on constate toutefois que l'entité certifiée paie des droits annuels pour la licence lui permettant d'apposer le sceau sur son site. En revanche, les frais imposés dans le cas du mécanisme contractuel se limitant à la portion d'évaluation de l'entité concernée s'élèvent aux frais de cette évaluation et non en termes de droit d'utilisation du sceau. On y perçoit une plus grande indépendance du certificateur qui se reflète alors dans la valeur de la certification.

1.6 Le statut du certificateur

Le statut du certificateur est un élément important dans la valeur que se verra attribuée la certification. En effet, l'obtention d'une certification d'un organisme jouissant d'un statut reconnu et d'une bonne réputation peut jouer « un rôle primordial dans le succès que connaîtra un produit ou un service »¹⁶¹. Incidemment, ceci aura une influence considérable dans le développement d'un système de certification efficace.

C'est la raison pour laquelle les organismes privés actuels investissent autant, sinon plus, dans la mise en marché de leur marque que dans l'évaluation des entreprises. L'objectif est de se faire connaître et d'accroître leur crédibilité. Ils font grand bruit du fait qu'une entreprise importante a adopté leur type de certification pour la reconnaissance qu'un tel geste peut lui apporter.

Dans le même sens, une attention particulière est remarquée dans la conception des sceaux qui ont tous une apparence presque « officielle » qui peut entraîner de la confusion chez le consommateur. Un auteur américain estime que les organismes

¹⁶¹ Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberespace*, Montréal, Les Éditions Thémis, 1997, à la page 3-49.

privés jouissent actuellement d'un statut, d'une crédibilité et d'une influence au-delà de ce qu'ils méritent¹⁶².

À ce sujet, l'indépendance du certificateur est un élément important lorsqu'il est question de fiabilité de la certification. Ainsi, un organisme privé est susceptible d'avoir des intérêts qui peuvent mettre en cause son impartialité dans le processus de certification¹⁶³. L'exemple le plus flagrant serait la situation où le certificateur exerce son activité dans un but lucratif. Il est donc important de soupeser le besoin d'expertise et l'absence de conflit d'intérêt¹⁶⁴.

Mis à part l'aspect pécuniaire, l'origine du certificateur et ses sources de motivation toucheront certainement sa crédibilité. Dans le cas de certificateurs privés, le fait qu'ils soient issus d'une coalition d'entreprise ou encore qu'ils soient commandités par des entreprises importantes d'un secteur influencera beaucoup la perception de la certification qui en découle, que ce soit dans le sens positif ou négatif.

De même, si le statut du certificateur est gouvernemental ou découle d'une délégation de l'État de quelque façon que ce soit¹⁶⁵, une certaine notoriété et crédibilité en transpirera. Toutefois, les contraintes géographiques des états pourraient devenir éventuellement un écueil à la valeur de la certification. En ce sens, l'endossement par une organisation internationale serait plus valable.

Finalement, il est important de rappeler que la confiance est un sentiment difficile à construire. Dans un milieu où les développements technologiques sont très rapides,

¹⁶² Clark C. Havighurst, « *The Place Of Private Accrediting Among The Instruments Of Government* » (1994) 57 Law and Contemporary problems, 1, à la page 4.

¹⁶³ Voir à ce sujet : Clark C. Havighurst, « *The Place Of Private Accrediting Among The Instruments Of Government* » (1994) 57 Law and Contemporary problems, 1, à la page 2.

¹⁶⁴ Cette question a été abordée en droit américain concernant le système d'accréditation en matière de soins de santé. Michael J. Astrue, « *Health care reform and the constitutional limits on private accreditation as an alternative to direct government regulation* », 57 Law and Contemporary Problems, 75.

¹⁶⁵ Cette méthode est fréquemment utilisée au États-Unis dans les domaines de l'éducation et de la santé. Voir à ce sujet : Jeffrey C. Martin, « *Recent Developments Concerning Accrediting Agencies in Postsecondary Education* », (1994) 57 Law and Contemporary Problems, 121; Matthew W. Finkin, « *The Unfolding Tendency In The Federal Relationship To Private Accreditation In Higher Education* », (1994) 57 Law and Contemporary Problems, 89; Michael J. Astrue, « *Health care reform and the constitutional limits on private accreditation as an alternative to direct government regulation* », 57 Law and Contemporary Problems, 75 ; Eleanor D. Kinney, « *Private Accreditation As A Substitute For Direct Government Regulation In Public Health Insurance Programs: When Is It Appropriate?* », (1994) 57 Law and Contemporary problems, 47.

il peut apparaître ardu de bâtir la confiance. Le certificateur est tout aussi important que le sceau ou le certificat. Or, les organismes de certification sont de nouvelles entités. Les plus anciennes ont émergé il n'y a pas plus de cinq ans. Certaines ont disparu ou changé de nom¹⁶⁶, d'autres les ont remplacées.

À quand la certification des organismes de certification ? Cette solution, qui peut paraître loufoque pour certains, a néanmoins déjà été utilisée¹⁶⁷.

1.7 La reconnaissance

La reconnaissance globale assure la stabilité et le développement de la certification. Elle s'inscrit dans la suite logique de la reconnaissance du statut du certificateur.

Non seulement la certification doit-elle être reconnue et apporter la confiance chez le consommateur, mais encore la reconnaissance doit s'étendre le plus loin possible.

Dans la réalité il ne sera pas question de reconnaissance de la certification mais plutôt de reconnaissance du certificateur. Dans le cas où celui-ci est reconnu par les industries d'un secteur d'activité donné ou encore par un gouvernement, la valeur de la certification alors émise s'en verra grandement augmentée. Dans certaines situations, la reconnaissance par le gouvernement est obligatoire. C'est le cas lorsque l'accréditation du certificateur est exigée par l'autorité gouvernementale¹⁶⁸.

Ainsi, la reconnaissance de la certification se fait par les entreprises d'un même secteur d'activité ou encore par le gouvernement. Il existe également un troisième type de reconnaissance qui est tout aussi important dans le cadre de commerce sur Internet.

¹⁶⁶ Par exemple, le programme TRUSTe s'appelait à l'origine « eTRUST » comme l'illustre l'article de Esther Shein, « *You can eTRUST us* », PC Week, 16 décembre 1996, vol. 13, n° 50, page E-1 ; Elizabeth Wasserman, « *Getting A Website Seal Of Approval* », San Jose Mercury News, 16 octobre 1996, page 1A.

¹⁶⁷ Voir à ce sujet : Clark C. Havighurst, « *The Place Of Private Accrediting Among The Instruments Of Government* » (1994) 57 Law and Contemporary problems, 1, à la page 10.

¹⁶⁸ Jean-Marie Ponthier, « La certification outil de la modernité normative », 30 (1996) *Dalloz-Sirey*, c. 355-360., page 360.

Le caractère intrinsèquement sans frontière de ce réseau rend nécessaire un mécanisme de certification couvrant la géographie la plus grande possible des entreprises et consommateurs auxquels il s'adresse. Ainsi, la reconnaissance réciproque des certificats émis par divers organismes sera très utile dans le cas d'Internet, comme ce fut le cas pour le marché européen¹⁶⁹. Bien entendu, cette reconnaissance ne saura apparaître d'un seul coup et peut donc se faire graduellement. Comme l'explique le professeur Couret dans le cas de la certification sur le marché européen :

« Il commence par la reconnaissance d'essai, d'audit puis de procédure de certification, la phase ultime étant la reconnaissance de marque de certification entre elles »¹⁷⁰.

La reconnaissance réciproque est également un moyen de limiter la concurrence qui s'instaure entre les organismes de certifications. Celle-ci peut s'avérer néfaste au consommateur en favorisant le magasinage des marques de certification, la diminution des coûts et, éventuellement, un certain laxisme dans l'application des standards¹⁷¹.

On réalise donc que la portée et la valeur des certifications peuvent varier de façon substantiellement importante de l'une à l'autre. Toutefois, l'essentiel du travail est axé sur l'apport de la confiance et non sur la communication d'information concernant l'objet, les standards ou les mécanismes utilisés.

Dans le but de simplifier la procédure, les consommateurs peuvent ainsi se trouver rassurés sans toutefois comprendre la portée de la certification qui est apposée sur un site Web. D'ailleurs, plus la procédure se veut fiable, de portée large et complète,

¹⁶⁹ Alain Couret, Jacques Igalens et Hervé Penan, *La Certification*, Presses Universitaires de France, Paris, 1995, Collection Que sais-je ?, numéro 3006, page 113.

¹⁷⁰ Alain Couret, Jacques Igalens et Hervé Penan, *La Certification*, Presses Universitaires de France, Paris, 1995, Collection Que sais-je ?, numéro 3006, page 114.

¹⁷¹ Voir à ce sujet : Clark C. Havighurst, « *The Place Of Private Accrediting Among The Instruments Of Government* » (1994) 57 *Law and Contemporary problems*, 1, aux pages 10 à 13.

plus elle est complexe et coûteuse. Elle met alors sa survie en péril puisque les entreprises risquent de se tourner vers un autre organisme de certification¹⁷².

Un élément ayant également un impact important sur la portée de la certification et que nous étudierons séparément est celui des responsabilités sous-jacentes à celle-ci.

2. Les responsabilités sous-jacentes

Les objectifs poursuivis par les divers intervenants au processus de certification sont variés. De même, l'octroi de la certification aura un impact sur les tiers qui percevront l'émission de la certification.

Dans ce contexte, des attentes peuvent être déçues et des litiges peuvent apparaître entre diverses parties et à différents niveaux. Les consommateurs et les entreprises candidates à la certification constituent les deux groupes à risque en ce qui a trait aux dommages éventuels découlant du processus et de l'octroi d'une certification¹⁷³.

Un acte tel que la certification engendre une série de conséquences légales pour l'organisme de certification, dont des responsabilités envers l'entité certifiée ou la candidate à la certification et les consommateurs. Précisons que nous nous limiterons ici aux conséquences civiles, sans aborder les incidences possibles sur le plan criminel.

La nature légale des obligations engendrées par la certification doit être examinée avant d'aborder la responsabilité, tant contractuelle que délictuelle, à l'égard de l'entité certifiée ou du consommateur.

¹⁷² Un bel exemple est le cas de la procédure de certification WebTrust, sans doute le processus le plus complet que nous ayons analysé dans la présente recherche. Toutefois, la certification WebTrust est à ce jour moins populaire que ses concurrents. Ceci semble le résultat de l'orientation de mettre l'accent sur la publicité et le marketing pour rassurer les consommateurs plutôt que sur la certification comme telle.

¹⁷³ Peter H. Schuck, « *Tort Liability To Those Injured By Negligent Accreditation Decisions* », (1994) 57 *Law and Contemporary Problems*, 185.

2.1 Nature de la relation entre le certificateur et le candidat

Tel que mentionné précédemment, l'ensemble des étapes entourant l'octroi de la certification s'inscrit dans le cadre d'un processus contractuel entre le candidat et l'organisme de certification.

À ce lien contractuel s'ajoute le fait que dans plusieurs cas, il y a « contamination » de la relation en raison du statut de commanditaire du programme de certification dont jouissent certains candidats. Cette situation est bien réelle en matière de certification par un organisme privé dans un milieu tel que Internet. Les commanditaires sont nombreux et représentent dans la majorité des cas des acteurs majeurs dans le milieu. Or, tous se prévaudront de la certification qu'ils commanditent¹⁷⁴. Le conflit d'intérêts apparaît alors indéniable¹⁷⁵.

Quant à la portée des obligations, mentionnons simplement que tant l'organisme de certification que le candidat ont une obligation réciproque, celle de collaborer de bonne foi¹⁷⁶. Les risques de fausses déclarations ou de fraudes de la part du candidat seront proportionnels au mode d'évaluation mis en place.

Dans le cadre de leur travail, les organismes de certification ont l'obligation d'agir équitablement surtout lorsque la certification émise confère un avantage commercial notable sur les concurrents¹⁷⁷. En raison de cet impact commercial et du fait que

¹⁷⁴ À titre d'illustration, l'annexe « C » donne la liste des commanditaires de l'organisme TRUSTe.

¹⁷⁵ Ce risque est d'ailleurs utilisé comme argument à l'appui de l'instauration d'un mécanisme public de certification : Geist, Michael, « *Consumer Protection and Licensing Regimes Review: The Implications of Electronic Commerce* », Janvier 2000, Rapport préparé pour le ministère de la Consommation et du Commerce, p. 12, disponible à : <http://aix1.uottawa.ca/~geist/mccrgeist.pdf> (consulté le 23 mars 2000).

¹⁷⁶ Article 1375 du *Code civil du Québec*. Le droit civil se distingue à ce niveau de la common law et de son concept de « caveat emptor ». Rappelons simplement que ce concept veut qu'il n'existe pas d'obligation de bonne foi entre les parties contractantes et que c'est à chacune d'entre elles de se renseigner adéquatement sur l'étendue de ces obligations. Voir à ce sujet : Louise Bélanger-Hardy et Aline Grenon, *Éléments de common law et aperçu comparatif du droit civil québécois*, Montréal, Carswell, 1997 ; et plus particulièrement dans le domaine de la certification : Andrew K. Rae, Hans-Ludwig Hausen, Philippe Robert, *Software Evaluation for Certification, Principles, Practice and Legal Liability*, (1995), McGraw Hill Book Company, England, aux pages 214 et 215. De plus, rappelons le principe de preuve selon lequel la bonne foi se présume toujours (article 2804 du *Code civil du Québec*).

¹⁷⁷ Ceci est particulièrement le cas en droit américain. Voir : Tedd Blecher, « *Products Standards and Certification Programs* », 46 (1980) *Brooklyn Law Review* 223, à la page 227 ; Jonathan T. Howe et Leland J. Badger, « *The Antitrust Challenge To Non-Profit Certification Organizations : Conflicts of Interest and a Practical Rule of Reason*

l'organisme privé de certification puisse se trouver en situation de conflit d'intérêt, le professeur Trudel rapporte que les tribunaux américains en sont venus à « imposer certaines obligations procédurales »¹⁷⁸, lesquelles sont assimilables à une forme d'obligation de bonne foi.

Finalement, l'obligation contractuelle du certificateur envers le candidat est limitée par le cadre que s'est fixé le type de certification choisi. C'est sans doute pourquoi ce cadre est défini si vaguement ou encore ne cible que certains aspects des affaires du candidat. À l'intérieur de ces paramètres, nous sommes d'avis que le certificateur s'engage à un résultat quant à l'attestation de conformité.

Aussi stricte qu'elle puisse paraître, cette obligation n'est pas si contraignante pour le certificateur, puisque ce dernier est libre d'établir les critères de la certification qu'il émet. De plus, la reconnaissance ou le refus de reconnaître la conformité aux critères n'est valable au moment de la certification.

2.2 Responsabilité face au certifié

La relation entre le certificateur et l'entité qui recherche, ou a obtenu la certification, étant de nature contractuelle, les principes de la responsabilité contractuelle leur sont donc applicables¹⁷⁹.

Le certificateur doit respecter ses engagements à l'égard du candidat à la certification. Si un contrat a été conclu, le certificateur doit suivre les standards stipulés et procéder à l'évaluation selon le mécanisme prévu à celui-ci.

Approach to Certification Programs as Industry-Wide Builders of Competition and Efficiency », (1982) 60 Washington University Law Quarterly 357, à la page 366.

¹⁷⁸ Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, à la page 3-51.

¹⁷⁹ Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, à la page 3-49.

L'objectif poursuivi par le candidat est clair : il s'agit d'obtenir la certification. Le rôle du certificateur, quant à lui, est de bien suivre le processus établi. Parfois, il peut avoir un intérêt financier à émettre la certification en raison du fait que c'est l'octroi du sceau qui lui procure une rémunération plutôt que l'évaluation de l'entité.

En théorie, rien ne garantit au candidat l'émission de la certification. Des litiges pourront donc survenir dans une situation où le certificateur refuse d'octroyer la certification à un candidat ou encore suite à la décision de retirer la certification déjà émise.

2.2.1 Le refus de certification

Les refus de certification peuvent apparaître à deux étapes du processus de certification. La première situation de refus survient dès les premières démarches du processus, soit lorsque l'entité candidate ne répond pas aux critères de qualification. La seconde se présente si l'évaluation effectuée s'est avérée insatisfaisante.

Au niveau des critères de qualification, on remarque que la plupart des organismes présents sur le marché refusent d'émettre une certification à un site Web « pour adultes ». À ce niveau, les certificateurs déclareront sans doute qu'ils sont libres d'établir une relation d'affaires avec qui ils le désirent. Toutefois, lorsqu'un tel service est offert à l'ensemble du public, le refus de traiter avec certains types de site ne doit pas s'avérer discriminatoire compte tenu des motifs de discrimination prohibés par la loi¹⁸⁰.

Quant au refus de certification suite à l'évaluation de l'entité, la question devra s'analyser à la lumière des critères établis et du mode d'évaluation effectué. Le candidat a une obligation de son côté, soit celle de collaborer avec le certificateur. Une fois son obligation remplie, c'est au certificateur qui refuse d'octroyer la certification de démontrer que le candidat a échoué l'évaluation. On remarque ici

¹⁸⁰ Article 10 de la *Charte des droits et libertés de la personne*, L.R.Q., c. C-12.

que les certificateurs se munissent habituellement d'un large pouvoir discrétionnaire dans leurs clauses contractuelles en stipulant que l'évaluation doit avoir démontré à leur satisfaction le respect des critères établis.

Un cadre de certification dont la partie contractuelle se limite à régir le mode d'évaluation du candidat donne une latitude plus grande encore au certificateur puisque aucune obligation contractuelle ne vient régir l'octroi de la certification.

2.2.2 Le retrait de certification

Une éventualité à prévoir au sein du mécanisme est le retrait de la certification émise. Elle constitue un élément essentiel à la crédibilité du processus.

Le mécanisme sera alors sensiblement le même que celui étudié précédemment. Le fardeau de démontrer que l'entité certifiée ne répond plus aux critères de certification incombera au certificateur ou à l'entité certifiée, selon le mécanisme contractuel existant entre les parties et le moment du retrait de la certification.

À titre d'exemple, la certification peut être de durée déterminée et ainsi exiger que l'entité renouvelle celle-ci à intervalle régulier. Dans un tel cas, le fardeau de se qualifier de nouveau incombe à l'entité¹⁸¹. En revanche, Le défaut de stipuler une durée à la certification fera en sorte que ce sera au certificateur de démontrer un changement de situation et que l'entreprise ne répond plus aux critères établis pour retirer celle-ci¹⁸².

La possibilité de révocation de la certification est un élément important de la crédibilité du processus. Elle semble toutefois peu exploitée à ce jour¹⁸³.

¹⁸¹ Voir par exemple le retrait de la certification TRUSTe à la compagnie MotherNature, commenté dans l'article suivant : Alex Lash, « TRUSTe Cracks the Whip », *The Standard*, 22 mars 2000, <http://www.thestandard.com/article/display/0,1151,13238,00.html> (consulté le 23 mars 2000).

¹⁸² En effet, c'est la partie qui prétend qu'un droit est nul, modifié ou éteint sur laquelle repose le fardeau de la preuve (Article 2803 du *Code civil du Québec*).

¹⁸³ Le comportement du certificateur TRUSTe est éloquent à ce niveau. Des critiques affirment que malgré des violations évidentes des règles de certification à deux occasions, l'organisme n'a pas retiré la certification émise. L'article suivant trace un portrait intéressant du comportement de l'organisme face aux certifiés en faute : Michelle Rafter, « *Trust or*

2.3 Nature de la relation entre le certificateur et le tiers

La nature du lien entre le certificateur et le tiers est plus difficile à identifier. D'emblée, notons qu'il n'existe pas de relation contractuelle directement entre eux. En effet, ils n'ont pas conclu de contrat et la certification ne saurait être assimilée à une promesse du fait d'autrui¹⁸⁴, à une stipulation pour autrui¹⁸⁵, ou même, à une assurance telle que définie par notre code civil¹⁸⁶.

S'il n'y a pas de contrat, la question est de savoir quelles sont les obligations entre eux s'il en existe et quelle en est la nature. De leur côté, les organismes de certification soutiennent toujours qu'ils ne donnent pas de garantie ou d'endossement des produits et services offerts par l'entité certifiée. Il n'en demeure pas moins que la certification constitue une affirmation quant à la conformité à certains critères. À cet égard, le certificateur pose un geste positif en octroyant une certification, geste qui est de nature à avoir un impact sur le comportement du consommateur.

Il existe un contrat entre le candidat et le certificateur, mais le tiers ne peut se prévaloir des règles établies entre ceux-ci en raison du principe de l'effet relatif des contrats¹⁸⁷. Néanmoins, comme le rappelle le juge Baudoin, le contrat produit quand même des effets envers les tiers. Ces effets ne proviennent toutefois pas du contrat lui-même, mais du fait juridique créé par le contrat et qui a un impact sur les tiers¹⁸⁸.

Bust? », The Standard, 6 mars 2000, <http://www.thestandard.com/article/display/0,1151,12445,00.html> (consulté le 23 mars 2000).

¹⁸⁴ Article 1443 du *Code civil du Québec*.

¹⁸⁵ Article 1444 et suivants du *Code civil du Québec*.

¹⁸⁶ Article 2389 du *Code civil du Québec*.

¹⁸⁷ Article 1440 du *Code civil du Québec* : « Le contrat n'a d'effet qu'entre les parties contractantes ; il n'en a point quant aux tiers, excepté dans les cas prévus par la loi. »

¹⁸⁸ Jean-Louis Baudouin et Pierre-Gabriel Jobin, *Les obligations*, 5^e édition, Cowansville, Les Éditions Yvon Blais, 1998, à la page 261.

En raison du fait que la certification est un acte qui se destine de façon ultime au consommateur, l'octroi de celle-ci engendre des effets directs à leur égard. Sans être de nature contractuelle, l'acte du certificateur n'en demeure pas moins un fait juridique dont les effets envers les tiers peuvent être source de responsabilité.

2.4 La responsabilité face aux tiers

La certification vise à accroître la confiance des consommateurs. Il ne faut donc pas se surprendre que la marque de certification ait créé certaines attentes de leur part et, dans certains cas, ait constitué un élément déterminant dans la décision d'effectuer une transaction. Ces derniers feront peut-être affaires avec une entreprise en raison du fait qu'une marque de certification est affichée sur le site et leur apporte un sentiment de confiance envers celle-ci.

La perception du public en regard de la certification s'apparente souvent à la garantie¹⁸⁹. C'est la conséquence logique du désir de vouloir bâtir la confiance. Pour ce faire, la certification doit avoir une signification réelle. Bien que les termes « certification » et « garantie » soient des concepts différents, il n'en demeure pas moins que la certification engendre des responsabilités, lesquelles sont essentielles à la constitution d'un sentiment de confiance.

Avant d'aborder la question de la responsabilité potentielle du certificateur, soulignons que le recours contre ce dernier n'est habituellement pas le premier réflexe du consommateur. Pourquoi ? Pour la simple raison qu'il n'y a pas, tel qu'expliqué précédemment, de lien contractuel entre le certificateur et le tiers. Or, en cas de difficulté avec une entreprise, le consommateur commencera par s'adresser à son cocontractant. Ainsi, le différend entre l'entreprise et le consommateur risque d'être plus aigu lorsque ce dernier se retourne vers le certificateur puisque cela

¹⁸⁹ Andrew K. Rae, Hans-Ludwig Hausen, Philippe Robert, *Software Evaluation for Certification, Principles, Practice and Legal Liability*, (1995), McGraw Hill Book Company, England, page 6.

démontre généralement que d'autres alternatives plus aisées se sont avérées inefficaces.

Dans ces cas, un consommateur insatisfait ou vivant des difficultés dans le cadre de sa relation avec l'entité certifiée pourrait se retourner vers le certificateur. Dans un tel cas, son recours ne reposera pas sur une base contractuelle, mais sur une base délictuelle, avec les différences qui en découlent au niveau du fardeau de la preuve¹⁹⁰.

Or, c'est au consommateur qu'incombe ce fardeau de la preuve¹⁹¹. Ainsi, pour s'attaquer au certificateur, le consommateur devra démontrer les éléments traditionnels, soit la faute de la part du certificateur, ensuite qu'il a subi un dommage à cette occasion et finalement le lien de causalité entre la faute commise et le dommage subi.

Traduit en terme certification, le premier élément à démontrer est que la difficulté vécue par le consommateur relève du cadre de la certification¹⁹². Si tel n'est pas le cas, le certificateur rejettera d'emblée les doléances qui lui seront adressées¹⁹³. Celui-ci aura cependant avantage à utiliser une marque ou un sceau illustrant bien le champ d'application de la certification, ou encore à rendre facilement accessible les paramètres de celle-ci. À défaut, les concepts de fausse représentation ou encore d'attente raisonnable pourraient jouer contre lui.

Par la suite, la preuve de la faute, notion intimement liée au concept de responsabilité délictuelle, doit être apportée. En matière de certification, la faute consistera à avoir accordé à tort la certification hors des paramètres établis ou encore à l'avoir laissée à l'entité alors que les critères n'étaient plus respectés. Le

¹⁹⁰ Article 1457 du *Code civil du Québec*.

¹⁹¹ Article 2803 du *Code civil du Québec*.

¹⁹² Il est question ici de l'objet de la certification et de ses limites temporelles si c'est le cas.

¹⁹³ À ce niveau, l'organisme de certification TRUSTe semble porté à rejeter les plaintes sur cette bases. À titre d'exemple, les plaintes contre le certifié RealNetworks en novembre 1999 ont ainsi été rejetées au motif que la violation de la vie privée résultait d'un programme et non du site Web. En conséquence, TRUSTe a jugé que la plainte tombait hors de sa juridiction... Pour une analyse plus complète de cette question, voir : Michelle Rafter, « *Trust or Bust?* », *The Standard*, 6 mars 2000, <http://www.thestandard.com/article/display/0,1151,12445,00.html> (consulté le 23 mars 2000).

consommateur doit donc démontrer que la certification émise est inexacte, peu importe si l'inexactitude repose sur une évaluation inadéquate, incomplète ou incorrecte du certificateur, ou encore une fausse déclaration de l'entité certifiée¹⁹⁴. Les paramètres et limites temporelles de la certification prennent une importance considérable à ce niveau.

Si la certification est erronée, il convient alors d'évaluer le dommage, qui consistera dans la perte subie par le consommateur. En droit américain, il semble que la nature de la certification ait une incidence sur le fardeau de la preuve et la responsabilité de du certificateur¹⁹⁵.

Finalement, l'élément le plus difficile à prouver sera de démontrer le lien de causalité, à savoir que n'eut été de la certification, le consommateur n'aurait pas transigé avec le site Web concerné. Or, le lien entre la certification d'un site Web et l'acte de transiger par le biais de celui-ci en raison de la certification du site nous apparaît très difficile¹⁹⁶.

De leur côté, les organismes de certification pourront exercer des recours en garantie contre l'entité certifiée. Les certificateurs se prémunissent contre les conséquences des réclamations des consommateurs en stipulant dans les textes contractuels qui les lient aux entités certifiées que ces dernières s'engagent à les tenir indemnes de toute réclamation qui leur serait adressée en raison de la certification du site. De telles clauses n'ont pas pour effet d'empêcher les recours des consommateurs à leur égard, mais de leur donner la possibilité de réclamer à leur tour de l'entité qui n'aurait pas dû obtenir la certification. Elles nous apparaissent de portée quelque peu limitée sur le plan pratique. En effet, la recherche de la responsabilité poursuit de façon ultime un objectif de compensation par le consommateur. Dans les faits, celui-ci

¹⁹⁴ Voir à ce sujet : Andrew K. Rae, Hans-Ludwig Hausen, Philippe Robert, *Software Evaluation for Certification, Principles, Practice and Legal Liability*, (1995), McGraw Hill Book Company, England, à la page 213.

¹⁹⁵ Peter H. Schuck, « *Tort Liability To Those Injured By Negligent Accreditation Decisions* », (1994) 57 *Law and Contemporary Problems*, 185, à la page 193.

¹⁹⁶ Le même raisonnement développé en matière d'accréditation est à notre avis applicable : « Consumers' claims of negligent accreditation are likely to be barred at the threshold by a narrowly defined scope of legal duty for accreditors and by a robust requirement that consumers show detrimental reliance on, and increased risk from, the accrediting

s'adressera naturellement en premier lieu à l'entité avec laquelle il a transigé. Il se retournera contre le certificateur pour des raisons de capacité financière, comme par exemple s'il appert que l'entité certifiée est insolvable. Dans ce dernier cas le certificateur sera à risque puisqu'il aura perdu ses recours contre l'entité certifiée.

Somme toute, il semble peu probable que la responsabilité de l'organisme de certification face au tiers soit retenue, et ce, tant en droit civil qu'en common law¹⁹⁷. En vue de limiter leur responsabilité, les organismes de certification ont toutefois intérêt à bien indiquer les paramètres et limites de la certification de même que la date d'évaluation de l'entité certifiée.

Au surplus, pour que le mécanisme de certification de site Web soit efficace, il devra cependant prévoir des modes de résolution des conflits, à la fois accessibles et peu coûteux aux consommateurs.

2.5 La résolution des conflits

Il n'est pas question ici de la résolution des conflits par voie judiciaire. En fait, le processus de certification a entre autres pour objectif d'éviter le recours aux tribunaux. Il s'agit d'une forme d'autoréglementation qui vise à pallier l'intervention de l'État.

De plus, la voie judiciaire se prête mal à la résolution des conflits de petites sommes ou mettant en présence des intervenants situés dans des juridictions différentes. Ainsi, pour que la certification ait une utilité concrète, elle doit prévoir un

decision. », Peter H. Schuck, « *Tort Liability To Those Injured By Negligent Accreditation Decisions* », (1994) 57 *Law and Contemporary Problems*, 185, à la page 196.

¹⁹⁷ Nous sommes d'avis que l'on peut faire une analogie avec l'accréditation à ce niveau : « At present, the risk of tort liability for accreditors appears to be very low. » « In order for consumers to succeed in this endeavor, however, the courts would have to impose new, more expansive liabilities. [...] it seems unlikely that this will occur in the near future. », Peter H. Schuck., « *Tort Liability To Those Injured By Negligent Accreditation Decisions* », (1994) 57 *Law and Contemporary Problems*, 185, aux pages 187 et 196.

mécanisme de résolution des conflits pouvant survenir entre l'entité certifiée et ses consommateurs.

Si le conflit porte sur le processus ou l'octroi de la certification, il se peut que le recours aux tribunaux soit la seule avenue possible. En revanche, le litige qui concerne l'objet ou les effets de la certification pourra se résoudre au moyen de modes alternatifs de résolution des conflits, ce dont il est question ici.

Sans que la certification elle-même soit en cause, le différend doit se situer dans le cadre de la certification. Il doit porter sur l'un des éléments ayant fait l'objet de la certification. Le mécanisme proposé est un arbitrage entre les parties. Dans ces circonstances, le certificateur agit généralement comme arbitre¹⁹⁸.

Le principal défi auquel font face les certificateurs réside dans les importantes limites de leur pouvoir en matière de sanctions. Les organismes privés de certification ne jouissent pas des mêmes possibilités que les autorités législatives en cette matière¹⁹⁹.

La force contraignante du processus envers l'entité certifiée découle du caractère contractuel de la relation entre le certificateur et l'entreprise²⁰⁰. De plus, le meilleur atout dont dispose l'organisme de certification est l'impact important que peut avoir sa certification dans un marché. Les organismes misent beaucoup sur la force dissuasive à l'endroit des certifiés en créant un registre des plaintes. Le certificateur peut également inviter les internautes à lui adresser directement leurs doléances envers un certifié²⁰¹.

¹⁹⁸ Cet élément soulève d'emblée des interrogations concernant l'impartialité de l'arbitre. Des systèmes de résolution de conflits faisant appel à des tiers indépendants pourraient s'avérer plus adéquats dans ce rôle. Voir à ce sujet le Cybertribunal, <http://www.cybertribunal.org>, qui a toutefois cessé ses opérations ; Eresolution, <http://www.eresolution.ca>, et SquareTrade, <http://www.squaretrade.com> aux États-Unis.

¹⁹⁹ Clark C Havighurst, « *The Place Of Private Accrediting Among The Instruments Of Government* » (1994) 57 *Law and Contemporary problems*, 1, à la page 3.

²⁰⁰ Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, à la page 3-48.

²⁰¹ Voir par exemple à ce sujet le mécanisme « Watchdog » du certificateur TRUSTe.

Les certificateurs ne travaillent cependant pas uniquement au niveau du certifié mais également au niveau du consommateur en invitant ce dernier à entrer en contact directement avec l'entreprise pour tenter de régler le conflit. Si une telle procédure échoue, l'arbitrage mentionné précédemment peut se révéler un moyen efficace de règlement du conflit.

Force nous est de constater toutefois les lacunes de ces mécanismes. En effet, le certificateur peut donner l'illusion de jouer un rôle de juge et partie puisqu'il a déjà procédé à une évaluation de l'entité certifiée. De même, le certificateur n'a pas l'autorité pour condamner une partie au paiement d'une somme d'argent ou à poser un geste particulier tel la correction de dossier ou l'envoi de marchandise. Or, c'est précisément ce genre de remède que recherche le consommateur.

Actuellement, le milieu mise donc beaucoup sur la bonne volonté des parties et le fait que les entreprises désirant s'implanter dans ce nouveau marché ont intérêt à soigner leur image et à développer une bonne relation avec leur clientèle.

Malgré son obligation de résultat, le certificateur est somme toute peu au risque dans le processus de certification. En effet, le seul résultat promis est celui de la conformité à des critères établis. Si le refus ou le retrait de la certification peut engendrer un litige entre le certificateur et le candidat à la certification, il s'agit d'un risque relativement faible pour le certificateur.

De même, face au consommateur, le lien entre le dommage subi par ce dernier et la certification du site Web apparaît difficile à prouver. Finalement, le certificateur a tendance à se placer davantage dans la position d'un médiateur que d'une cible à conflits.

La certification est un outil très utile pour les nouveaux marchés, surtout lorsqu'elle comporte la caractéristique d'être internationale. Elle apporte cet élément essentiel de confiance qui pourrait normalement prendre des années à bâtir. Elle peut donc

devenir un enjeu important, notamment dans un milieu tel que celui-ci où la concurrence est très féroce.

3. Le droit de la concurrence

Les systèmes ouverts favorisent la concurrence entre entreprises. Le marché y est plus étendu et le nombre d'entreprises également.

Internet est l'exemple ultime du système ouvert. Sans frontières géographiques et avec des gouvernements qui osent peu réglementer le commerce qui s'y effectue, la concurrence y atteint des niveaux extrêmement élevés. Ceci se reflète alors dans la pugnacité des entreprises à défendre ou vouloir accroître leur part de marché.

La certification a des impacts importants sur la concurrence, impacts qui peuvent être de la favoriser ou parfois de la limiter.

3.1 Effets de la certification sur la concurrence

Une étape incontournable du processus de certification est l'établissement de standards. Or, la mise en place de standards poursuit indirectement l'objectif de favoriser la concurrence puisqu'elle permet de comparer les biens et services et ainsi d'accroître le libre échange de ceux-ci²⁰².

La certification, quant à elle, va au-delà de l'application de standards ou de normes. Il s'agit alors d'une assurance concernant la conformité à des critères. La certification fait donc davantage que faciliter les comparaisons, elle facilite le libre

²⁰² Jean-Baptiste Racine, « Normalisation, certification et droit de la concurrence », page 148.

commerce²⁰³ et procure un avantage commercial certain à l'entreprise qui en bénéficie²⁰⁴. Comme l'explique le professeur Couret :

« La certification vise d'abord et avant tout à mieux vendre, en apportant au marché la preuve objective émanant d'un organisme indépendant, que le produit ou service proposé, ou l'organisation qualité de l'entreprise, dispose effectivement de caractéristiques et performances propres à répondre aux besoins des clients. La certification procure un avantage commercial à celui qui en dispose par rapport à ceux qui ne peuvent s'en prévaloir. La certification, qui s'appuie sur des résultats d'essais et de contrôle, ajoute la confiance liée à l'intervention systématique d'un organisme tiers, indépendant, qui exerce en outre une surveillance dans le temps du maintien de la conformité »²⁰⁵.

Sans nier cet aspect de la question, certains soulignent toutefois que les standards et la certification peuvent restreindre la compétition en raison des limites qu'ils imposent sur les entreprises²⁰⁶. Il peut s'agir tant des contraintes économiques pour obtenir la certification que des contraintes des standards eux-mêmes.

Dans le même esprit, les standards de fait développés dans des secteurs d'activité peuvent constituer une menace à cette concurrence. La même situation se présente en matière d'accréditation. Bien que se basant sur le droit américain, l'extrait suivant résume bien la situation sur cette question :

« The adoption and application of quality standards by industry group can, and in most instances does, enhance competition and promote efficiency by clarifying and informing choices that market actors must make. But private accrediting may sometimes enable special interests in an industry to limit the

²⁰³ Andrew K. Rae, Hans-Ludwig Hausen, Philippe Robert, *Software Evaluation for Certification, Principles, Practice and Legal Liability*, (1995), McGraw Hill Book Company, England, à la page 6.

²⁰⁴ Voir à ce sujet : Jonathan T. Howe et Leland J. Badger, « *The Antitrust Challenge To Non-Profit Certification Organizations : Conflicts of Interest and a Practical Rule of Reason Approach to Certification Programs as Industry-Wide Builders of Competition and Efficiency* », (1982) 60 *Washington University Law Quarterly* 357.

²⁰⁵ Alain Couret, Jacques Igalens et Hervé Penan, *La Certification*, Presses Universitaires de France, Paris, 1995, Collection Que sais-je ?, numéro 3006, page 10.

²⁰⁶ Kees Stuurman, « *Legal Aspects of Standardization and Certification of Information Technology and Telecommunications* », page 88.

independence of individual competitors or to deny desirable options to consumers. »²⁰⁷

Il faut également noter que la certification, ou plutôt la marque de certification obtenue, peut être considérée comme une forme de publicité²⁰⁸. Il s'en suit que les principes de droit relatif à la publicité seraient applicables en matière de marque de certification.

3.2 L'impact des standards *de facto*

Les standards *de facto* sont des standards développés par une entreprise ou un regroupement d'entreprises d'un secteur déterminé. À l'instar des standards publics, l'accessibilité à ceux-ci peut donc être limitée. Pour certains, de tels standards créent une situation dangereuse qui s'apparente à un effet de monopole²⁰⁹.

En effet, le fait que les membres d'une industrie se réunissent et s'accordent pour élaborer des standards sur lesquels ils garderont le contrôle suscite des interrogations légitimes quant à l'impact sur la concurrence et le risque de donner naissance à une situation monopolistique²¹⁰.

Ce scénario n'a rien de nouveau. C'est l'histoire trop connue du grand qui réalise qu'il est en position de force et qui décide d'imposer ses règles du jeu :

« Des entreprises en position dominantes sur un marché ont parfois la possibilité d'imposer à leurs concurrents les standards

²⁰⁷ Clark C. Havighurst et Peter M. Brody, « *Accrediting and the Sherman Act* », (1994) 57 *Law and Contemporary Problems*, 199, à la page 200.

²⁰⁸ Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, à la page 3-51.

²⁰⁹ Kees Stuurman, « *Legal Aspects Of Standardization And Certification In Information Technology And Telecommunication : An Overview* », dans Kaspersen, HWK et A. Oskamp, *Amongst Friends in Computer Law : a Collection of Essays in remembrance of Guy Vanderberghe*, 1990, Kluwer Law and Taxation Publishers, Deventer, Hollande, page 75 à 91.

²¹⁰ Les américains sont particulièrement sensibles à ce genre de question. Voir : Clark C. Havighurst et Peter M. Brody, « *Accrediting and the Sherman Act* », (1994) 57 *Law and Contemporary Problems*, 199.

qu'elles ont elles-mêmes élaborés, autrement dit des normes de fait. »²¹¹

Or, le secteur informatique et des technologies de l'information est très sensible à l'imposition de telles normes étant donné qu'il s'agit d'un secteur relativement nouveau et à croissance très rapide dans lequel nous retrouvons des acteurs majeurs qui côtoient de petites entreprises en développement.

Certaines entreprises iront plus loin et tenteront de protéger les standards développés par un droit d'auteur²¹² et de protéger leur sceau de certification au moyen d'une marque de commerce²¹³. Cela a pour effet de restreindre considérablement l'accès à la certification, ce qui peut avoir des impacts négatifs sur la concurrence.

Les standards de fait sont en réalité ce qui se rapproche le plus de l'autoréglementation recherchée par le mécanisme de certification. Les normes sont développées directement par une industrie ou un secteur d'activité. Sans pouvoir réglementaire, les entreprises ne peuvent théoriquement imposer directement leurs standards. Toutefois, si le standard prend trop d'importance et devient un élément incontournable pour les entreprises d'un secteur d'activité, c'est la concurrence qui en souffrira.

La certification des sites Web peut potentiellement porter sur des éléments si variés qu'il nous apparaît impossible pour des entreprises d'un secteur d'élaborer et de s'approprier des normes de fait. À ce sujet, mentionnons simplement qu'une norme telle TRUSTe est précisément développée par un ensemble d'acteurs majeurs du secteur des technologies de l'information qui agissent à titre de commanditaires²¹⁴.

²¹¹ Jean-Baptiste Racine, « *Normalisation, certification et droit de la concurrence* », (1998) 1 Revue Internationale de Droit Économique 147, à la page 150.

²¹² Kees Stuurman, « *Legal Aspects Of Standardization And Certification In Information Technology And Telecommunication : An Overview* », dans Kaspersen, HWK et A. Oskamp, *Amongst Friends in Computer Law : a Collection of Essays in remembrance of Guy Vanderberghe*, 1990, Kluwer Law and Taxation Publishers, Deventer, Hollande, page 75, à la page 42.

²¹³ Kees Stuurman, « *Legal Aspects Of Standardization And Certification In Information Technology And Telecommunication : An Overview* », dans Kaspersen, HWK et A. Oskamp, *Amongst Friends in Computer Law : a Collection of Essays in remembrance of Guy Vanderberghe*, 1990, Kluwer Law and Taxation Publishers, Deventer, Hollande, page 75, à la page 85.

²¹⁴ Voir l'annexe C.

De plus, il est certain que des normes portant sur les pratiques commerciales pourront difficilement faire l'objet d'une appropriation par une entreprise.

Le danger se situe davantage au niveau du sceau de certification. Un tel sceau largement reconnu et ayant acquis une notoriété suffisante pourra être protégé et peut-être même accaparé par certains acteurs de l'industrie. C'est là qu'un tort considérable peut être causé à la concurrence.

Bien entendu, des règles ont été mises en place par les gouvernements pour assurer une saine présence de la concurrence. Sur internet, celles-ci se heurtent toutefois à la difficulté de régir le réseau ouvert. De plus, les règles visant à régir la concurrence ne s'attaquent habituellement pas à la standardisation et à la certification qui sont normalement considérées comme des facteurs favorisant la concurrence.

Ainsi, au Canada, la *Loi sur la concurrence*²¹⁵ donne un encadrement aux règles en matières de commerce. Sa partie VI porte sur les infractions relatives à la concurrence. Or, l'appropriation de standards et de sceaux de certification par un groupe d'entreprise pourrait entrer dans la définition de complot au sens de cette loi et, par conséquent, constituer une infraction. En effet, la loi prohibe tout accord ou coalition qui a pour effet pour restreindre indûment la concurrence ou lui causer un préjudice indu²¹⁶.

De même, comme l'exprime le professeur Trudel :

« Constituerait une pratique déloyale le processus de certification fondé sur des standards restrictifs et non pertinents ayant pour effet d'exclure des produits équivalents par ailleurs fonctionnels. »²¹⁷

²¹⁵ L.R.C., c. C-34.

²¹⁶ Article 45 (1), *Loi sur la concurrence*, L.R.C., c. C-34. Toutefois, cette loi prévoit spécifiquement certains moyens de défense, dont notamment le fait qu'une association d'intérêts, un accord ou un arrangement se rattache exclusivement à la définition de normes de produits (article 45 (3), *Loi sur la concurrence*, L.R.C., c. C-34).

²¹⁷ Pierre Trudel, France Abran, Karim Benyekhlef, Sophie Hein, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997, à la page 3-49. Voir également, Blecher, Tedd, « *Products Standards and Certification Programs* », 46 (1980) *Brooklyn Law Review* 223, à la page 224.

Une manière plus subtile de procéder est pour les grandes entreprises d'imposer des standards qu'elles seront seules à pouvoir respecter²¹⁸.

Si la non intervention des gouvernements et organismes internationaux poursuit des objectifs louables, il faut garder à l'esprit que l'imposition de standards de faits comporte des risques importants pour l'avenir de la concurrence sur Internet en limitant l'accès à la certification.

La meilleure façon de contrer ce danger est peut-être de favoriser la concurrence entre les organismes de certification eux-mêmes. Internet étant un terrain fertile à l'apparition de nouvelles industries, le domaine de la certification n'y échappe pas et la concurrence s'installe rapidement, même entre les organismes de certification. Trop de concurrence à ce niveau nuira cependant à la reconnaissance de la certification.

3.3 L'imposition d'un standard officiel

L'alternative au standard *de facto* est d'instaurer un standard officiel. Les conséquences sont cependant nombreuses sur le plan légal.

D'abord, la certification sur Internet est actuellement un acte privé, pris en charge par le secteur privé. Les standards sont élaborés par celles-ci et il n'y a pas d'accréditation ni d'endossement des organismes de certification par l'État. La mise en place de standards officiels importerait un caractère public à la procédure.

L'adoption de standards officiels comporte également des avantages notables. Les normes seraient plus uniformes et ne varieraient plus d'un organisme à l'autre (bien qu'elles pourraient varier d'un état à l'autre). Le consommateur serait sans doute rassuré par la présence étatique. Sans être nécessairement meilleures, les normes

²¹⁸ Jean-Baptiste Racine, « *Normalisation, certification et droit de la concurrence* », (1998)1 Revue Internationale de Droit Économique 147, à la page 151.

atteindraient plus facilement un seuil minimal acceptable, ce qui n'est pas toujours le cas avec les organismes privés.

D'un autre côté, s'il est imposé par un gouvernement se trouvant en situation dominante sur ce marché, on risque de se retrouver dans une situation similaire au standard *de facto* avec les risques que cela comporte.

Il nous apparaît qu'en raison de la structure décentralisée du réseau Internet et de son caractère international, le standard officiel soit, à tout le moins pour l'instant, difficile à mettre en place et donc peu adapté aux besoins pressants du commerce sur Internet.

Il est donc important que les standards et le mécanisme de certification dans son ensemble soient accessibles à tous, y compris aux petites entreprises. Un organisme supra national ou même un organisme privé sans but lucratif et ayant suffisamment d'indépendance face aux grandes entreprises pourrait jouer un rôle adéquat à ce niveau.

CONCLUSION

En matière d'échanges commerciaux, nous sommes dans une période de changements rapides en raison de l'influence de nouvelles politiques, de l'émergence de nouvelles technologies ainsi que de nouveaux marchés, dont Internet constitue sans doute l'élément le plus important.

Actuellement, les gouvernements ont tendance à prendre leurs distances quant à l'option d'intervenir trop vigoureusement relativement à une réglementation du commerce sur Internet. Les autorités publiques préfèrent laisser ce type de commerce prendre son envol et se stabiliser avant de succomber à la tentation de légiférer et de risquer de mettre en péril son développement rapide.

Dans l'intervalle, il y a des possibilités intéressantes d'autoréglementation de l'industrie sur ce marché. Même s'il est en plein essor, celui-ci risque toutefois d'atteindre rapidement des limites si les entreprises n'arrivent pas à rassurer les consommateurs sur la fiabilité des échanges commerciaux.

Pour bâtir cette confiance, la certification apparaît comme une mesure toute indiquée. Elle doit être précédée par l'instauration de standards adaptés et rigoureux pour ouvrir davantage le marché et rendre possible l'évaluation et la comparaison des produits et services offerts. La certification vient la compléter en donnant une assurance de conformité à certains critères. Ces possibilités sont décrites de façon intéressante dans le passage suivant :

« Dans ce cadre, la certification constitue pour les consommateurs un appréciable outil d'identification de la qualité des produits et un puissant vecteur de promotion pour les producteurs. »²¹⁹

²¹⁹ Alain Couret, Jacques Igalens et Hervé Penan, *La Certification*, Presses Universitaires de France, Paris, 1995, Collection Que sais-je ?, numéro 3006, à la page 118.

Les consommateurs trouvent leur compte en obtenant une information plus adéquate et plus complète sur les entreprises avec lesquelles ils désirent transiger. Les entreprises, quant à elles, peuvent utiliser les standards développés et la certification pour supprimer les barrières commerciales et s'ouvrir à de nouveaux marchés.

Les standards doivent cependant demeurer accessibles à toutes les entreprises dans le but d'éviter une concentration de l'avantage commercial conféré par la certification à un groupe d'entreprises déterminé. De même, si l'industrie est incapable de se bâtir des règles accessibles et uniformes, la tentation d'intervenir des autorités gouvernementales s'en trouvera d'autant augmentée.

Il existe donc une dualité d'intérêts entre, d'une part, la nécessité d'avoir des standards menant à la certification les plus universels, uniformes et accessibles possibles et, d'autre part, que ces standards ne soient pas issus d'une autorité étatique et demeurent entre les mains de l'industrie. Il s'agit là du plus grand défi pour les acteurs de ce nouveau marché.

L'intégration des standards dans une réglementation ou une législation risquerait de devenir un frein à l'accessibilité globale de la certification des sites Web. Une organisation internationale pourrait sans doute donner de bons résultats, dans la mesure où elle dispose de suffisamment d'autonomie, tant face à l'industrie qu'au gouvernement pour établir ces standards.

Quant à la certification, de nombreux organismes se sont d'ores et déjà lancés dans cette aventure. Il s'agirait ainsi davantage d'établir un système de reconnaissance réciproque ou d'évaluation de la portée de la certification émise. Une certification de qualité devra disposer de certaines caractéristiques telles que :

- être basée sur des standards harmonisés, reconnus et accessibles à tous, qu'il s'agisse de standards officiels ou de standards *de facto*. Dans le cadre de

standards *de facto*, les droits sur ceux-ci, s'il en existe, devront avoir été aliénés à l'ensemble de l'industrie.

- demeurer une mesure accessible à l'ensemble des industries dans le secteur. Elle ne doit donc pas se baser sur des standards impossibles à atteindre ou encore comporter une charge économique excessive rendant son obtention illusoire pour les petites entreprises.
- le processus d'évaluation est effectué par un tiers indépendant. Idéalement, il devrait être effectué au moyen d'un audit externe.
- communiquer l'objet et la portée de la certification au consommateur. La marque de certification, certificat ou sceau, devrait faire état de la portée et des limites de l'évaluation effectuée de la certification octroyée.
- comporter un système de reconnaissance réciproque des certifications effectuées par divers organismes dans le but d'éviter la multiplication des sceaux susceptible de confondre les consommateurs. Une spécialisation de ceux-ci pourrait apparaître comme une solution avantageuse, certains sceaux se préoccupant de la protection des renseignements personnels tandis que d'autres pourraient porter plutôt sur la sécurité.
- Finalement, les méthodes de résolution des conflits devront être revues et corrigées pour être plus accessibles aux consommateurs et surtout donner une totale apparence d'impartialité, ce qui ne semble pas être le cas présentement. Une autorité centrale pour l'arbitrage de tels conflits ou un tiers organisme²²⁰ pourrait convenir à cet effet.

²²⁰ Comme par exemple l'initiative du Cybertribunal, <http://www.cybertribunal.org>, qui a toutefois cessé ses opérations ; Eresolution, <http://www.eresolution.ca>, et SquareTrade, <http://www.squaretrade.com>, récemment retenu par la compagnie Ebay pour la résolution de ses conflits en ligne (Il est intéressant de noter que le site SquareTrade est lui-même certifié par TRUSTe). Voir également : John Roemer, « Site for Sore Customers SquareTrade partners with eBay to resolve disputes online », 29 mars 2000, <http://interactive.wsj.com/articles/SB953582315197322396.htm> (consulté le 29 mars 2000).

La certification est donc susceptible d'accroître la confiance des consommateurs quant à l'information et aux offres qu'ils retrouvent sur les sites Web et ainsi de les inciter davantage à conclure une transaction commerciale sur Internet. Toutefois, les standards qui sous-tendent la certification et les qualités que doit comporter celle-ci ne se retrouvent pas actuellement dans les systèmes de certification en place.

Par ailleurs, les consommateurs n'ont pas accès à l'information à laquelle ils ont droit et ne sont pas en mesure de juger de la valeur de la certification qu'ils perçoivent sur un site. Si l'industrie veut faire la preuve de sa capacité à s'autoréglementer et à offrir des marques de confiance aux consommateurs, elle devra améliorer ses mécanismes de certification en conséquence.

BIBLIOGRAPHIE

Ouvrages généraux

Ouvrages et articles sur le droit de l'internet

Ouvrages et articles sur le commerce électronique

- a) Le commerce électronique en général
- b) La sécurité dans le commerce électronique
- c) L'échange des consentements
- d) Les mécanismes de paiement
- e) La protection des consommateurs

Ouvrages et articles sur la certification et les standards

Ouvrages et articles sur l'audit

Organismes de certification de sites Web

Organismes divers

OUVRAGES GÉNÉRAUX

Baudouin, Jean-Louis et Patrice Deslauriers, *La responsabilité civile*, 5^e édition, Cowansville, Les Éditions Yvon Blais, 1998.

Baudouin, Jean-Louis et Pierre-Gabriel Jobin, *Les obligations*, 5^e édition, Cowansville, Les Éditions Yvon Blais, 1998.

Louise Bélanger-Hardy et Aline Grenon, *Éléments de common law et aperçu comparatif du droit civil québécois*, Montréal, Carswell, 1997.

Berryman, Jeffrey B. et al., *Remedies, Cases and Materials*, 3rd Ed., 1997, Emond Montgomery Publications Limited, Toronto.

Carbonnier, Jean, *Droit civil, t. 4, Les obligations*, 20^e édition, Paris, Presses Universitaires de France, 1996.

Fleming, John G., *The law of Torts*, 7th Ed., 1987, The Canada Law Book Company Limited, Agincourt, Ontario.

Fridman, Gerald H. L., *The law of Contract in Canada*, 2nd Ed., 1986, Carswell, Toronto.

L'Heureux, Nicole, *Droit de la consommation*, 4^e édition, Cowansville, Les Éditions Yvon Blais, 1993.

Linden, Allen M., *Canadian Tort Law*, 6th Ed., Butterworths, Toronto.

Pitch, Harvin D. And Snyder, Ronald M., *Damages for Breach of Contract*, 2nd Ed., 1999, Carswell, Scarborough, Ontario.

OUVRAGES ET ARTICLES SUR LE DROIT DE L'INTERNET

Bensoussan, Alain, « Internet, Aspects juridiques », (1996), Hermès, Paris.

Edwards, Lilian, Charlotte Waelde, *Law and the Internet, Regulating Cyberspace*, (1997), Hart Publishing, Oxford, Royaume Uni.

Gahtan, Alan, Kratz, Martin P.J., Mann, J. Fraser, *Internet Law, A Practical Guide For Legal And Business Professionnal*, 1998, Carswell, Canada.

Gaskin, James E., *Corporate Politics and the Internet*, (1997), Prentice Hall Printers, Upper Saddle River, USA.

Hance, Olivier, Suzan Dionne-Balz, *Business et droits d'Internet*, (1996), McGraw-Hill, Paris.

Iteanu, Olivier, *Internet et le droit, aspects juridiques du commerce électronique*, (1996) Édition Eyrolles, France.

Katsh, M. Ethan, *Law in a Digital World*, (1995), Oxford University Press, USA.

Kunze, Carole A., « Website Legal Issues », (1998), Santa Clara Computer and High Technology Law Journal, vol. 14, p. 477

Kurz, Raymond A., *Internet and the Law, Legal Fundamentals for the Internet User*, (1996), Government Institutes inc., Brockville, USA.

Lamy *Droit de l'informatique et des réseaux*, (1999) Édition Lamy, Paris.

Maher, Marcus, « An Analysis of Internet Standardization », 3 Va. J.L. & Tech. 5 (Spring 1998)
http://scs.student.virginia.edu/~vjolt/graphics/vol3/home_art5.html.

Ministère de la Justice du Canada, *Étude des questions de droit entourant la sécurité des renseignements électroniques*,
http://canada.justice.gc.ca/Commerce/index_fr.html (consulté le 20 août 1999)

POST, David G., " *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace* ", 1995 Journal Online L. article 3.

John Roemer, « Site for Sore Customers SquareTrade partners with eBay to resolve disputes online », 29 mars 2000,

<http://interactive.wsj.com/articles/SB953582315197322396.htm> (consulté le 29 mars 2000).

Rosenoer, Jonathan, *Cyberlaw, the Law of the Internet*, (1996), Springer-Verlag, USA

Schulman, Martin A., Rick Smith, *The Internet Strategic Plan, A Step-by Step Guide to Connecting Your Company*, Wiley Computer Publishing, (1997), États-unis.

Scott, Michael D., « *Website development agreement* », <http://www.perkinscoie.com/webrelease/webdevagmt.htm> (Dernière modification le 15 juin 1999, consulté le 14 août 1999).

Sédallian, Valérie, « *Création d'un site sur Internet : Aspects juridiques* », <http://62.161.196.163/lij/sitejuridique.html> (décembre 1998)

Smith, Graham G.H., *Internet Law and Regulation*, (1996), FT Law and Tax, Royaume-Uni.

Pierre TRUDEL, France ABRAN, Karim BENYEKHFLEF, Sophie HEIN, *Droit du Cyberspace*, Montréal, Les Éditions Thémis, 1997.

OUVRAGES ET ARTICLES SUR LE COMMERCE ÉLECTRONIQUE

a) Le commerce électronique en général

Anderson, Tim, « *Ten steps to help reduce legal disputes for E-commerce entrepreneurs* », (juin-juillet 1999), *Computers and Law*, p. 27.

Angel, John, « *Legal risks of providing services on the Internet* », (1996) *Communications Law*, vol. 1, n°3, 1996, p. 105.

Cheskin Research and Studio Archetype/Sapient, *Commerce Trust Study*, Janvier 1999.

Chissick, Michael, Alistair Kelman, *Electronic Commerce : Law and Practice*, (1999), Sweet and Maxwell, Royaume Uni.

Faique-Pierrotin, Isabelle, « *Commerce électronique: un cadre de confiance est indispensable* », 4 *Les Cahiers de l'Audit* 4.

« *Gaining trust from online consumers (A survey on what online customers expect from a commerce site)* », *Infoworld*, 1^{er} février 1999, vol. 21, p. 41.

Helft, Miguel, « *Commerce on the Net : whom do you trust ?* », *Los Angeles Times*, 10 mars 1997, vol. 116, page D-1, colonne 4.

- Kosiur, David, « *Understanding Electronic Commerce* », (1997), Microsoft Press, Redmond, USA.
- Mallan, Paul, « *The legal implications of electronic commerce in international trade* », (1997), *Computer and Law*, vol. 8, n° 4, page 24.
- Perritt, Henry H., *Law and the Information Super Highway*, (1996), Wiley Law Publications, John Wiley & sons inc., USA.
- Organisation de coopération et de développement économique (OCDE), « *Le commerce électronique, opportunités et défis pour le gouvernement* », (1997), France.
- Prins, J. « *Contracting in an on-line market place, Emerging electronic highways, new challenges for politics and law* », (1996), Kluwer Law International, Nouvelle-Zélande.
- Trudel, Pierre, « *Introduction au droit du commerce électronique sur Internet* », (1995) *Revue du Barreau*, Tome 55, page 521.
- Vérificateur Général, *Rapport (Chapitre 19)*, Ottawa, Ministère des Travaux publics et des Services gouvernementaux, décembre 1998.

b) La sécurité dans le commerce électronique

- « *Accountants band together for safe transactions* », *PC Week*, 29 septembre 1997, vol. 14, n° 41, page 32.
- Kellner, Mark A., « *Net transaction security : a state of mind* », *Communication Week*, 19 février 1996, n° 597, page 1 à 7.
- Lefer, Stéphane, « *Sécurité et confiance : maître mot du commerce électronique* », *Lamy Droit de l'informatique*, janvier 1998, n° 1999.
- Philips, Marc, « *Bombproof your site* », *Australian Netguide*, janvier-février 1998, vol. 4, page 68.
- Rogers, Amy, « *Maximum Security - Standards facilite E-business* », *Computer Reseller News*, 1999, page 1.

c) L'échange des consentements

- Morgan, John P., « *Electronic Authentication Standards And Development* », <http://www.perkinscoie.com/webrelease/electronic.htm> (20 mai 1999).
- Pierre TRUDEL, Guy LEFEBVRE et Serge PARISIEN, *La preuve et la signature dans l'échange de documents informatisés au Québec*, Québec, Les Publications du Québec, 1993.

d) Les mécanismes de paiement

Roger CLARKE, " Introduction to Electronic Payment Mechanisms ", Australian National University, 24 mai 1998,
<http://www.anu.edu.au/people/Roger.Clarke/EC/EPMIntro.html>;

Andreas FURCHE, Graham WRIGTSON, *Computer Money: A Systematic Overview of Electronic Payment Systems*, Les Éditions Morgan-Kaufman, 1997;

Alain PLAMONDON, "Le paiement électronique sur Internet, Recensement et analyse", Août 1996, <http://www.rambit.qc.ca/plamondon/ecashind.htm>;

Greg TUCKER, "Electronic Payment system", Law Institute Journal, janvier 1997;
 David WARD, "Electronic Payment Systems for the Internet", 11-03-1996,
http://members.ecom.net/~davidward/eps/elec_pay.html

e) La protection des consommateurs

L'Heureux, Nicole, « *Les effets de la technologie et la protection des droits des consommateurs dans le paiement bancaire* », (1983) 24 Cahiers de Droit 253

Tassé, Roger et Kathleen Lemieux, « *Les droits à la protection du consommateur au Canada dans le contexte du commerce électronique* », mars 1998,
<http://strategis.ic.gc.ca/SSGF/ca01031f.html>.

OUVRAGES ET ARTICLES SUR LA CERTIFICATION ET LES STANDARDS

« *A question of trust* », Computer Weekly, 10 juillet 1997, page VII.

AICPA-ICCA, *Principes et critères CertifiCA pour le commerce électronique entreprise-consommateur*, Version 1.0, 23 décembre 1997.

Andrews, Whit, « *The international computers security associations website certification program is an attempt to promote safe electronic commerce* », Internet World, 20 avril 1998, vol. 4, n° 15, page 18.

ANMA (American Naturopathic Medical Association), Legal Guidelines for Unlicensed Practitioners, Dr. Lawrence Wilson,
<http://anmaamerica.com/licvscer.htm> (consulté le 20 octobre 1999).

Anthes, Gary H., « *In Web E-trust* », Computer World, 18 novembre 1996, vol. 30 n° 47, page 71.

- Anthes, Gary H., « *Look for the NCSA label* », *Computer World*, 5 août 1996, vol. 30, n° 32, page 57.
- Antoine, Mireille, « *La certification électronique* », (1995), *Revue de Droit Commercial Belge*, page 4.
- Astrue, Michael, J., « *Health care reform and the constitutional limits on private accreditation as an alternative to direct government regulation* », *57 Law and Contemporary Problems*, 75.
- Blecher, Tedd, « *Products Standards and Certification Programs* », 46 (1980) *Brooklyn Law Review* 223.
- Calderbank, Alison, « *E-commerce gets seal of approval* », *Computer Reseller news*, 22 septembre 1997, n° 755, page 16.
- Costa, Dan, « *Seal appeal* », *Computer Shopper*, juillet 1999, vol. 19, page 79.
- Costa, Dan, « *NCSA Launches Secure Website certification* », *Computer Shopper*, novembre 1996, vol. 16, n° 11, p. 84.
- Couret, Alain, Jacques Igalens et Hervé Penan, *La Certification*, Presses Universitaires de France, Paris, 1995, Collection Que sais-je ?
- Davio, Étienne, « *Preuve et certification sur Internet* », (1997), *Revue de Droit Commercial Belge*, page 660.
- Davio, Étienne, « *Questions de certification, signature et cryptographie* », *Cahiers du CRID*, n° 12.
- Deweese, Donald N., *The Regulation of quality : products, services workplaces and the environment*, Toronto : Butterworths, 1983.
- Dunlap, Roger, Amy Charlotte-Dunlap, « *Better Business Bureau tackles privacy problem - offering seal of approval* », *Computer Reseller News*, 15 février 1999, page 1.
- Dupont, E., « *La normalisation : une profonde évolution du contenu, des acteurs, des enjeux* » (1993) *137 Enjeux* 41.
- Ellison, Carl M., « *Certification infrastructure needs for electronic commerce and personal use* », <http://www.clark.net/pub/cme/nist-7-24> (14 août 1997).
- Fontana, John, « *Certification Plans to Help Web Confidence* », *Communications Week*, 5 août 1996, n° 622, page 75.

- Finkin, Matthew, W., « *The Unfolding Tendency In The Federal Relationship To Private Accreditation In Higher Education* », (1994) 57 *Law and Contemporary Problems*, 89.
- Gast, Olivier, « *La certification des services : enfin une reconnaissance officielle* », (1995) 59 *Les Petites Affiches* 8.
- Geist, Michael, « *Consumer Portection and Licencing Regimes Review: The Implications or Electronic Commerce* », Janvier 2000, Rapport préparé pour le ministère de la consommation et du commerce, disponible à : <http://aix1.uottawa.ca/~geist/mccrgeist.pdf>.
- Gunzlé, Gérard, « *Une conception nouvelle du rôle de l'État : la certification des produits industriels et des services* », (1996) 82 *Notes Bleues de Bercy* 1.
- Havighurst, Clark C., « *The Place Of Private Accrediting Among The Instruments Of Government* » (1994) 57 *Law and Contemporary problems*, 1.
- Havighurst, Clark C. et Peter M. Brody, « *Accrediting and the Sherman Act* », (1994) 57 *Law and Contemporary Problems*, 199.
- Hermitte, M.-A., « *Licence de marque et assurance qualité dans les ventes internationales d'ensembles industriels* » (1989) 45:116 *Journal du Droit International* 5.
- Howe, Jonathan T. et Leland J. Badger, « *The Antitrust Challenge To Non-Profit Certification Organizations : Conflicts of Interest and a Practical Rule of Reason Approach to Certification Programs as Industry-Wide Builders of Competition and Efficiency* », (1982) 60 *Washington University Law Quarterly* 357.
- Iacono, Geneviève, « *La certification d'assurance qualité : De nouvelles questions pour le Droit ?* », (1994) *Revue Internationale de Droit Économique* 63, p. 70.
- Igalens, Jacques et Penan, Hervé, *La normalisation*, Presses Universitaires de France, Paris, 1994, Collection Que sais-je ?, numéro 1984
- Jost, Timothy-Stoltzfus, « *Confidentiality and Disclosure in Accreditation* », (1994) 57 *Law and Contemporary Problems*, 171.
- Jost, Timothy-Stoltzfus, « *Medicare And The Joint Commission On Accreditation Of Healthcare Organizations* », (1994) 57 *Law and Contemporary Problems*, 15.
- Kinney, Eleanor D., « *Private Accreditation As A Substitute For Direct Government Regulation In Public Health Insurance Programs : When Is It Appropriate ?* », (1994) 57 *Law and Contemporary problems*, 47.

- Lash, Alex, « *TRUSTe Cracks the Whip* », *The Standard*, 22 mars 2000, <http://www.thestandard.com/article/display/0,1151,13238,00.html> (consulté le 23 mars 2000).
- Lautsch, John C., *American Standard Handbook Of Software Business Law*, (1985), Reston Publishing Company inc., Reston, USA
- Lewis, Jimmy, « *Certifying Authorities Must Build Trust* », *PC Week*, 29 juin 1998, vol. 15, n° 26, page 107.
- Maass, Richard A., John O. Brown et James L. Bossert, *La certification des fournisseurs*, (1994), Les Éditions Transcontinentales inc., (traduction française), Montréal, Canada.
- MacDonald, Diane, « *Sectoral Certification : A Case Study Of British Columbia* », (1997) 5 *Can. Lab. And Emp. L.J.* 243.
- Martin, Jeffrey, C., « *Recent Developments Concerning Accrediting Agencies in Postsecondary Education* », (1994) 57 *Law and Contemporary Problems*, 121.
- Melek, Adel, Victor Keong et Karen Nemani, « *Sceaux de confiance* », (octobre 1998) *CaMagazine* 43.
- Merrill, Charles, R., « *The Accreditation Guidelines - a progress report a work in process of the ABA Information Security Committee* », (1998) 38 *Jurimetrics* 345.
- Morgan, John P., « *Electronic Authentication Standards And Development* », <http://www.perkinscoie.com/webrelease/electronic.htm> (20 mai 1999).
- Notes : « *Tort Liability of Independent Testing Agencies* », (1968) 22 *Rutgers Law Review* 299.
- Note : « *Voluntary Codes and the Consumer Interest* », *Consumers Quarterly*, October 1996, Volume 1, Number 4, <http://strategis.ic.gc.ca/SSG/ca00218e.html>.
- Parisien, Serge, Trudel, Pierre, *L'identification et la certification dans le commerce électronique, Droit, sécurité audit et technologies*, (1996), Les Éditions Yvon Blais, Québec.
- Pelesh, Mark, L., « *Due Process In The Accreditation Context : A Reply* », (1995) 22 *The Journal of College and University Law* 175.
- Piette-Coudol, Thierry, « *Certification électronique : pratique et modélisation* », <http://www.e-betobe.com/texteece.htm> (consulté le 20 octobre 1999).

- Ponthier, Jean-Marie, « *La certification outil de la modernité normative* », 30 (1996) Dalloz-Sirey, c. 355-360.
- Prairie, M.W. et L.A. Chamberlain, « *Discussion Of The Due Process In The Accreditation Process* », (1994) 21 *The Journal of College and University Law* 61.
- Racine, Jean-Baptiste, « *Normalisation, certification et droit de la concurrence* », (1998)1 *Revue Internationale de Droit Économique* 147.
- Rae, Andrew, K., Hans-Ludwig Hausen, Philippe Robert, *Software Evaluation for Certification, Principles, Practice and Legal Liability*, (1995), McGraw Hill Book Company, England.
- Rafter, Micelle, « *Trust or Bust?* », *The Standard*, 6 mars 2000, <http://www.thestandard.com/article/display/0,1151,12445,00.html> (consulté le 23 mars 2000).
- Royon, Michel, « *L'émergence de systèmes nationaux de normalisation-certification et leur connexion internationale* », (1999) *Revue Internationale de Droit Économique* 107.
- Schuck, Peter, H., « *Tort Liability To Those Injured By Negligent Accreditation Decisions* », (1994) 57 *Law and Contemporary Problems*, 185.
- Scott, Michael D., « *Establishing a legally safe presence in cyberspace* », <http://www.perkinscoie.com/webrelease/safecyberbres.htm> (consulté le 24 août 1999)
- Shein, Esther, « *You can eTRUST us* », *PC Week*, 16 décembre 1996, vol. 13, n° 50, page E-1.
- Sigel, Skip, Theo Ling, et Joshua Izenberg, « *The validity and Enforceability of Web-Wrap Agreements and Assessing the Need for Legislation* », prepared for the Uniform Law Conference of Canada, May 1999, <http://www.law.ualberta.ca/alri/ulc/current/ewebwrap.htm>.
- Stuurman, Kees, « *Legal Aspects Of Standardization And Certification In Information Technology And Telecommunication : An Overview* », dans Kaspersen, HWK et A. Oskamp, *Amongst Friends in Computer Law : a Collection of Essays in remembrance of Guy Vanderberghe*, 1990, Kluwer Law and Taxation Publishers, Deventer, Hollande, page 75.
- Stuurman, Kees, *Certificatie van software in juridisch perspectief (Certification of software in legal perspective)*, 1988, Netherlands Association for Computers and Law, Amsterdam, Hollande.

Tomlinson, Timothy, « *Certificate Authorities : Four Choices* », (1997), Computer Law Strategists, page 5

Trompette, Thierry, « *Une nouvelle mission : la certification des sites Web de commerce électronique* », (1999) 4 Les Cahiers de l'Audit 34.

Wasserman, Elizabeth, « *Getting A Website Seal Of Approval* », San Jose Mercury News, 16 octobre 1996, page 1A.

Wegner, Judith Welch, « *Two Steps Forward, One Step Back : Reflections On The Accreditation Debate* », (1995) 45 Journal of Legal Education, 441.

OUVRAGES ET ARTICLES SUR L'AUDIT

Arens, Alvin A., James K. Loebbecke, *Auditing, An Integrated Approach*, (1997), 7^e Edition, Prentice Hall, Upper Saddle River.

Barbier, Etienne, *L'audit interne, permanence et actualité*, (1996), 3^e Edition, Les Éditions d'Organisation, France.

Blaustein, Rochelle S., « *Does Your Website Need A Legal Audit ?* »
<http://www.patentplus.com/webaudit.html> (Dernière modification le 21 novembre 1998 ; consulté le 24 août 1999)

Brandt, Stephen C., « *Legal Audit Checklist* », Stafford Frey Cooper,
<http://www.buildyourbusiness.com/> (consulté le 24 août 1999);

Cushing, Barry E., Marshall B. Romney, *Accounting Information Systems*, (1993), 6^e Edition, Addison-Wesley Publishing Company, USA.

Dunn, Gary, « *Legal Audit for Websites* », November/December 1997, Computer & Technology Law, <http://www.cc.ubc.ca/ccandc/nov-dec97/audit.html> (consulté le 24 août 1999).

Gallegos, Frederick, Dana R. Richardson, A. Faye Borthick, *Audit and Control of Information Systems*, (1987), South Western Publishing Company, USA.

Gélinas, Ulric G., Steve G. Sutton, Allan E. Oram, *Accounting Information Systems*, (1998), 4^e Edition, South Western College Publishing, USA.

Ince, Darrill, *Software Quality Assurance - A Student Introduction*, (1996), McGraw-Hill Book Company, USA.

Konrath, Larry F., *Auditing, Concept And Application, A Risk Analysis Approach*, (1993), 2nd Edition, West Publishing Company.

- Mair, William C., Donald R. Wood, Keagle W. Davis, *Computer Control and Audit*, (1976), USA.
- McIntosh, Norman G., *The Social Software Of Accounting And Information Systems*, (1986), John Wiley & Sons, USA.
- Messier, William F., *Auditing, a Systematic Approach*, (1997) McGraw-Hill, USA
- Mills, Charles A., *The Quality Audit, A Management Evaluation Tool*, (1992), ASQC Quality Press, Milwaukee, USA.
- Robertson, Jack C., Timothy J. Louwers, *Auditing*, (1999), 9^e Edition, McGraw-Hill, USA.
- Sawyer, Lawrence B., Mortimer A. Dittenhofer, *Sawyer's Internal Auditing, The Practice Of Modern Internal Auditing*, (1998), 4^e Edition, The Institute of Internal Auditor, Alta Monte Springs, USA
- Smith, Janet L., *The Quality Audit Handbook*, (1997), ASQC Quality Press, Milwaukee, USA.
- Wong, Nicole A. et James F. Brelsford, « *Conducting Website Legal Audits* » : a *U.S. perspective*, <http://www.perkinscoie.com/webrelease/webaudits.html> (consulté le 24 août 1999)

ORGANISMES DE CERTIFICATION DE SITES WEB

- ADDSecure.Net inc., <http://www.addsecure.net>.
- BBBOnline, <http://www.bbbonline.com/>.
- Better Internet Bureau, <http://www.better-internet-bureau.org>
- Check-marks , <http://www.check-mark.com>
- European Information Technology Security Evaluation Criteria (ITSEC).
<http://www.itsec.gov.uk>
- ICSA (NCSA) Firewall Certification, <http://www.icsa.net>
- TRUSTe, <http://www.truste.org/>.
- US GOLD.gov, <http://www.usgold.gov/certification.html>.
- WebAssured.com (anciennement le Web Assurance Bureau)
<http://www.WebAssured.com>

Webtrust, <http://www.cica.ca/new/index/f-wt-in.htm>.

Beck & Arad LLP, « Legal SiteCheck », www.legalsitecheck.com (1998, consulté le 14 août 1999)

ORGANISMES DIVERS

Bureau de normalisation du Québec (BNQ), <http://www.criq.qc.ca/bnq>.

Le conseil canadien des normes (CCN), <http://www.scc.ca>.

Federal Electronic Commerce Program Office, <http://www.ec.fed.gov/>

L'association canadienne de normalisation (CSA), <http://www.csa.ca>.

L'association française de normalisation (AFNOR), <http://www.afnor.fr>

L'association française pour l'assurance de la qualité (AFAQ),
<http://click.rever.fr/afaq/>.

L'organisation internationale de normalisation (ISO), <http://www.iso.ch>.

Secretariat for Federal EDI, <http://snad.ncsl.nist.gov/fededi/> (standards pour EDI)

INDEX DES TEXTES LÉGISLATIFS CITÉS

CANADA

Loi sur la concurrence, L.R.C., c. C-34;

Loi sur le droit d'auteur, L.R.C. chapitre C-42;

Loi sur les dessins industriels, L.R.C. chapitre I-9;

Loi sur les brevets, L.R.C., chapitre P-4;

Loi sur les marques de commerce, L.R.C., chapitre T-13;

Loi sur les topographies de circuits intégrés, L.C. 1990, chapitre 37.

Projet de loi fédéral C-6, Loi sur la protection des renseignements personnels et les documents électroniques (anciennement Projet de loi C-54, Loi sur la protection des renseignements personnels et documents électroniques, première session, 36^e législature, 46-47 Élisabeth II, 1997-1998), disponible à :
http://www.parl.gc.ca/36/1/parlbus/chambus/house/bills/government/C-54/C-54_1/C-54_cover-F.html (consulté le 23 mars 2000).

QUÉBEC

Code civil du Québec, L.Q. 1991, c. 64 ;

Loi sur le Barreau, L.R.Q., c. B-1 ;

Loi sur la protection des consommateurs, L.R.Q., c. P-40.1;

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

INTERNATIONAL

United States Code, Title 15 (Commerce and Trade), disponible à
<http://www4.law.cornell.edu/uscode/>

Loi n° 78-23 du 10 janvier 1978 sur la protection et l'information des consommateurs de produits et de services. (dite "loi Scrivener"), disponible à <http://www.admi.net/jo/loi78-23.html>

ANNEXE A**ORGANISMES DE CERTIFICATION D'IDENTITÉ****États-Unis**

ARCANVS , <http://www.arcanvs.com/>

ARINC , <http://www.digsig.arinc.com/>

CertCo , <http://www.certco.com/>

Columbia University , <http://www.columbia.edu/acis/rad/columbiaca/>

CommerceNet, <http://www.commerce.net/certification>

Cyberguard , <http://www.cybg.com/>

Digital Signature Trust , <http://www.digsigtrust.com/>

Equifax, <http://www.equifaxsecure.com/>

Gartner Group, <http://www.gartner.com>

GTE Cybertrust , <http://www.bbn.com/>

IBM Vault Registry , <http://www.software.ibm.com/security/registry/index.html>

IDCertify , <http://www.idcertify.com/>

IPRA , <http://bs.mit.edu:8001/ipra.html>

Texstar Technology, <http://www.texstartech.com>

TradeWave (Trade VPI) , <http://www.tradewave.com/>

UMS , <http://www.cu.edu/~security/pki/>

USERFirst , <http://www.usertrust.com/>

VeriSign , <http://digitalid.verisign.com/>

Canada

BCE Emergis, <http://www.public-key.com/en/default.htm>

Entrust , <http://www.entrust.com/>

Infrastructure à clés publiques du gouvernement du Canada,
<http://www.cse.dnd.ca/cse/francais/gov.html>

WebTrust , <http://WebTrust.net/>

xcert, <http://www.xcert.com/>

Autres pays

AD AEQUITATEM (Espagne) , <http://aequitas.encomix.es/indexf.htm>

Bankgate (Afrique du Sud), <http://www.bankgate.com/market/index.htm>

BelSign (Belgique & Luxembourg), <http://www.kpmg.com.au/certauth.html>

BiNary Surgeons (Afrique du Sud) , <http://www.surgeons.co.za/cert/>

CARYNET (Asie) , <http://sun.cary.net/CA/>

Compu Source (Afrique du Sud), <http://www.compusource.co.za/id/personal/>

Cost (Suède) , <http://www.cost.se/>

EuroSign (Europe), <http://eurosign.com/>

GlobalSign, <http://www.globalsign.com>

Initiatives for Computer Authentification Technology (ICAT), (Japon) ,
<http://www.icat.or.jp/English/index.html>

IKS (Information Kommunikation Systeme) (Allemagne) , <http://www.iks-jena.de/produkte/ca/index.en.html>

InterClear (Royaume-Uni) , <http://www.interclear.net/>

KeyPost (Australie), <http://www.auspost.com.au/keypost/>

KPMG (Australie), <http://www.kpmg.com.au/certauth.html>

mTrust (Malaisie), <http://www.mtrust.com.my/trial/trialcps.html>

Netrust (Singapour), <http://www.netrust.com.sg/>

Policy Certification Authority , PCA-DFN (Allemagne) ,
<http://www.pca.dfn.de/eng/dfnpca/>

SACA (South African Certification Agency), Afrique du Sud, <http://www.saca.net/>

Signet (Australie) , <http://www.signet.org.au/>

SISCER (Espagne) , <http://www.siscer.com/siscer.en.html>

SSE (Secure Solutions Experts), Irlande, <http://www.sse.ie/>

Thawte, Afrique du Sud, <http://www.thawte.com/>

World Wide Wedlin (Suède) , <http://www.wedlin.pp.se/ca/index.html>

ANNEXE B**LA PROBLÉMATIQUE DES NOMS DE DOMAINE**

G. Peter Albert, Jr., Right on the Mark: Defining the Nexus Between Trademarks and Internet Domain Names, 15 J. Marshall J. Computer & Info. L. 277 (1997);

G. Andrew Barger, Cybermarks: A Proposed Hierarchical Modeling System of Registration and Internet Architecture for Domain Names, 29 J. Marshall L. Rev. 623, 660-66 (1996);

Scott N. Barker, Famous.com: Applying the FTDA to Internet Domain Names, 22 U. Dayton L. Rev. 265 (1997);

Andre Brunel, Billions Registered, But No Rules: The Scope of Trademark Protection for Internet Domain Names, J. Proprietary Rts., Mar. 1995;

Kenneth Sutherlin Dueker, Trademark Law Lost in Cyberspace: Trademark Protection for Internet Addresses, 9 Harv. J. Law & Tech. 483 (1996);

Neal J. Friedman & Kevin Siebert, The Name Is Not Always the Same, 20 Seattle U. L. Rev. 631 (1997);

Mark Gould, An Island in the Net: Domain Naming and English Administrative Law, 15 J. Marshall J. Computer & Info. L. 493 (1997);

Gary W. Hamilton, Trademarks on the Internet: Confusion, Collusion or Dilution?, 4 Tex. Intell. Prop. L.J. 1 (1995);

Deborah Howitt, War.com: Why the Battles over Domain Names Will Never Cease, 19 Hastings Comm. & Ent. L.J. 719 (1997);

David J. Loundy, A Primer on Trademark Law and Internet Addresses, 15 J. Marshall J. Computer & Info. L. 465 (1997);

Ira S. Nathenson, Comment, Showdown at the Domain Name Corral: Property Rights and Personal Jurisdiction over Squatters, Poachers and other Parasites, 58 U. Pitt. L. Rev. 911 (1997);

Carl Oppedahl, Analysis and Suggestions Regarding NSI Domain Name Trademark Dispute Policy, 7 Fordham Intell. Prop. Media & Ent. L.J. 73 (1996);

Carl Oppedahl, Remedies in Domain Name Lawsuits: How Is a Domain Name Like a Cow?, 15 J. Marshall J. Computer & Info. L. 437;

Daniel R. Pote, A Domain by Any Other Name: The Federal Trademark Dilution Act of 1995 Applied to Internet Domain Names, 37 Jurimetrics J. 301 (1997);

Stacy B. Sterling, New Age Bandits in Cyberspace: Domain Names Held Hostage on the Internet, 17 Loy. L.A. Ent. L.J. 733 (1997);

Gayle Weiswasser, Domain Names, the Internet, and Trademarks: Infringement in Cyberspace, Computer & High Tech. L.J. 137 (1997)

ANNEXE C**COMMANDITAIRES DE TRUSTe****Premier Corporate Sponsors**

AOL
Compaq
Ernst & Young LLP
Excite
IBM
Intel
Microsoft
Novell

Premier Media Sponsors

The Industry Standard
MacWEEK
Macworld
PC Week
Wired Ventures
Yahoo Internet Life

Contributing Corporate Sponsors

AdForce
AT&T
Engage Technologies
Lands' End
PricewaterhouseCoopers LLP
RD/FOX
RealNetworks

Official Auditors

PricewaterhouseCoopers LLP
KPMG Peat Marwick

Professional Contributors

Alexa Internet
Gray Cary Ware & Friedenrich
ImageLock
Wiley, Rein and Fielding
World Pages

Founding Organizations

CommerceNet
Electronic Frontier Foundation
The Boston Consulting Group

Advisory Companies

A.D. Little
CyberSource
EDventure Holdings
Info Online
Organic Online
Pacific Digital
Perot Systems
Pretty Good Privacy
Preview Systems
Scala ECE
Stanford Law & Technology Policy Center
TestDrive
TS Communications
United Telecommunications
WebCrawler
Wilson Sonsini Goodrich & Rosati
WorldPages

(liste tirée du site TRUSTe : http://www.truste.org/about/about_sponsors.html, consulté le 23-03-2000)