LES SCEAUX DE CERTIFICATION DES SITES WEB : UN OUTIL DE CONFIANCE, OUTIL DE CONFUSION

Louise Martel, René St-Germain

LES SCEAUX DE CERTIFICATION DES SITES WEB : UN OUTIL DE CONFIANCE, OUTIL DE CONFUSION

Louise, Martel et René, St-Germain
HEC Montréal
3000 chemin de la Côte-Ste-Catherine, Montréal (Québec) Canada H3T 2A7
(514) 340-6785 - louise.martel@hec.ca

Résumé

Avec l'évolution des technologies, les entreprises doivent s'adapter au nouveau concept de commerce électronique; les clients aussi. Comment garder leur confiance et ce, au bout des doigts. Ce texte présente un cadre conceptuel de la certification de conformité des sites Web ainsi qu'une typologie des sceaux de certification (labels) existants.

Mots clés : Sceaux de certification - Certification de conformité - E-Commerce - Affaires électroniques - Gestion des risques

Abstract

Trust is analysed as it influences e-business. A Web site attest framework with a focus on the subject matter, the attest process and the attest strategies described. The paper also present a typology of Web site labels which has been developed from a study conducted in the summer of 2001.

Keywords :Label – Attest - E-Commerce - E-Business - Risk Management

1 Introduction

Malgré les mesures technologiques mises en place par les cybermarchands, on constate que les consommateurs entretiennent toujours une grande méfiance lorsque vient le moment de fournir leur numéro de carte de crédit sur un site transactionnel. Lors de la phase de paiement, plus de la moitié des internautes ne complèteraient pas leurs transactions. L'instauration de mesures de contrôle et de sécurité n'augmente pas nécessairement la confiance des consommateurs envers le commerce électronique. Cela s'explique par le fait que les préoccupations des consommateurs ne concernent pas uniquement la sécurité des transactions mais aussi les délais de livraison, la qualité des produits, le respect des garantis, etc.

Afin d'augmenter la confiance des intervenants dans le commerce électronique, des organismes publics ou privés ont créé divers sceaux de certification également appelés «labels». Ces sceaux portent tantôt sur l'évaluation du contenu, tantôt sur l'authentification des parties et l'intégrité des transactions et tantôt sur la satisfaction de la clientèle. En fait, ces sceaux constituent un moyen visuel qui permet à l'utilisateur de savoir si le site Web est conforme à certains critères. Ajoutons que les périmètres de ces critères sont très variables.

Le sceau de certification signifie à la clientèle qu'une personne ou une organisation a évalué les pratiques commerciales et/ou les contrôles relatifs au site Web afin de déterminer si ces derniers sont conformes aux «principes et critères» pour le commerce électronique. Les principes doivent avoir été respectés en regard des principes et critères reflétant des normes fondamentales en matière notamment de transparence des pratiques commerciales, d'intégrité des opérations et de protection de l'information.

Au cours de l'année 1999-2000, une première étude portant sur la certification de conformité des sites Web a permis d'identifier certaines tendances observables sur le phénomène des

sceaux de certification[1]. Cette étude a permis de développer un modèle de certification des sites Web en plus d'identifier certains sceaux de certification ainsi que leurs caractéristiques. De même, les principales questions d'ordre juridique que soulève la certification, les obligations qui y sont associées et les responsabilités civiles découlant de leur non-respect y ont été débattues.

Dans le présent article, un cadre conceptuel développé dans le but de comprendre la certification de sites Web sera présenté. Dans la première section, le concept de certification sera défini et les notions/clés qui en découlent seront traitées : le lien de confiance entre les consommateurs, le certifié et le certifiant ainsi que le partage de risque existant entre ces acteurs. Comme la certification implique la conformité à des critères ou à des normes, c'est à la question du processus de normalisation que sera consacré la deuxième section. Quant à la troisième section, elle décrira différents modèles de certification. Pour conclure, une typologie des différents types de sceaux de certification élaborée à partir de la recension de quelques 170 sceaux existants sur le marché sera présentée.

2 La certification

Il est important de bien définir le concept de certification puisque plusieurs termes sont couramment utilisés pour désigner des concepts similaires tels que : attestation, vérification ou accréditation. Selon Royon[2], la certification est une *procédure* selon laquelle une *tierce partie* donne une *assurance écrite* qu'un produit ou un service est conforme aux exigences spécifiées dans les référentiels de certification c'est-à-dire aux *normes* spécifiées.

Selon une vision plus technologique, le guide de la gestion des risques d'atteinte à la sécurité des technologies de l'information du Centre de la sécurité des télécommunications du Canada[3] définit la certification comme *étant la façon d'exécuter une évaluation complète des dispositifs de sécurité d'un système de technologie de l'information pour déterminer s'ils satisfont à la politique sur la sécurité.* L'accréditation du point de vue technologique est définie par cet organisme comme étant l'acceptation officielle de la gestion des risques informatiques que comporte un système de technologie de l'information. Ainsi, l'accréditation constitue une déclaration formelle, effectuée par la direction responsable, selon laquelle un système automatisé est approuvé pour fonctionner dans un mode déterminé, avec un ensemble donné de paramètres.

La certification remplit, au cours du cycle de vie d'un système, un rôle semblable à celui de l'assurance de la qualité : elle sert à valider, vérifier et tester les dispositifs de sécurité. Elle permet en outre d'établir que le système fonctionne comme il se doit et qu'il n'engendre aucune fonctionnalité nouvelle susceptible d'exposer les biens qu'il comporte à de nouveaux risques. L'accréditation est le processus officiel par lequel la direction autorise l'exploitation du système, et accepte les risques résiduels qu'elle comporte. L'accréditation dépend des résultats de la certification ainsi que d'autres considérations de nature administrative. La

[1] La sécurité et la certification de conformité des sites Web, étude réalisée par le Centre de recherche en droit public, le Centre de recherche informatique de Montréal et HÉC Montréal, juillet 2000. Cette étude est disponible sur le site : www.sceauxdecertification.org.
[2] Royon, Michel. L'émergence de systèmes nationaux de normalisation/certification et leur connexion internationale, *Revue internationale de droit économique*, 1999, pages 107 à 118.
[3] http://www.cse.dnd.ca/cse/francais/Manuels/mg4int-f.htm

certification est une évaluation complète des dispositifs de sécurité techniques et non techniques d'un système informatique, effectuée à l'appui de l'accréditation, et établissant le degré selon lequel ce système satisfait à une politique de sécurité déterminée.

Dans le cadre de nos recherches, nous retenons la définition ci-dessous de la certification : *Reconnaissance, écrite ou sous forme d'image, qui affirme (atteste ou assure) qu'une organisation se conforme à des normes spécifiées*[4].

Cette définition, assez large, laisse beaucoup de place à différents types de certification. Ainsi, les formes écrites de reconnaissance peuvent varier de beaucoup. Il en va de même pour les représentations imagées. De plus, cette définition ne précise pas quel organisme atteste ou assure. S'agit-il de l'organisation elle-même ou d'une tierce partie indépendante ? Il va de soi que la provenance de la certification change la nature de celle-ci. Enfin, la définition retenue ne spécifie pas le processus de certification retenu par l'organisme certifiant pas plus que les normes auquel le certifié s'est conformé. Nous reviendrons un peu plus loin dans le texte sur cette question.

L'objectif de la certification est de réduire les risques réels et perçus. Du point de vue de l'organisation certifiée, il s'agit en effet d'un outil de gestion du risque puisque, une fois certifiée, l'organisation peut prétendre que le partenaire avec qui elle a transigé est au courant des normes qu'elle suit. En cas de litige, elle invoquera certainement cet argument. Du point de vue du consommateur ou de la partie avec laquelle l'organisation transige, il s'agit en effet d'un outil de confort. Le partenaire sait que l'organisation se conforme à des normes établies. Ceci a pour effet d'augmenter la confiance du partenaire envers l'organisation certifiée. On peut représenter la certification avec le Schéma 1.

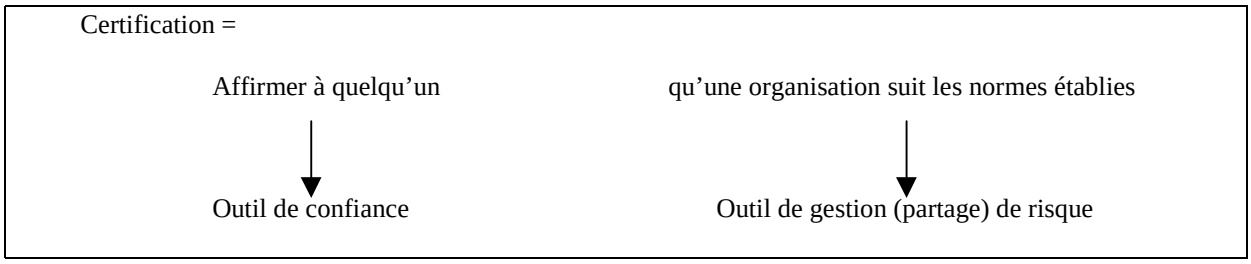


Schéma 1

2.1 La certification : une question de confiance

Le réel défi du commerce électronique relève d'une question de confiance. La confiance a toujours été un facteur essentiel dans le monde des transactions économiques; elle fait partie intégrante de tous les modes transactionnels à travers les structures et les processus.

Le commerce électronique vient changer les structures et les processus modifiant du même coup la confiance. Les relations entre les acheteurs ou utilisateurs de services et les vendeurs ou pourvoyeurs de services se redéfinissent de façon drastique. Les cadres de référence du commerce ont toujours inclus des éléments tangibles et intangibles qui définissent ce que constitue un environnement commercial acceptable. Par exemple, tous reconnaissent la valeur

[4] La sécurité et la certification de conformité des sites Web, étude réalisée par le Centre de recherche en droit public, le Centre de recherche informatique de Montréal et HÉC Montréal, juillet 2000, p.20.

d'une poignée de main ou d'un établissement physique. Ces signes de confiance et leur signification se sont bâtis sur de longues périodes de temps mais aujourd'hui le rythme de développement du commerce électronique n'a pas encore permis à un modèle de confiance d'émerger. Il en découle un nouvel espace de marché où existent des zones d'incertitude et de risques. Les consommateurs/citoyens n'ont pas de moyens familiers pour déterminer avec qui ils font affaires comme ils ont traditionnellement l'habitude de faire. Ils ne peuvent plus toucher et inspecter. Il n'y a plus de lieux physiques à visiter et même les marques de commerce changent. Ils ont également des soucis à propos du service après vente et sur les coûts de livraison ou les frais de douane. Ils craignent également que les différends avec les détaillants en ligne ne puissent être réglés équitablement.

La notion de confiance dépasse également les frontières auxquelles la plupart des individus ont été confrontés. En effet, le commerce électronique permet des échanges n'importe où sur la planète. Comment faire confiance à une organisation qu'on ne connaît pas, qu'on n'a jamais vue, qu'on ne verra probablement jamais et qui vit à l'autre bout de la planète dans un pays où les gens ne partagent peut-être pas les mêmes valeurs fondamentales que les nôtres ?

Le tout se déroule dans un environnement technologique qui a été développé avec un objectif de recherche et non de commerce électronique. Dans un tel contexte, les mécanismes de contrôle prévus pour Internet sont basés sur la notion de respect mutuel, d'honneur et de connaissance mutuelle des méthodes de conduite du domaine de la recherche donc de l'éthique propre à la recherche. Enfin, la technologie est un domaine plus complexe qui n'est pas bien connu des intervenants. Les échanges d'informations et les transactions se font donc dans un environnement avec lequel les intervenants sont moins familiers et où les problèmes de sécurité et les fraudes font fréquemment l'objet d'articles de journaux ou de nouvelles télévisées.

L'expansion du commerce électronique à partir du réseau Internet nous amène à repenser la notion de confiance. Le manque de confiance, basé sur une connaissance approfondie des partenaires, constitue le frein le plus souvent mentionné au niveau du développement du commerce électronique. La confiance peut être définie de la façon suivante : *the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the agility to monitor or control that other party*[5].

En d'autres mots, la confiance est la volonté d'agir d'un individu d'une telle façon parce qu'il assume que l'autre partie réagira de telle autre façon. Il s'agit donc d'une évaluation, consciente ou non, du comportement de l'autre partie. Par exemple, je confie un secret à quelqu'un parce que j'évalue que cette autre personne saura garder ce secret. Il est important d'avoir confiance parce que la confiance constitue le seul facteur qui permette d'établir la continuité dans les relations. En effet, sans confiance, une personne ne peut prendre de risques. Et sans prendre de risques, on ne peut rien faire.

En s'appuyant sur le modèle d'échange décrit plus haut, la confiance signifie que les parties impliquées dans un échange sont dignes de foi, sont des personnes sur lesquelles on peut se fier et qu'elles tiendront leur promesse. De plus, dans le monde virtuel, la transaction passe par un processus dans lequel les partenaires doivent avoir confiance. On parlera alors de

[5] Mayer, R.C., Davis, J.H. et Schoorman, F.D. An Integrative Model of Organizational Trust, *Academy of Management Review*, Vol. 20, No. 3, 1995, pages 709 à 734.

sécurité du processus. Les parties impliquées dans l'échange électronique doivent donc avoir confiance à la fois envers les partenaires avec lesquels ils transigent mais également envers le processus incluant la sécurité du support informatique plus spécifiquement du réseau Internet.

La confiance passe par la connaissance mutuelle des partenaires et par un processus. Dans le cas du commerce électronique, les deux composantes de la confiance sont affectées.

Dans le commerce traditionnel, un individu intervient avec un partenaire qu'il voit, qu'il entend ou qui utilise une autre forme de communication avec laquelle il est familier. La plupart du temps, ce même individu communique avec des individus avec lesquels il a déjà fait affaires. Dans le monde virtuel, la prolifération des partenaires croît à un rythme sans précédent, ce qui laisse peu de temps à chaque individu pour se familiariser avec son nouveau partenaire. Il faut remplacer la poignée de main, le face à face, par des signes avec lesquels les individus se sentent en confiance. Il est nécessaire de rebâtir un filet de sécurité, mais ceci prend du temps. La facilité avec laquelle les personnes peuvent établir et abandonner une identité virtuelle crée des doutes sérieux sur la qualité des identités virtuelles. En effet, il est fréquent de retourner sur un site que l'on avait noté et de découvrir qu'il n'existe plus.

De plus, l'internationalisation constitue une nouvelle dimension avec laquelle les individus doivent composer. Entrer dans une boutique du quartier est fort différent que de visiter un site Web à l'autre bout du monde. Comment savoir si le partenaire à l'autre bout du monde respectera ses engagements? À qui avoir recours en cas de problème?

Par processus, il est entendu les pratiques commerciales ainsi que le support technologique sous-jacent. Cette technologie n'est pas connu de tous et ses mécanismes de contrôle encore moins.

En ce qui concerne la confiance, les objets de normalisation doivent répondre aux préoccupations des participants aux échanges électroniques. Ces liens sont représentés dans le Schéma 2.

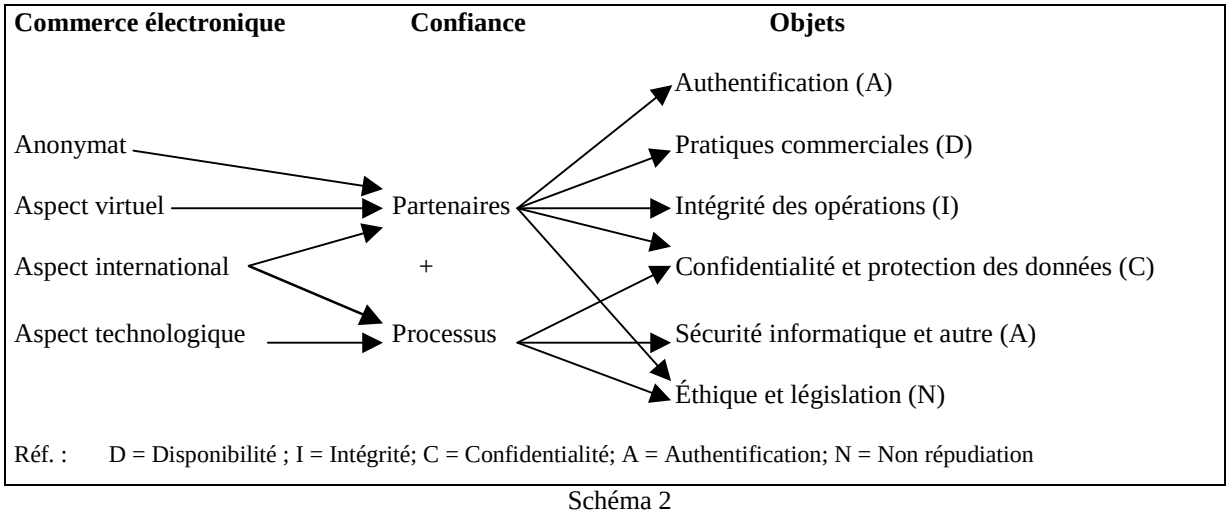


Schéma 2

2.1.1 Authentification des parties

L'authentification porte sur la capacité d'un système de démontrer à toute entité intéressée la vraie source d'un message transactionnel. Le destinataire est assuré que la transaction provient bien de l'expéditeur attendu, et ce dernier est assuré qu'il s'agit bien du destinataire présumé[6]. L'authentification vise aussi bien les individus que les sociétés ou les gouvernements et les intermédiaires.

2.1.2 Pratiques commerciales

Le commerce électronique suppose souvent des opérations entre de véritables inconnus. Les apparences peuvent être trompeuses : comment le consommateur peut-il être sûr que les biens et services présentés dans une page Web bien structurée seront livrés tels quels par l'entité qui les offre? Comment le consommateur peut-il savoir si cette entité accepte les retours d'articles vendus et si ces articles sont garantis? Comment sont gérées les plaintes du client concernant l'exactitude, l'exhaustivité et la diffusion des renseignements personnels qui le concernent? Étant donné le caractère anonyme du commerce électronique et la facilité avec laquelle les personnes malhonnêtes peuvent établir puis abandonner une identité virtuelle, il est essentiel que les consommateurs sachent que les entités avec lesquelles ils font affaires déclarent leurs pratiques commerciales et les respectent. Sans ces renseignements utiles et sans l'assurance que l'entité a respecté dans le passé les pratiques déclarées, les consommateurs courent un risque accru de subir des pertes, d'être victimes de fraude, d'éprouver des contrariétés ou de voir leurs attentes déçues[7].

2.1.2.1 Intégrité des opérations

L'intégrité des opérations réfère à la protection du contenu en cours de route, avant d'arriver à son destinataire. Le contenu de la transaction ne doit pas avoir été modifié entre le moment de son émission et celui de sa réception. En outre, il touche toutes les étapes des commandes de biens et/ou services : exactitude, exhaustivité, confirmation, le traitement, la livraison, le paiement et l'historique des commandes.

2.1.2.2 Confidentialité ou protection de l'information

La confidentialité ou la protection de l'information porte sur la capacité de ne révéler aux entités concernées que les informations qui sont nécessaires au bon fonctionnement des transactions. Seul le destinataire d'une transaction confidentielle est en mesure d'en lire le contenu. Il porte sur la transmission des renseignements personnels du client, sur la cueillette de renseignements auprès du client, la protection et l'utilisation des renseignements personnels du client, l'exactitude et l'exhaustivité des renseignements, la responsabilité de l'entité à l'égard des renseignements transmis à un tiers, la protection des ordinateurs et des fichiers du client et la surveillance de la confidentialité et de la protection de l'information

[6] Paiements électroniques sur Internet – caractéristiques & synthèse, Ministère des Finances, Québec, p. 10.
[7] Principes et critères *WebTrust* SM/MD pour le commerce électronique entre entreprises et consommateurs, Version 2.0, Le 15 octobre 1999, p. 7

2.2 La certification : un outil de partage de risque

Comme nous l'avons défini auparavant, la certification est un outil de partage de risques mais elle n'en précise pas le niveau de partage de risques. Si le niveau de partage de risques n'est pas connu, il est impossible de déterminer la force de l'outil de confiance. Le niveau de partage de risque dépend de la qualité de la certification qui, elle, dépend de la rigueur du processus de certification.

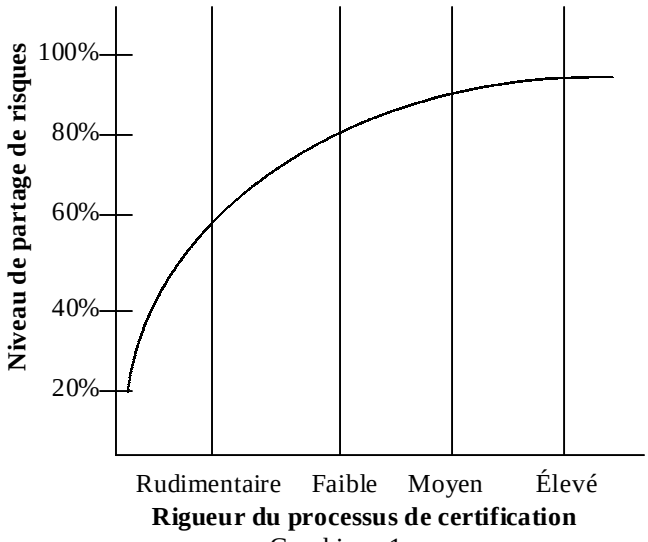
Nous pouvons illustrer la certification de sites Web de la façon suivante. Le marché, c'est-à-dire les consommateurs, les partenaires d'affaires ou les citoyens, manifeste un besoin d'assurance afin de transiger en ligne avec le détaillant, le fournisseur ou le gouvernement. Ce besoin vient essentiellement d'un manque de confiance réel ou perçu concernant un ou plusieurs aspects de la relation. Une façon de répondre à ce besoin est d'assurer le client, partenaire ou citoyen que des mesures de contrôle sont en place pour éviter quelque non-respect que ce soit dans la relation. En guise d'exemple, quatre niveaux d'assurance pouvant être atteints grâce à la certification seront décrit dans les paragraphes qui suivent.

Au premier niveau, le commerce n'est pas certifié. Le détaillant indique seulement parmi ses conditions de vente en ligne qu'il s'engage à respecter les conditions de crédit telles que décrites sur son site Web. Pour le client, le niveau d'assurance apporté par une telle déclaration est assez faible. En effet, le consommateur connaît les conditions de crédit et doit se fier à la bonne foi du marchand. En cas de litige, le consommateur fera valoir que les conditions étaient décrites et qu'il s'est fié à l'information présentée.

Ce même détaillant pourrait également obtenir un sceau de certification auprès d'une tierce partie indépendante qui offre un service de certification. Il est possible de distinguer deux types de service de certification. Dans un premier cas, une entreprise peut obtenir un sceau de certification auprès d'une société qui appose un sceau de confiance après avoir demandé aux marchands de se conformer aux normes qu'elle prescrit. Afin de s'assurer que les marchands se conforment aux normes, cet organisme de certification se fie à l'auto-déclaration de son client et le marchand doit débourser une somme prédéterminée pour obtenir le sceau. Nous qualifions le niveau d'assurance atteint par ce type de certification de bas à moyen.

Dans un deuxième cas, une organisation peut obtenir un sceau de certification auprès d'une tierce partie indépendante qui, avant d'apposer son sceau, se livre à un processus de vérification de conformité aux normes prescrites. Ce modèle de certification sera plus amplement décrit plus loin. Pour le moment, nous nous contenterons de qualifier le niveau d'assurance ainsi atteint de moyen à élevé.

Enfin, un organisme de certification pourrait garantir les faits et gestes d'un marchand dûment enregistré auprès de lui. Ce mode de fonctionnement permet d'atteindre un niveau élevé de certification. La relation entre la rigueur du processus de certification et le niveau de partage de risques ou encore le niveau d'assurance atteint peut se présenter ainsi (voir le Graphique 1) :



Graphique 1

La rigueur du processus dépend de son mode de fonctionnement. Selon Michel Royon[8], l'organisation des activités de certification apparaît comme particulièrement complexe du fait de la multiplicité des fonctions et des acteurs qui interviennent dans chaque système. Cependant, tout processus devrait comprendre au moins trois niveaux qui correspondent chacun à une fonction bien spécifique. Ces fonctions sont : la production de normes, la certification de conformité et l'accréditation des organismes certificateurs (voir le Schéma 3).

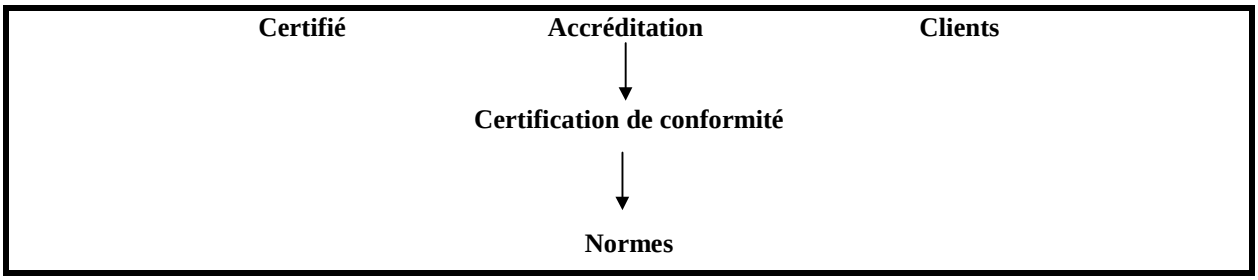


Schéma 3

3 Normes

3.1 Le processus de normalisation

Selon l'Organisation internationale de normalisation (ISO), les normes sont des accords documentés contenant des spécifications techniques ou autres critères précis destinés à être utilisés systématiquement en tant que règles, lignes directrices ou définitions de caractéristiques pour assurer que les matériaux, produits, processus et services sont aptes à leur emploi[9].

[8] Michel ROYON, L'émergence de système nationaux de normalisation/certification et leur connexion internationale, *Revue internationale de droit économique*, 1999, pages 107 à 118.
[9] http://www.iso.ch/info/intro.html

Quel que soit le processus de normalisation, les normes doivent répondre à quatre critères de base : elles doivent être objectives et vérifiables, publiques, justes et crédibles. Avant de devenir des normes, certaines affirmations ne sont que des principes. Certaines organisations préfèreront donc parler de principes et de critères. Dans ce cadre, on pourra définir l'émission de principes par des énoncés généraux encadrant les pratiques relativement au commerce électronique.

On entend par processus de normalisation, le mode de fonctionnement retenu par une organisation pour établir des normes. Il existe plusieurs modèles de normalisation. Nous les avons regroupés en cinq catégories afin de faciliter la compréhension du texte sans toutefois penser que cette catégorisation ne puisse laisser place à d'autres modèles de processus de normalisation.

D'abord, il existe le modèle international élaboré par l'ISO, le modèle le plus connu. ISO est une fédération mondiale regroupant des organismes nationaux de normalisation. Son objectif est de développer des normes techniques volontaires donnant une valeur ajoutée à tous les types d'activités économiques. Les normes ISO contribuent à un développement, à une production et à une livraison des produits et services plus efficaces, sûrs et respectueux de l'environnement ainsi qu'à des échanges facilités et plus équitables entre les pays. Les normes ISO servent également à protéger les consommateurs et les utilisateurs en général, des produits et services non conformes, ainsi qu'à leur simplifier la vie.

Ensuite, on retrouve un modèle développé par des associations professionnelles. Par exemple, l'American Institute of Chartered Public Accountants (AICPA) et l'Institut canadien des comptables agréés (ICCA) représentent deux organisations regroupant des comptables agréés dans chacun des deux pays. À la différence de l'ISO, les membres de l'IACPA et de l'ICCA sont essentiellement des comptables agréés c'est-à-dire des membres d'une même profession. Leur processus de normalisation est un processus interne mais sollicitant la participation de non-membres intéressés par ces normes soit en tant qu'utilisateurs ou en tant qu'experts. Quoique différent, ce processus de normalisation est caractérisé par le développement de normes par des experts et un processus d'approbation formel des normes par les membres lors d'un vote.

Lorsque plusieurs organisations d'un même secteur industriel consentent à suivre les mêmes critères, nous parlerons de normalisation sectorielle. Il s'agit donc du développement de standards industriels. Par exemple, l'industrie automobile a développé des normes sectorielles et a même établi une co-entreprise ayant pour but de fournir l'infrastructure technologique nécessaire au déploiement du commerce électronique. Antérieurement à Internet, les normes sectorielles EDI sont un parfait modèle de ce type de normes.

Le modèle privé est caractérisé par un processus de normalisation initié et entièrement contrôlé par une société privée ou un regroupement de sociétés privées. L'objectif poursuivi par les normes élaborées est certes l'amélioration d'un produit ou d'un service. Cependant, ces sociétés poursuivent également un objectif commercial et n'ont pas de contraintes aussi nombreuses à respecter. Les normes ainsi élaborées peuvent être beaucoup plus sévères parce qu'elles n'ont pas à tenir compte des commentaires de différents intervenants et n'ont pas à atteindre une forme de consensus. En même temps, elles doivent tout de même tenir compte des contraintes de marché. Ces contraintes peuvent également mener à l'excès contraire c'est-à-dire à une certaine forme de laxisme au niveau des normes elles-mêmes. La qualité des normes dépend essentiellement de la société qui en fait l'élaboration et la promotion.

Finalement, il existe aussi un modèle gouvernemental qui consiste en un processus d'élaboration de normes relevant de l'État. Ce dernier doit non seulement se comporter en consommateur et commerçant modèle, mais il doit de plus aller à l'avant-garde des attentes de la population. Quand le citoyen transige avec le gouvernement, il s'attend à d'avantage de sécurité et de confidentialité qu'avec un simple commerçant.

3.2 La certification de conformité

La certification a été définie antérieurement comme une affirmation au certifié qu'il se conforme à des normes établies. Mais quels sont les moyens disponibles permettant au certifiant de faire une telle affirmation?

Dans un premier temps, il est important de bien définir les parties en cause. En effet, il s'agit d'une relation impliquant trois parties, chacune ayant ses droits et ses obligations (voir le Schéma 4).

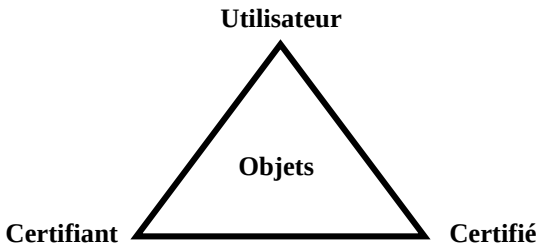


Schéma 4

3.2.1 Normes / critères

Appliqués à la certification de conformité de sites Web, les utilisateurs représentent soit les consommateurs dans un contexte de relation entreprise/consommateur, soit une autre entreprise dans la relation entreprise/entreprise, soit le citoyen ou encore une entreprise dans la relation gouvernement/citoyen ou entreprise. Le certifié pour sa part est l'organisation qui désire obtenir le sceau de certification soit une entreprise, soit le gouvernement. Le certifiant représente la personne ou l'organisation autorisée à octroyer le sceau de certification. Les objets font référence aux produits ou aux attributs sur lesquels le certifiant offre un degré d'assurance en relation avec les normes définies par l'organisme certifiant. Enfin, les normes sont des points de référence auxquels seront comparés les objets du certifié. Le graphique 1 n'explique cependant pas le processus de certification lui-même c'est-à-dire les procédés appliqués par le certifiant pour être en mesure d'assurer que les objets du certifié sont conformes aux normes du certifiant. Deux modèles sont retenus pour expliquer ce processus. Les deux modèles reposent sur l'hypothèse que le certifiant développe ses propres normes ou fait référence à des normes reconnues.

3.3 Les modèles de certification

3.3.1 Auto-déclaration

Certains organismes offrent un sceau de certification par auto-déclaration. Le commerçant déclare être conforme aux normes édictées par l'organisme et, moyennant rémunération, peut par la suite afficher le sceau de certification prévu. Ce type d'auto-déclaration ne comporte pas de valeur intrinsèque, mais peut porter le consommateur à se croire en toute sécurité.

Selon le modèle de l'auto-déclaration, le certifiant ayant en main les normes du certifiant confirme par écrit à ce dernier qu'il se conforme à celles-ci. Dans le cas de non-conformité, le certifié doit, avant d'obtenir son sceau, effectuer les modifications nécessaires pour se conformer aux normes. La caractéristique de ce processus de certification est qu'il est essentiellement basé sur l'honnêteté du certifié. Cependant, le certifiant met souvent en œuvre d'autres processus de contrôle afin de s'assurer que son sceau n'est affiché que par des clients dignes de le conserver. À titre d'exemple, BBBOnline a développé un mécanisme de contrôle des plaintes lui procurant ainsi une assurance raisonnable que ses membres se conforment à ses standards d'éthique.

Même si ce modèle de certification fait en sorte qu'il n'y ait pas de vérification du site Web du certifié, il demeure tout de même qu'il permet au certifié de prendre connaissance des normes et l'oblige à s'y confirmer. La valeur du sceau de certification dépend également de la réputation du certifiant. Si l'on reprend BBBOnline à titre d'exemple, il s'agit d'une organisation qui a fait ses preuves par le passé et qui a tout à perdre si elle s'associe à des sites Web non conformes à ses propres normes. En certifiant ces sites Web, BBBOnline assume également une part du risque.

3.3.1.1 Auto-déclaration avec validation

Les dirigeants d'une organisation désirant être certifiée font une déclaration dans laquelle ils confirment que l'organisation est conforme aux normes prescrites, laquelle déclaration fait par la suite l'objet d'une validation par le certifiant. Si l'organisation n'est pas en mesure de confirmer qu'elle respecte les normes, elle doit tout d'abord faire les modifications qui s'imposent. Pour valider l'assertion du certifié, le certifiant obtient toutes les informations probantes dont il a besoin pour se faire une opinion au sujet de la conformité du site Web aux normes établies. Pour obtenir les informations dont il a besoin, le certifiant utilise divers moyens dont : l'inspection, la prise de renseignements, la demande de confirmation, les tests de contrôle et l'analyse.

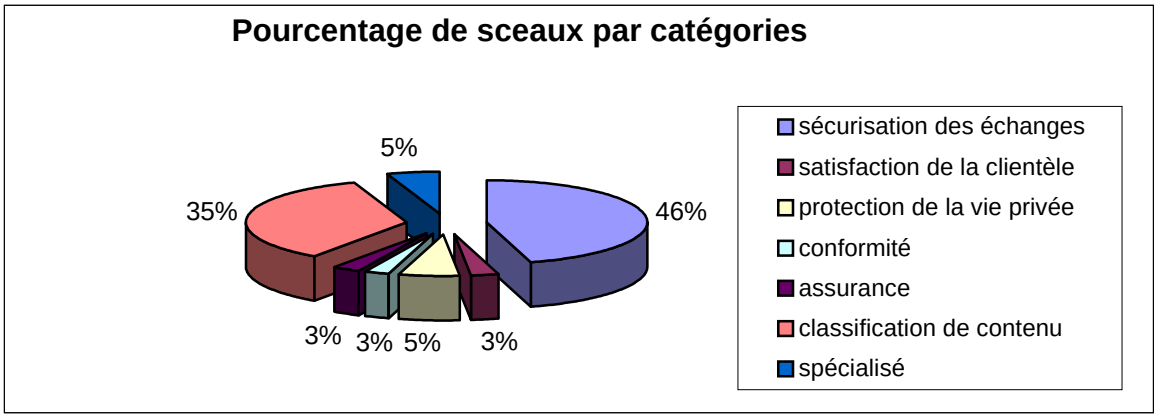
Quel que soit le modèle de certification retenu, il est primordial qu'il soit appliqué de façon continue et objective. Les systèmes d'information et de communication évoluent tellement rapidement qu'il est impensable de penser qu'un système ne subira aucun changement pendant une période plus ou moins longue. Ainsi, tout sceau de certification s'applique à un système à une date donnée et il faut donc que le certifiant mette en place un processus continu d'évaluation de la conformité afin d'être en mesure de continuer à octroyer le sceau sans prendre de risques indus. L'objectivité signifie qu'avec les mêmes renseignements, deux certifiants arriveraient à la même conclusion.

3.4 Typologie des sceaux de certification de sites Web

Les lignes qui suivent décrivent les sceaux de certification recensés selon les variables mentionnées et en fonction des caractéristiques certifiées par ces différents sceaux. Sans prétendre avoir recensé tous les sceaux, 170 sceaux ont été recensés au cours de l'été 2001[10]. En fonction de leurs attributs, il est possible de classer les sceaux de certification selon les sept grandes catégories suivantes (voir le Graphique 2) :

[10] Pour chaque sceau, on a produit une fiche signalétique décrivant son fonctionnement, son processus d'obtention et sa couverture. Ces informations sont disponibles sur le site www.sceauxdecertification.org .

- sceaux de sécurisation des échanges électroniques
- sceaux de satisfaction de la clientèle ou encore de classification des marchands
- sceaux de protection de la vie privée
- sceaux de conformité
- sceaux d'assurance
- sceaux de classification du contenu offensant
- sceaux spécialisés



Graphique 2

Les *sceaux de sécurisation des échanges électroniques* (46 %), indiquent aux intervenants que la société, publique ou privée, avec laquelle ils font affaires a mis en place des mécanismes de contrôle permettant d'assurer soit l'authentification des parties, la transmission sécuritaire des informations, la sauvegarde sécuritaire des informations ou encore la sécurité des paiements. Il s'agit de sociétés qui émettent des certificats numériques ou qui ont développé d'autres mécanismes de contrôle et qui permettent à l'entreprise cliente d'afficher un sceau à cet effet.

Les *sceaux de satisfaction de la clientèle* (3 %) visent à augmenter la confiance des consommateurs en privilégiant la divulgation d'informations concernant l'expérience réelle d'achat des consommateurs. Les partisans de cette approche croient que le marché du commerce électronique ne prendra son essor véritable que lorsque les consommateurs auront suffisamment confiance pour faire des achats réguliers dans des magasins virtuels. Un des critères importants pour donner cette confiance, si nécessaire à l'essor du commerce électronique, est le partage d'informations sur les expériences d'achat faites par de vrais consommateurs. Ainsi, un consommateur peut faire une recherche pour savoir si les consommateurs ont été satisfaits lors de leurs transactions avec un marchand spécifique. Les promoteurs de ces sceaux de satisfaction offrent généralement en plus un service de résolution des plaintes. Ce mécanisme encourage les consommateurs à utiliser le commerce électronique en offrant un autre outil de dernier recours pour augmenter la confiance.

Il est apparu au cours des dernières années que la confidentialité des renseignements personnels est une préoccupation majeure des consommateurs. La confidentialité ou la protection de l'information porte sur la capacité de ne révéler aux entités concernées que les informations qui sont strictement nécessaires au bon fonctionnement des transactions. Selon une étude d'Equifax, 78% des consommateurs sont préoccupés par l'utilisation que font les entreprises de leurs données personnelles[11]. Les *sceaux de protection de la vie privée* (5 %)

[11] Milne, G.R. et Boza, M.E. Trust and concern in consumer's perceptions of marketing information management practices, *Journal of interactive marketing*, Vol 13, 1999.

offre une certification spécifique pour garantir un contrôle sur la collecte et l'utilisation des données à caractère personnel par les entreprises œuvrant sur le Web.

Dans la quatrième catégorie, *sceaux de conformité* (3 %), nous retrouvons des sceaux qui couvrent un champ plus large de certification. L'objectif commun de ces sceaux est d'augmenter la confiance des intervenants en offrant aux vendeurs d'afficher un sceau de certification assurant aux consommateurs que le certifié se confirme à certains critères de bonnes pratiques du commerce électronique. Quoique ayant tous un même objectif, les 25 sceaux identifiés diffèrent par le nombre de critères que doivent respecter les certifiés, par le processus de développement des normes, par le processus de certification lui-même ainsi que par les agents certifiants.

Depuis deux ans, on peut signaler l'arrivée des compagnies d'assurance sur le marché de la certification, particulièrement en Europe. En plus d'attester la sécurité d'un site, ces *sceaux d'assurances* (3 %) offrent un service d'assurance et de remboursement au client et au marchand en cas de problème. D'une part, les marchands peuvent s'assurer, par exemple, contre le vol de cartes bancaires et/ou la répudiation d'une commande par un client. D'autre part, les consommateurs sont protégés contre la non-conformité d'un produit acheté, les délais excessifs, vol de cartes de crédit, etc.

Les *sceaux de classification du contenu offensant* (35 %) ont comme objectif commun la protection du public au niveau de l'accès de certaines catégories de personnes aux contenus de sites Web. Plus particulièrement, il s'agit de protéger des enfants en ce qui concerne les sites à caractère sexuel, pornographique, violent, ou encore affichant de la nudité. Il y a une véritable prolifération de sceaux dans cette catégorie. On en retrouve plus d'une soixantaine. Le grand débat qui anime les intervenants dans ce milieu est la controverse entre la liberté d'expression d'un côté et la protection des enfants de l'autre. Il est à noter que plusieurs sites pornographiques participent à un processus de certification et on assiste même à l'émergence de sceaux gérés par des membres de l'industrie pour adultes. Le but est de s'auto-réglementer afin d'éviter que l'État ne légifère mais aussi de limiter les fraudes.

Une dernière catégorie a été créé et que nous appelons *sceaux spécialisés* (5 %). Il s'agit de sceaux qui ciblent un secteur ou un groupe d'utilisateurs très précis : sites médicaux, sites religieux, sites pour les personnes non-voyantes, etc. La plupart du temps, ces sceaux accordent une attention particulière à la qualité du contenu du site à certifier. Par exemple, pour garantir la validité des informations contenues sur un site médical, TRUSTe a créé un sceau spécialisé dans le domaine de la santé. Pour afficher ce sceau sur un site, les renseignements présentés et les services offerts doivent être en accord avec les pratiques professionnelles reconnues.

4 Conclusion

Sur le plan théorique, la certification de sites Web constitue un excellent outil pour augmenter la confiance des consommateurs envers le commerce électronique et pour partager les risques liés au commerce électronique. Il s'agit pour le propriétaire du site Web de s'associer à une marque externe ou une pratique reconnue afin de bénéficier de son capital de confiance et développer ainsi la confiance du consommateur ou de l'utilisateur par le biais d'un référentiel.

Entièrement basé sur un lien de confiance, l'avenir de la certification de sites Web repose sur la capacité des certifiants de se faire connaître des consommateurs. Pour qu'une certification devienne une valeur ajoutée dans le processus d'achat sur le Web, les consommateurs doivent être préalablement informés et avoir développé une confiance envers les normes et standards liés à l'émission des sceaux. Un sceau doit avoir acquis une certaine notoriété auprès du public afin qu'il puisse augmenter la confiance des consommateurs envers des marchands qu'ils ne connaissent pas.

Or, le problème réside précisément dans le fait que très peu de consommateurs connaissent les sceaux de certification. Jusqu'à présent, à l'exception de BBBOnline qui est connue par 36% des internautes américains, aucun sceaux n'a acquis cette notoriété et crédibilité nécessaire auprès du public. De plus, la multiplication des sceaux et la non-existence de normes communes ont créé une véritable confusion aux yeux du public. Chaque organisme, public ou privé, émet son sceau de certification en fonction de ses propres normes et standards. Comment le consommateur pourra-t-il s'y retrouver devant la prolifération de sceaux comportant différentes caractéristiques et offrant différents niveaux de protection?

Malgré la popularité croissante des sceaux de certification, aucune étude empirique n'a été effectuée sur le sujet. Nous ne connaissons ni le nombre de sites transactionnels certifiés, ni dans quel secteur ils sont et encore moins s'ils ont réussi à atteindre leur objectif de sécuriser les consommateurs. La suite de notre étude propose donc de combler certaines de ces lacunes. Les principaux objectifs que nous nous sommes fixés sont de : 1) déterminer la perception qu'ont les internautes et le public en général sur les sceaux de certification et; 2) vérifier empiriquement si la certification d'un site Web crée effectivement une valeur ajoutée pour les consommateurs et pour les organisations.

Références bibliographiques

Cheskin Research, *Trust in the Wired Americas*, July 2000, 32 pages.

Royon, Michel. «L'émergence de systèmes nationaux de normalisation/certification et leur connexion internationale», *Revue internationale de droit économique*, 1999, p. 107-118.

Http://www.cse.dnd.ca/cse/francais/Manuels/mg4int-f.htm.

Centre de recherche en droit public, Centre de recherche informatique de Montréal, HEC Montréal. *La sécurité et la certification de conformité des sites Web*, juillet 2000, p. 20.

WebTrust. *Principes et critères WebTrust SM/MD pour le commerce électronique entre entreprises et consommateurs*, version 2.0, 15 octobre 1999, p. 7.

Deloitte & Touche et Information Systems Audit and Control Foundation. *E-Commerce Security, A Global Status Report*, United States, 2000, 88 pages.

US Department of Commerce Report. *The Merfing Digital Economy*, 1998.

Http://www.iso.ch/info/intro.html

Http://www.sceauxdecertitifaction.org

Milne, G.R. et M.E. Bosa. *Trust and Concern in Consumer's Perception of Marketing Information Management Practices*, Journal of Interactive Marketing, vol. 13. 1999.