Convention WIN-CRID : étude et recommandations sur la labellisation, 29 juin 1999

Gobert, Didier; Salaun, Anne; Poullet, Yves

Publication date:
1999

Document Version
le PDF de l'éditeur

Convention WIN – CRID

Étude et recommandations sur la labellisation

29 juin 1999

Auteurs : Didier GOBERT et Anne SALAÜN

Sous la direction du Professeur Yves POULLET

Contenu

1ère Partie :

Etat des lieux des initiatives en matière de labellisation

Auteurs : Didier GOBERT et Anne SALAÜN

Sous la direction du Professeur Yves POULLET

En collaboration avec Monsieur Emile PEETERS

Contenu de la 1ère partie :

1. Initiatives de labellisation opérationnelles

- WebTrust
- BBB OnLine
- Sello de Garantía de la Proteccion de Datos
- TRUSTe

2. Initiatives de labellisation en projet

- Globalsign
- FEDMA (Fédération Européenne de Marketing Direct)
- Ready
- Institut des Réviseurs d'Entreprise
- CRC – Centre Régional de la Consommation (France)

3. Annexes

1. Initiatives de labellisation opérationnelles

WebTrust

http://www.cpawebtrust.org
http://www.icca.ca
http://www.aicpa.org
http://www.verisign.com/webtrust/siteindex.html

INTRODUCTION

Internet offre aux consommateurs de nouveaux moyens d'obtenir des renseignements utiles, des biens et des services. Bien que cette forme de commerce électronique ait connu une croissance rapide, particulièrement par l'entremise du Web, sa croissance a été freinée par les craintes et les inquiétudes des consommateurs quant aux risques, réels ou imaginaires, du commerce électronique.

En réaction à ces craintes et à ces inquiétudes et pour accroître la confiance des consommateurs à l'égard de ce nouveau marché électronique, les experts-comptables ont élaboré et font connaître le présent ensemble de principes et de critères pour le commerce électronique entre les entreprises et les consommateurs, les «Principes et critères *WebTrust* », et le label de certification *WebTrust* qui s'y rattache, aussi appelé CPA WebTrust ou CA WebTrust. Les cabinets d'experts-comptables et les praticiens qui ont reçu un permis autorisant la prestation du service WebTrust de l'American Institute of Certified Public Accountants (AICPA), de l'Institut Canadien des Comptables Agréés (ICCA) ou d'autres organismes nationaux autorisés (les «praticiens») sont en mesure d'offrir des services de certification afin d'évaluer et de contrôler dans quelle mesure un site Web donné respecte ces principes et ces critères. Le label de certification WebTrust est une représentation graphique d'un rapport sans réserve délivré par un praticien. Il indique également aux clients qu'il leur faut cliquer pour vérifier le label et pour voir le rapport du praticien. Ce label peut être affiché sur le site Web, avec des liens donnant accès au rapport du praticien et à d'autres renseignements pertinents.

1. - LES INTERVENANTS DE LA LABELLISATION

L'utilisation du label *WebTrust* suppose l'implication de quatre intervenants :

- les initiateurs des principes et critères *WebTrust* : l'ICCA et l'AICPA ;
- les auditeurs : les CA et les CPA ;
- le gestionnaire du label : Verisign ;
- le demandeur du label : l'entité.

1.1. - Initiateurs des principes et critères *WebTrust*

Le 16 septembre 1997, l'institut Canadien des Comptables Agréés (ICCA) et l'American Institute of Certified Public Accountants (AICPA) ont annoncé la création d'un label de certification pour le commerce électronique baptisé *WebTrust.* Cette initiative a été mise sur pied dans le but d'essayer de développer le commerce électronique entre entreprises et consommateurs.

A cet effet, l'ICCA et l'AICPA ont élaboré les principes et critères *WebTrust* (confer *infra*).

1.2. - Auditeurs

Les inquiétudes des consommateurs quant à l'intégrité, au contrôle, à l'autorisation, à la confidentialité et au caractère anonyme des opérations sont souvent légitimes. Dans un univers où l'interlocuteur demeure invisible, chacun a besoin d'obtenir une assurance d'une tierce partie objective. Cette assurance peut être fournie par un comptable agréé («CA») ou par un certified public accountant («CPA») indépendant et objectif, et constatée par l'affichage d'un label de certification *WebTrust* dans le site *Web.*

Le label de certification *WebTrust* symbolise, pour les clients éventuels, le fait qu'un CA ou un CPA a évalué les pratiques commerciales et les contrôles du site *Web* afin de déterminer s'ils sont conformes aux «Principes et critères *WebTrust*» pour le commerce électronique entre entreprises et consommateurs, et qu'il a délivré un rapport dans lequel il formule une opinion sans réserve indiquant que les principes sont respectés au regard des critères *WebTrust*.

Le choix du CA et du CPA comme auditeurs s'explique par le fait qu'ils sont des professionnels de la certification. En effet, les CA et les CPA offrent des services de certification. Leur rôle est de fournir une assurance au lecteur ou utilisateur, la plus connue étant celle qui résulte d'une vérification d'états financiers. On accorde de la valeur à une opinion de vérificateur signée par un CA ou un CPA parce que ces professionnels ont de l'expérience en matière de certification et de comptabilité financière et qu'ils sont reconnus pour leur indépendance, leur intégrité, leur discrétion et leur objectivité. En outre, les CA et les CPA se conforment à un ensemble complet de règles de déontologie et de normes professionnelles dans la prestation de leurs services. Toutefois, l'assurance fournie relativement à des états financiers n'est qu'un seul des types de service de certification que peuvent offrir les CA et les CPA. Ils sont également appelés à procurer une assurance en matière de contrôle interne et en ce qui concerne la conformité de certains éléments avec des critères déterminés. L'expérience professionnelle, l'expérience du monde des affaires, la connaissance approfondie du domaine (sécurité, vérifiabilité et contrôle des systèmes de commerce électronique) et les caractéristiques professionnelles (indépendance, intégrité, discrétion et objectivité) nécessaires dans le cadre de telles missions sont aussi les éléments clés qui permettent à un CA ou à un CPA d'évaluer de manière exhaustive et objective les risques, les contrôles et les informations sur les pratiques suivies qui sont associés au commerce électronique.

1.3. - Le gestionnaire du label

Pour le label WebTrust, Verisign (tiers indépendant) a été désigné comme gestionnaire du label.

Il appartient notamment à Verisign de :

- délivrer un certificat numérique WebTrust ;
- fournir un applet pour pouvoir afficher le label ainsi que le rapport de l'auditeur ;
- retirer l'autorisation d'utiliser le label en cas de révocation ou de non renouvellement du rapport.

1.4. - Le demandeur du label

L'entité qui désire obtenir le label WebTrust pour son site web doit effectuer sa demande auprès d'un CA ou CPA en faisant une déclaration ad hoc (confer *infra*).

2. - DOMAINES COUVERTS PAR LE LABEL

2.1. - Présentation

De différentes enquêtes menées concluant au manque de confiance des consommateurs à participer au commerce électronique, l'AICPA a identifié trois grands secteurs de risques associés au commerce électronique : les pratiques commerciales, l'intégrité des opérations et la protection de l'information. Cette constatation a débouché sur les trois « principes WebTrust ».

a) Les pratiques commerciales:

Constatation : Le commerce électronique suppose souvent des opérations entre des partenaires

inconnus. Etant 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 affaire déclarent leurs pratiques commerciales et les respectent.

De cette constatation découle le **principe** de la transparence des pratiques commerciales : l'entité s'engage à indiquer ses pratiques en matière de commerce électronique et à effectuer ses opérations conformément à ces pratiques. Par conséquent, l'entité doit indiquer convenablement ses pratiques concernant des éléments comme les commandes, les retours éventuels et les réclamations au titre d'une garantie. En outre, l'entité doit effectuer ses opérations conformément à ces pratiques. Ce principe a trait à la façon normale d'agir de l'entité en matière de commerce électronique. Il ne concerne d'aucune manière la qualité des biens ou des services, ou leur pertinence par rapport aux besoins du consommateur.

b) Intégrité des opérations

Constatation : Sans des contrôles adéquats, les opérations et les documents électroniques peuvent être aisément modifiés, perdus ou reproduits et faire l'objet d'erreurs de traitement. L'intégrité des opérations et des documents électroniques risque alors d'être mise en cause, ce qui pourrait provoquer des conflits au sujet des conditions de l'opération et de la facturation. Il est donc normal que les personnes qui envisagent d'avoir recours au commerce électronique cherchent à obtenir l'assurance que l'entité a mis en place des contrôles efficaces sur l'intégrité des opérations, qu'elle a, dans le passé, traité les opérations de façon précise, complète et rapide, et qu'elle a facturé ses clients conformément aux sommes convenues.

De cette constatation découle le **principe** du respect de l'intégrité des opérations : l'entité a mis ou s'engage à mettre en place (avant l'obtention du label) des contrôles efficaces de nature à procurer une assurance raisonnable que les commandes passées par le client par la voie du commerce électronique sont traitées et facturées comme convenu. Ces contrôles et pratiques ont notamment trait aux aspects suivants des opérations : identification appropriée de l'opération ; validation de l'opération ; exactitude, exhaustivité et rapidité du traitement de l'opération et des facturations y afférentes; indication des modalités de l'opération et de la facturation et, le cas échéant, du règlement électronique.

c) Protection de l'information : vie privée

Constatation : Il importe que les consommateurs soient persuadés que le site *Web* qu'ils consultent est identifié de manière adéquate et que l'entité a pris les mesures voulues pour protéger la confidentialité des données personnelles des clients. En effet, la confidentialité des données de nature délicate transmises par Internet peut se trouver compromise. Par exemple, sans le recours à des techniques de chiffrement élémentaires, les numéros de carte de crédit des consommateurs pourraient être interceptés pendant la transmission et volés. De même, en l'absence de coupe-feu et d'autres mesures de sécurité, des renseignements personnels d'un client qui se trouvent sur le système informatique de commerce électronique d'une entité pourraient être, délibérément ou non, mis à la disposition d'un tiers non lié aux activités de l'entité. Les entorses à la sécurité peuvent également comprendre l'accès non autorisé à des réseaux d'entreprises, à des serveurs Internet *Web* et même à la connexion Internet du consommateur (par exemple, son ordinateur à la maison). Il est donc normal que les personnes qui envisagent d'avoir recours au commerce électronique cherchent à obtenir l'assurance que l'entité a mis en place des contrôles efficaces sur la protection de l'information et

qu'elle a, dans le passé, protégé la confidentialité des données personnelles des clients.

De cette constatation découle le **principe** de la protection des données à caractère personnel : l'entité a mis ou s'engage à mettre en place (avant l'obtention du label) des contrôles efficaces de nature à procurer une assurance raisonnable que les renseignements personnels du client obtenus dans le cadre d'une opération de commerce électronique sont protégés contre toute utilisation étrangère aux activités de l'entité. Ces contrôles et pratiques ont notamment trait au chiffrement ou à d'autres modes de protection des renseignements personnels du client (numéros de carte de crédit ou données personnelles et financières) transmis à l'entité par l'entremise d'Internet, à la protection de ces renseignements une fois qu'ils ont été reçus par l'entité, et à l'obtention de la permission du client pour utiliser l'information dans un but autre que celui lié aux activités de l'entité, ou pour stocker, modifier ou copier des données provenant de l'ordinateur du client.

2.2. - Les critères WebTrust

Les principes WebTrust, évoqués ci-dessus, sont libellés en termes généraux. Pour des raisons pratiques, l'ICCA et l'AICPA ont dégagé de ces principes WebTrust une liste de critères très précis. Cette liste de critères WebTrust est disponible à l'URL suivant : http://www.icca.ca/cica/cicawebsite.nsf/public/Aproposdeswebtrust. La première version (version 1.0) date du 23 décembre 1997. Une nouvelle version vient de sortir (version 1.1) le 1er février 1999 et a été soumise à consultation.

Les points nouveaux apportés par la version 1.1 sont les suivants :

a) développement des exemples illustrant la transparence des pratiques commerciales, les contrôles relatifs à l'intégrité des opérations et les principes visant la protection de l'information pour couvrir les opérations bancaires en ligne et les entités faisant commerce des valeurs;
b) (non)prise en compte des risques liés au passage à l'an 2000 et modification du rapport de vérificateur en conséquence; et
c) dispositions concernant l'appréciation directe en application du Statement on Standards for Attestation Standards No. 9 de l'AICPA, *Amendments to Statements on Standards for Attestation Standards Nos. 1, 2 and 3,* récemment adopté. L'ICCA et l'AICPA sont conscients que des révisions ultérieures seront nécessaires pour mettre à jour les critères et la documentation connexe. En outre, ils sont conscients qu'il faudra peut-être établir des principes et critères supplémentaires pour étendre la focalisation aux opérations interentreprises et à d'autres aspects du commerce électronique.

Les critères *WebTrust* ont été élaborés afin de fournir des indications plus précises au sujet du respect des principes *WebTrust.* Ces critères constituent une base de référence au regard de laquelle une entité peut faire une auto-évaluation de la façon dont elle se conforme aux principes. Il s'agit en outre d'un ensemble cohérent de critères de mesure applicables par les praticiens aux fins de l'essai et de l'évaluation des sites *Web.*

Dans la version 1.1, une disposition sur quatre colonnes a été utilisée pour présenter les critères (voir http://www.icca.ca/cica/cicawebsite.nsf/public/Aproposdeswebtrust). La première colonne présente les critères en tant que tels, c'est-à-dire les conditions auxquelles l'entité doit répondre pour être en mesure de démontrer que le principe a été respecté. Les deuxième, troisième et quatrième colonnes fournissent des exemples d'informations et de contrôles relatifs au commerce de biens de consommation et de services non financiers, aux opérations bancaires en ligne et au commerce de valeurs en ligne, respectivement. Il s'agit d'exemples d'informations que l'entité peut fournir ou de

contrôles qu'elle a pu mettre en place afin de se conformer aux critères. Des informations et contrôles différents ou supplémentaires peuvent également être valables.

L'entité doit être en mesure de démontrer que sur une période d'au moins deux mois:

1) elle a réellement effectué ses opérations conformément aux pratiques de commerce électronique indiquées;
2) ses contrôles ont fonctionné efficacement;
3) elle avait en place un environnement de contrôle propice à la communication d'informations fiables sur ses pratiques commerciales et à l'application de contrôles efficaces; et
4) elle avait en place des procédures de surveillance permettant d'assurer que les pratiques commerciales indiquées sont toujours suivies et que ses contrôles continuent d'être efficaces.

Ces dernières notions constituent une partie intégrante des critères *WebTrust.*

3. - PROCEDURE D'ATTRIBUTION DU LABEL

3.1. - Démarche initiale

Pour obtenir un label WebTrust, la démarche doit émaner de la direction de l'entité qui demande ce label pour son site web. Concrètement, cette dernière fait une déclaration au praticien (CA ou CPA)[1].

Dans le cas d'une déclaration initiale, la durée de la période couverte devrait être d'au moins deux mois ou peut-être davantage selon ce que déterminera le praticien. Dans le cas des déclarations ultérieures, la période couverte devrait avoir comme point de départ la fin de la période précédente, de manière à éviter toute rupture de continuité entre deux déclarations.

Pour que la déclaration soit fondée, la direction de l'entité doit s'être dotée d'une structure de contrôle interne appropriée pour ses opérations de commerce électronique.

Un praticien indépendant, objectif et bien informé contrôle par sondages la validité d'une telle déclaration en se fondant sur les normes professionnelles de l'ICCA ou de l'AICPA, et fournit une opinion professionnelle qui ajoute à la crédibilité des déclarations de la direction de l'entité.

3.2. - Conditions d'obtention du label

---

[1] Cette déclaration ressemble à celle-ci :
« Dans son site Web consacré au commerce électronique (à l'adresse www.abc.com), la société ABC:
- a indiqué les pratiques qu'elle a adoptées pour ses opérations de commerce électronique et a effectué ses opérations conformément à ces pratiques,
- a mis en place des contrôles efficaces de nature à procurer une assurance raisonnable que les commandes passées par le client par la voie du commerce électronique ont été traitées et facturées comme convenu,
- a mis en place des contrôles efficaces de nature à procurer une assurance raisonnable que les renseignements personnels du client obtenus dans le cadre d'une opération de commerce électronique sont protégés contre toute utilisation étrangère aux activités de ABC, pour la période allant du JOUR MOIS 199X au JOUR MOIS 199Y, en conformité avec les critères WebTrust établis conjointement par l'ICCA et l'AICPA. »

Pour obtenir le label de certification *WebTrust,* l'entité doit respecter tous les principes *WebTrust.* L'évaluation se fait par référence aux critères *WebTrust* associés à chacun de ces principes. De plus, l'entité doit:

1) faire appel à un CA ou à un CPA à qui l'ICCA ou l'AICPA a expressément délivré un permis autorisant la prestation du service *WebTrust;*
2) obtenir un rapport sans réserve de ce praticien[2].

Si le rapport du praticien est émis sans réserve, ce dernier avise le gestionnaire du label (Verisign) que le label ainsi que son rapport peuvent être affichés sur le site web de l'entité. Il appartient également à l'entité de demander et obtenir du gestionnaire du label un certificat WebTrust de classe 3 afin de permettre au utilisateur d'authentifier ce label.

Verisign dispose d'une page sur son site avec les différentes entreprises qui ont obtenu le label WebTrust (http://www.verisign.com/webtrust/siteindex.html).

3.3. - Conditions de conservation du label

Une fois le label obtenu, l'entité peut continuer de l'afficher dans son site *Web* si les conditions suivantes sont remplies.

Premièrement, le praticien met *périodiquement* à jour sa certification de la déclaration. Dans tous les cas, l'intervalle séparant deux mises à jour ne saurait excéder trois mois, mais il sera souvent considérablement plus court. L'intervalle entre les mises à jour est fonction d'éléments tels que les suivants:

- la nature et la complexité des activités de l'entité;
- la fréquence des changements importants apportés au site *Web;*
- l'efficacité relative des contrôles de surveillance et de gestion des changements que l'entité a mis en place pour assurer le respect continu des critères *WebTrust* chaque fois que des changements sont apportés au site *Web;*
- le jugement professionnel du praticien.

Par exemple, les mises à jour seront plus fréquentes dans le cas du site *Web* en constante évolution d'une institution financière dans lequel s'effectuent des opérations sur des titres que dans le cas d'un service en ligne qui vend des données d'archives dans un site *Web* rarement modifié.

Deuxièmement, l'entité s'engage à informer le praticien, entre deux mises à jour, de tous les changements importants apportés à ses politiques commerciales, à ses pratiques, à ses processus et à ses contrôles dans la mesure où ces changements sont susceptibles d'influer sur la capacité de l'entité de continuer à respecter les «Principes et critères *WebTrust»,* ou sur la manière dont ils sont respectés. En cas de tels changements, il pourrait s'avérer nécessaire de procéder à une mise à jour de la certification ou, dans certaines situations, au retrait du label jusqu'à ce qu'une vérification de mise à jour soit possible. Lorsque le praticien découvre qu'un tel changement s'est produit, il détermine s'il doit effectuer une vérification de mise à jour et s'il s'avère nécessaire de retirer le label de certification jusqu'à l'achèvement de la vérification de mise à jour et la délivrance du rapport de vérificateur mis à jour.

---

[2] Un questionnaire d'auto-évaluation (qui se trouve en annexe) devrait aider la direction de l'entité à établir le bien-fondé de ses assertions (de sa déclaration).

4. - PROCESSUS DE GESTION ET SECURISATION DU LABEL

4.1. - Processus de gestion du label

Le label de certification *WebTrust* est géré par un tiers de confiance : Verisign (le «gestionnaire de label»), selon certaines lignes directrices.

a) Obtention du certificat associé au label

Avant d'afficher la label, il est nécessaire que l'entité demande et obtienne un certificat spécial de catégorie 3 (special Class 3 Certificate) - soit le certificat numérique *WebTrust* - du gestionnaire de label.

Si l'entité reçoit un rapport sans réserve, le praticien avise le gestionnaire de label que le label peut être affiché sur le site *Web* de l'entité, avec une identification numérique précise, et fournit une date d'expiration.

De plus, le praticien ou le gestionnaire de label fournit un applet (mini-application informatique utilisée sur le *Web)* à l'entité. L'applet indique à la page *Web* de communiquer avec le gestionnaire de label et, si l'autorisation a été accordée, d'afficher le label et les liens hypertextes associés au rapport du praticien et à toute autre information pertinente.

b) Retrait, révocation du label

Si pour une raison valable, le praticien décide que le label doit être retiré du site *Web* de l'entité, il en avise l'entité et demande que le label et le rapport connexe du praticien soient retirés du site *Web.*

Le praticien envoie aussi un avis de révocation de l'autorisation d'affichage du label au gestionnaire de label, ce qui entraîne la révocation électronique du label et empêche l'entité de continuer à l'afficher.

c) Expiration du label

A moins qu'un avis de mise à jour ne soit reçu, l'autorisation d'afficher le label prend fin. Dès lors, le site *Web* se voit demander de retirer le label et le rapport du praticien. Le gestionnaire de label, pour sa part, retire l'autorisation d'afficher le label à compter de la date d'expiration.

4.2. - Authentification du label

Pour vérifier l'authenticité d'un label affiché dans un site *Web,* le client peut cliquer sur le label afin de faire apparaître une représentation graphique d'un certificat. Ce certificat graphique indique au client comment procéder pour visualiser, à l'aide de son navigateur, le certificat numérique spécial *WebTrust* attribué par le gestionnaire de label. Ce certificat numérique fournit au client une preuve de la validité du label *WebTrust.*

Il indique que le label ainsi que le certificat ont été délivrés par Verisign, que le label a été délivré à la suite d'une vérification WebTrust, à qui le certificat et le label ont été délivrés, et comment entrer en communication avec l'entreprise à qui le certificat a été accordé (l'établissement de l'entreprise qui a obtenu le label est également indiqué). **En l'absence de ce certificat numérique, le** label ***WebTrust*** **ne doit pas être considéré comme valide.**

BBB OnLine

http://bbbonline.org

I. - LES INTERVENANTS

L'initiative BBB OnLine met en jeu les intervenants suivants :

- l'initiateur du label : les 'Better Business Bureaus',
- les demandeurs du label : les sites Web

1. - L'initiateur du label : les Better Business Bureau

BBB OnLine – Better Business Bureau – est une initiative créée en avril 1997 par le Conseil des BBB qui chapeaute les 135 BBB existants aux Etats-Unis depuis 86 ans. La création de BBB OnLine répond au souhait de promouvoir la confiance des consommateurs dans le commerce électronique. La mission que s'est donnée BBB OnLine est de créer un contexte de confiance sur Internet. Une étude réalisée dans le but de connaître le comportement des consommateurs vis à vis du commerce sur Internet a permis de mettre en évidence leur principales craintes, à savoir :

- la *sécurité*, liée principalement au risque dans la transmission du numéro de carte de crédit ;
- la *fiabilité des sites* ; et
- la *protection de la vie privée*.

Afin de répondre à ces craintes qui risquent d'entraver le développement du commerce sur Internet, BBB OnLine a créé trois labels, l'un garantissant la fiabilité du site, l'autre assurant un engagement en matière de protection des données personnelles et un troisième attestant d'un engagement plus spécifique relatif aux enfants. BBB OnLine propose également des conseils aux consommateurs ainsi qu'un système de traitement des plaintes. L'ensemble de ces services est basé sur un principe d'auto-réglementation qui s'inscrit dans la lignée de l'expérience des BBB dans le monde 'off-line', laquelle a permis de construire une crédibilité reconnue qui est désormais utilisée dans le monde 'on-line'.

BBB OnLine avance des résultats de ses initiatives : 84 % des internautes admettraient que la reconnaissance des sites par un tiers reconnu augmenterait leur confiance vis à vis de ses sites, notamment vis à vis des sites qu'ils ne connaissent pas ; 78 % estimeraient qu'une assurance de la fiabilité du site les inciteraient à acheter davantage.

2. - Les demandeurs du label

Les sites qui souhaitent bénéficier du label BBB OnLine doivent s'identifier et suivre la procédure ad hoc (voir informations infra). Seuls les sites dont les services sont destinés au territoire américain peuvent bénéficier du label.

Le label n'est pas attribué aux sites qui diffuseraient un contenu illicite, obscène, diffamatoire ou dont l'activité nuirait au label de BBB OnLine.

3. – Autres intervenants ?

Aucun autre intervenant dans la procédure d'attribution ou de gestion du label n'est mentionné sur le site de BBB OnLine.

II. - LES DOMAINES COUVERTS

Trois labels sont proposés par BBB OnLine :

- le label 'reliability',
- le label 'Privacy',
- le label 'Kid's Privacy'.

1. - Reliability label

Pour pallier à la difficulté majeure qu'est l'identification des vendeurs électroniques, BBB OnLine propose le label *'reliability'* afin, d'une part, d'aider les utilisateurs à trouver des sites fiables, dignes de confiance, et, d'autre part, de permettre aux vendeurs de s'identifier en tant que professionnels sérieux. Le tout est basé sur une démarche volontaire d'autorégulation qui permet d'éviter une intervention étatique sur Internet.

Le label placé sur le site Web offre aux internautes la possibilité d'obtenir des informations sur le site labellisé par un simple click, et d'être ainsi assurés de la fiabilité du site. BBB OnLine permet à ses utilisateurs d'accéder à une *base de données* via un moteur de recherche qui recense tous les participants au service BBB OnLine. Une liste alphabétique des participants est également proposée.

Les arguments commerciaux avancés pour inciter les sites à demander le label sont les suivants :

- donner aux consommateurs l'image d'un professionnel fiable;
- se distinguer par rapport à ses concurrents ;
- être intégré à la base de données de BBB OnLine ;
- montrer son engagement envers des principes de publicité loyale, de traitement honnête des clients, d'autorégulation ;
- participer au développement de la confiance des consommateurs sur Internet.

BBB OnLine avance le chiffre de 2.800 sites qui utiliseraient le label de fiabilité.

2. - Privacy label

Le but 'privacy' du label est de fournir aux consommateurs le degré le plus élevé de sécurité quant à l'utilisation de leurs données personnelles.

La politique du site relative à la vie privée est d'abord vérifiée par BBB OnLine, puis une estimation de l'application effective de la politique annoncée est effectuée. BBB OnLine propose un programme complet de règlement des litiges permettant aux consommateurs d'adresser des plaintes contre les sites qui ne respecteraient pas les engagements pris en matière de protection de la vie privée. Le but est de s'assurer que les sites qui affichent le label vie privée « disent ce qu'ils font, font ce qu'ils disent et se soumettent à un contrôle indépendant ».

Le programme relatif à la protection de la vie privée offre les services suivants :

- il accorde un label facilement reconnaissable aux sites qui respectent la politique à l'égard de la protection des données personnelles ;
- il fournit aux consommateurs un mécanisme aisé de règlement des différents ;
- il assure un suivi rigoureux du respect des engagements par les sites, au minimum une fois par an ;
- il offre des sanctions efficaces contre un non respect des engagements telles que le retrait du label et une publicité auprès des administrations concernées.

Les critères à respecter sont les suivants :

- attester l'adoption d'une politique de protection des données et de mesures de sécurité. Cette politique doit être clairement indiquée sur le site ;
- coopérer dans la procédure de vérification, à savoir fournir les informations relatives à l'accès aux données individuelles, au transfert des données à des tiers, à l'intégrité des données, à la sécurité des données, etc.
- participer au programme de résolution des litiges ;
- garantir la sécurité des données collectées et se prémunir contre un accès non autorisé par l'adoption de mesures de sécurité adéquates ;
- informer BBB OnLine de tout changement dans la politique à l'égard des données personnelles ;
- fournir un lien vers la politique à l'égard des données personnelles sur chaque page où des données sont collectées ;
- informer les tiers vers qui des données sont transférées de la politique en matière de vie privée ;
- exiger des tiers qui ont accès à des données qu'ils les gardent confidentielles.

3. - Kid's Privacy' label

Les sites qui proposent des produits ou des services aux enfants de moins de 13 ans, ou qui collectent des données auprès d'enfants de moins de 13 ans, doivent aussi remplir les critères du label relatif aux enfants.

Les sites dont les produits ou services sont *destinés aux enfants* sont ceux qui présentent une structure clairement destinée aux enfants, en fonction des critères tels que le sujet, l'âge des personnages, le langage, la publicité, le contexte. Les sites qui *collectent des données auprès d'enfants* sont ceux qui ne sont pas destinés principalement aux enfants mais qui collectent des données de certains de leurs visiteurs qui ont moins de 13 ans. Les sites visés sont ceux qui ont connaissance de l'âge de leurs visiteurs soit parce que le site est divisé par catégories d'âges, soit parce que les formulaires à remplir demandent l'âge du visiteur, soit parce que le site permet d'une quelconque manière de collecter des données d'enfants de moins de 13 ans.

Les critères se basent notamment sur le 'Children's Online Privacy Protection Act' de 1998. Pour obtenir le label, les sites doivent :

- obtenir l'accord des parents avant toute collecte ou utilisation de données à caractère personnel ;
- obtenir l'accord des parents avant que l'enfant ne communique d'informations ;
- fournir des avertissements et explications claires et facilement compréhensibles ;
- éviter de collecter plus d'informations que nécessaire dans le cadre d'activités destinées directement aux enfants ;
- être prudents dans le choix des hyperliens proposés ;
- suivre des règles strictes dans l'envoi de courriers électroniques ;
- fournir aux parents un accès raisonnable aux informations collectées par le biais de leurs enfants, et la possibilité de corriger ou enlever des données.

III. - LA PROCEDURE D'ATTRIBUTION

1. - Reliability label

Les sites qui souhaitent se voir attribuer le label de fiabilité doivent s'engager à respecter les standards du programme de fiabilité. Une fois attribué, le label peut être placé à tout endroit du site

Web.

La procédure à suivre est la suivante :

- devenir membre du bureau local de BBB ;
- fournir au BBB des informations concernant la société (adresse, téléphone, noms des dirigeants, etc.) : le BBB vérifie les informations fournies par une visite dans les locaux de la société ;
- exercer l'activité professionnelle en question depuis au moins un an ;
- disposer d'une procédure satisfaisante de traitement des plaintes ;
- accepter de participer au programme du BBB concernant l'autorégulation, accepter de modifier ou de retirer toute publicité qui serait en désaccord avec les règles en matière de publicité pour les enfants ;
- répondre rapidement aux plaintes des consommateurs ;
- accepter de s'engager, à la demande des consommateurs, dans une procédure d'arbitrage contraignante.

2. - Privacy label

2.1. - Procédure

La procédure d'attribution du label se déroule en deux étapes :

- dans un premier temps, les candidats doivent montrer qu'ils ont adopté et mis en œuvre une politique relative à la protection de la vie privée et des données personnelles conforme aux programmes standards de BBB OnLine en matière de vie privée[3] ;
- ensuite, les candidats doivent remplir un formulaire, un document garantissant leur conformité, signer une licence et s'acquitter du paiement du label.

Après réception de la demande et des documents, BBB OnLine procède à un examen de conformité et peut soit accorder le label, soit demander des informations complémentaires, soit informer le candidat des modifications nécessaires à apporter pour se voir attribuer le label. A titre d'illustration, BBB OnLine estime que seuls 12 à 15 % des sites audités ont nécessité un réajustement pour obtenir le label.

2.2. - Coût

Le prix du label est fonction du chiffre d'affaires de la société :

- 150 $	pour un chiffre d'affaires annuel :	inférieur à 1 million de dollars,
- 300 $		entre 1 et 5 millions de dollars,
- 500 $		entre 5 et 10 millions de dollars,
- 750 $		entre 10 et 50 millions de dollars,
- 1000 $		entre 50 et 100 millions de dollars,
- 1500 $		entre 100 et 500 millions de dollars,
- 2000 $		entre 500 et 2000 millions de dollars,
- 3000 $		supérieur à 2000 millions de dollars.

Une réduction est proposée pour les sites qui participent également au label 'reliability' : les 6 premiers mois sont gratuits.

---

[3] Les conditions relatives à la mise en œuvre d'une telle politique sont détaillées dans le paragraphe suivant.

3. - Kid's Privacy' label

L'affichage du label 'kid's privacy' dépend de la catégorie de laquelle le site relève : si le site est destiné aux enfants, il *doit* afficher le label, mais il a toutefois le choix de l'afficher seul ou avec le label 'privacy'. Par contre, s'il en fait que collecter des informations d'enfants de moins de 13 ans, il *peut décider* ou non d'afficher le label.

Les services du BBB se réservent le droit de n'attribuer aucun label – ni 'reliability' ni 'privacy' – aux sites qui soit proposent des produits ou des services aux enfants de moins de 13 ans, soit collectent des données auprès d'enfants de moins de 13 ans, et qui ne s'engageraient pas à respecter les principes relatifs aux enfants.

IV. - PROCESSUS DE GESTION ET DE SECURISATION DU LABEL

1. – Gestion du label

Le site de BBB OnLine offre la possibilité de connaître, par le biais d'un moteur de recherches, tous les sites qui affichent le label 'reliability', ce qui permet de vérifier le fonctionnement et l'utilisation du label. Par contre, cette procédure n'est pas proposée pour les deux autres labels.

Le label octroyé au site qui en fait la demande et qui respecte les critères BBB OnLine est affiché sur le site. La mention '*click to check*' apparaît sur l'icône même du label, et offre un lien vers une page appelée : « BBB OnLine Reliability – Participation Confirmed ». Cette page explique ce qu'est le label de fiabilité attribué au site et offre un lien vers le profil du participant. Ce profil contient un *formulaire type* avec les informations suivantes : les nom et adresse de la société, l'adresse Internet, le nom du responsable de la société, un point de contact pour les services clientèle, la nature des services proposés, et une partie facultative 'commentaires'.

Cette procédure est la même pour tous les sites qui affichent le label 'reliability'.

2. - Limitation de responsabilité

La page « BBB OnLine Reliability – Participation Confirmed » explique la responsabilité limitée de BBB OnLine à l'égard des sites labellisés : le simple affichage du label de BBB OnLine ne garantit pas au consommateur la satisfaction des produits ou services offerts par le site. Il est simplement précisé que les participants au label se sont engagés à respecter les standards de BBB OnLine (vers lesquels un lien est proposé), et qu'une procédure de résolution des litiges est mise en place. Une adresse électronique permet aux visiteurs qui auraient fait l'expérience de cliquer sur un label BBB OnLine sans qu'un lien les amène vers le site de BBB OnLine de le signaler.

3. – Sécurisation du label

Il n'est fait mention à aucun moment d'une autorité de certification qui viendrait délivrer un certificat pour sécuriser le label, et empêcher une utilisation frauduleuse. Il est donc difficile de se prononcer sur la sécurité du label octroyé par BBB OnLine. La question est de savoir dans quelle mesure le label peut être copié sans autorisation et sans passer par la procédure préalable mise en œuvre par BBB OnLine.

L'absence de certificat délivré par une autorité de certification semble laisser ouverte la possibilité de copier le label et de créer un lien vers une page confirmant la participation du site au programme de fiabilité, avec un lien vers le profil de la société et vers le site de BBB OnLine.

Sello de Garantía de la Proteccion de Datos

http://www.aece.org

I. - LES INTERVENANTS

1. - L'initiateur du label : l'AECE

L'AECE est l'Association Espagnole de Commerce Electronique. Elle est composée de sociétés espagnoles qui unifient leurs efforts pour développer un commerce électronique fiable et sécurisé. Née en mai 1998 grâce à l'impulsion de l'Association de Marketing Direct, l'AECE est considérée comme la principale association espagnole qui aide au développement du commerce électronique en Espagne.

Ses objectifs sont de défendre les intérêts des entreprises espagnoles face au commerce sur Internet tout en agissant pour son développement. Cela passe par la promotion de codes de conduite relatifs aux différentes activités liées au commerce sur Internet.

2. - Les demandeurs du label

Le label est ouvert aux sites espagnols de commerce électronique, que ceux-ci soient membres de l'association espagnoles de commerce électronique ou non.

II. - LE DOMAINE COUVERT

Le label proposé par l'AECE est relatif à la protection des données personnelles. Il est basé notamment sur la loi espagnole de protection des données : loi organique de régulation du traitement informatisé des données personnelles.

Les objectifs du label sont :

- d'assurer le respect par les sites qui affichent le label des principes énoncés dans le code de conduite ;
- d'informer du traitement des données obtenues sur Internet et d'offrir au consommateur la possibilité de s'opposer à un traitement.

III. - L'ATTRIBUTION DU LABEL

Le label peut être demandé à l'association par tous les sites espagnols présents sur Internet et qui utilisent, d'une manière ou d'une autre, des données personnelles. Il signifie une implication du site envers la protection de la vie privée et des données personnelles. Le label peut être accordé aux sociétés membres de l'association tout comme aux non-membres.

1. – La procédure

La procédure à suivre est la suivante :

1. solliciter l'octroi du label auprès de l'association et remplir un formulaire ad hoc ;
2. l'association envoie au demandeur le code de conduite et le contrat par lequel le demandeur doit s'engager à respecter le code ;
3. le demandeur doit signer le contrat et le renvoyer, et remplir un questionnaire pour définir et personnaliser sa politique à l'égard de la protection des données personnelles ;
4. une fois les formulaire et questionnaire remplis, ceux-ci sont introduits dans la base de données de l'association qui est en lien avec le site Internet de l'association ;

5. l'association confirme au demandeur la réception du contrat et l'enregistrement de sa politique de protection des données personnelles ;
6. le demandeur affiche le label sur la page principale de son site et sur toute page où des données personnelles sont demandées.

2. - Le prix

Une distinction est effectuée entre les sites déjà membres de l'association et les autres. Les sites déjà membres ne sont soumis à aucun paiement pour le service de labellisation. Ils peuvent utiliser gratuitement le label. Les sites non membres sont redevables d'une cotisation annuelle dont le montant varie selon le chiffre d'affaire annuel :

Pour un chiffre d'affaire annuel :

- supérieur à 5 milliards de pesetas : 90.000 pesetas,
- entre 1 milliard et 5 milliards : 60.000 pesetas,
- entre 200 millions et 1 milliard : 30.000 pesetas,
- inférieur à 200 millions : 15.000 pesetas.

Cette dernière catégorie s'applique également associations professionnelles qui ne poursuivent pas de but lucratif.

IV. - PROCESSUS DE GESTION ET DE SECURISATION DU LABEL

Un *Comité de Contrôle* est mis en place afin de contrôler le respect du code de conduite par les sites qui affichent le label. Ce Comité est composé notamment des trois associations de consommateurs qui ont participé à la rédaction du code de conduite, d'un organisme de contrôle de la publicité et de quatre représentants des entreprises.

Le Comité de Contrôle reçoit les plaintes des consommateurs relatives aux sites qui affichent le label et se sont engagées à respecter le code de conduite. Il ne traite que des plaintes relatives aux entreprises membres : les plaintes relatives aux entreprises non membres sont transmises aux associations de consommateurs.

Le Comité de Contrôle procède à un *audit périodique et aléatoire* pour vérifier que les sites qui affichent le label respectent le code de conduite.

Le site de l'AECE affiche une liste des sites qui utilisent le label, mais cette liste ne propose pas d'hyperliens vers chaque site. Une visite de quelques sites mentionnés dans la liste (comme *El Pais*, *El Mundo*, *Telefonica*) n'a malheureusement pas permis de trouver le label de l'AECE, ni de vérifier vers quel type d'information le label renvoie.

TRUSTe

http://www.truste.org

INTRODUCTION

TRUSTe est une initiative relative à la vie privée indépendante et sans but de lucre ayant pour objectifs de construire la confiance de l'utilisateur sur Internet et d'accélérer la croissance de l'industrie d'Internet. TRUSTe a notamment développé un programme de labellisation qui rencontre les préoccupations des utilisateurs en ce qui concerne le respect de leur vie privée en ligne, tout en rencontrant les besoins spécifiques de chacun des sites Web « licenciés » (labellisés). TRUSTe apparaît comme un équilibre entre d'une part, le besoin des utilisateurs de voir leur vie privée respectée sur le Web et d'autre part, le désir des sites Web de se lier uniquement à des standards découlant de l'autorégulation (sachant qui si l'autorégulation se développe efficacement, aucune initiative législative contraignante ne sera prise).

TRUSTe fut fondé par le Electronic Frontier Foundation (qui est une association sans but lucratif qui vise à promouvoir le respect de la vie privée, la liberté d'expression et la responsabilité sociale dans le nouveau média) et le CommerceNet Consortium (dont la mission est d'accélérer le développement du commerce électronique global, notamment en travaillant à la suppression des obstacles à ce développement).

L'idée de créer TRUSTe est née en mars 1996. Le 10 juin 1997, TRUSTe avait sa propre équipe, un programme complètement développé et deux auditeurs officiels (PriceWaterhouseCoopers et KPMG) et fut lancé officiellement ce jour lors d'un hearing sur la vie privée organisé par la Federal Trade Commission (FTC) américaine.

Depuis octobre 1998, TRUSTe dispose d'un nouvel accord de licence qui intègre les « pratiques d'information loyales » recommandées par la FTC et le Département de Commerce. Il incorpore également les exigences du nouveau label pour les enfants.

Le 9 mars 1999, TRUSTe a annoncé qu'il allait étendre ses activités en Europe. Cette décision est liée au fait que la directive européenne sur la protection des données à caractère personnel est désormais transposée et constitue une préoccupation de l'utilisateur d'Internet. TRUSTe travaille actuellement sur la modification de son programme afin de prendre en compte les différences culturelles et légales.

TRUSTe est actuellement le seul programme disponible commercialement qui s'occupe de la vie privée des consommateurs dans une perspective d'autorégulation de l'industrie. TRUSTe se présente aussi comme la seule organisation qui fournit une surveillance reconnue et complète ainsi qu'un mécanisme de résolution des litiges pour le consommateur afin d'assurer que les politiques établies en matière de vie privée sont effectivement en vigueur et que la vie privée de l'utilisateur en ligne est protégée. TRUSTe se démarque d'organisations telles que le NCSA, Verisign et le BBB qui s'occupent d'autres domaines importants concernant la confiance en ligne comme par exemple la sécurité, l'authentification et les « ethical business practices ».

TRUSTe ne se limite pas à délivrer des labels « vie privée » mais a un objectif beaucoup plus large. Il poursuit trois missions principales :

- Eduquer l'utilisateur sur les diverses options qui lui sont offertes par Internet pour protéger sa vie privée. Le site Web de TRUSTe a d'ailleurs été créé afin d'offrir les ressources, les outils et l'assistance nécessaire à cette fin (voir par exemple la page : http://www.truste.org/users/users_protect.html) ;

- Servir de point de liaison entre les consommateurs et les sites licenciés quand c'est nécessaire ;

- Encourager le milieu des affaires à afficher leur « déclaration vie privée » et à participer au programme de labellisation surveillé par une tierce partie.

TRUSTe dispose de nombreux sponsors tels que American Online, IBM, Microsoft, Netscape, etc (voir la liste à http://www.truste.org/about/about_sponsors.html).

Selon une enquête, 88 % (90 sur une autre page !) de l'ensemble des utilisateurs américains d'Internet visitent tous les mois un site Web licencié par TRUSTe. De plus, les sites licenciés par TRUSTe représentent 33 % de la totalité du trafic Internet américain.

1. LE LABEL TRUSTE ET SES INTERVENANTS

Un utilisateur d'Internet a le droit de s'attendre au respect de sa vie privée et à exercer le choix sur la manière dont le site Web va collecter, utiliser et partager ses données personnelles. TRUSTe a été créé en vue de répondre expressément à ce souhait.

Une pierre angulaire du programme est le TRUSTe « trustmark », un label affiché en ligne par les sites Web. Le « trustmark » est délivré uniquement aux sites qui adhèrent aux principes établis sur le respect de la vie privée et qui acceptent de se soumettre à une surveillance constante de TRUSTe et à la procédure de résolution des litiges avec les consommateurs.

Les principes et critères ont été élaborés par TRUSTe (mais reprennent en grande partie les pratiques d'information loyale approuvées par le département de commerce américain, la FTC et des associations représentatives de l'industrie). Pour le reste, il appartient à chaque responsable de site Web de faire une déclaration personnalisée en fonction de ses besoins, qui peut d'ailleurs offrir un plus haut niveau de protection.

Ces principes sont vérifiés par un représentant de TRUSTe. En cas de réclamation ou de litige, TRUSTe peut faire appel à une société d'audit (PriceWaterHouseCoopers ou KPMG).

L'utilisation du label TRUSTe n'implique pas l'intervention d'une autorité de certification.

2. - DOMAINES COUVERTS PAR LE LABEL

2.1. - Présentation

Tous les sites Web qui affichent le label doivent révéler leurs pratiques de collecte de données et de respect de la vie privée dans une déclaration franche, généralement avec un lien sur la page d'accueil. Plusieurs labels (et donc plusieurs déclarations) peuvent être affichés sur un même site si les pratiques varient à l'intérieur du site.

Les principes sur le respect de la vie privée reprennent les pratiques d'information loyale approuvées par le département de commerce américain, la FTC et des associations représentatives de l'industrie.

Ces principes incluent :

- l'adoption et l'implémentation d'une politique de respect de la vie privée qui prend en compte la crainte du consommateur à propos de la diffusion des données personnelles en ligne ;

- l'avertissement et la divulgation des pratiques de collecte et d'utilisation des données (pour identifier, contacter ou localiser une personne) ;

- le choix et le consentement, donnant à l'utilisateur l'opportunité d'exercer un contrôle sur ses données ;

- la sécurité et la qualité des données ainsi que des mesures d'accès : il faut protéger la sécurité et la véracité des données personnelles.

En sus des dispositions du programme standard, TRUSTe prévoit, le cas échéant, des exigences supplémentaires relatives à un label pour les enfants.

2.2.- Les critères retenus

a. Le programme standard

Les dispositions du programme standard de TRUSTe prévoient le respect de certains critères. Lorsque le label TRUSTe s'affiche, on est assuré que le site Web révèlera :

- quelles sont vos données personnelles qui sont rassemblées sur vous ;

- qui collecte ces données ;

- comment ces données seront utilisées ;

- avec qui l'information sera partagée ;

- vos choix possibles en ce qui concerne la manière dont les données sont collectées, utilisées et distribuées. Au minimum, il faut offrir la possibilité à l'utilisateur de refuser (option par défaut) la distribution à un tiers pour des utilisations autres ;

- la mise en place de garanties et de procédures de sécurité (protocole qui utilise l'encryptage) pour protéger les données contre la perte, l'utilisation abusive ou les altérations ;

- la manière par laquelle vous pouvez mettre à jour ou corriger les erreurs sur vos données.

b. Le programme supplémentaire pour les enfants

TRUSTe reconnaît qu'en ce qui concerne le respect de la vie privée, les enfants de moins de 13 ans ont des besoins spéciaux. Souvent, les jeunes enfants ne peuvent comprendre les implications lorsqu'ils donnent des données à caractère personnel. Dès lors, le site Web qui affiche le label pour les enfants s'engage à obtenir le consentement préalable des parents quand et si des données sont collectées ainsi qu'à avertir les parents de la manière dont ces dernières seront utilisées.

Les parents et les enfants qui visitent un site qui affiche le label pour les enfants savent également que TRUSTe effectue une surveillance régulière afin d'assurer que le site ne viole pas sa déclaration relative à la vie privée, et qu'une procédure de résolution des plaintes existe. Ainsi le consommateur peut réagir efficacement s'il constate que le site ne respecte pas le programme TRUSTe.

Si un site licencié par TRUSTe ne vise pas directement les enfants mais qu'il sait que l'âge de certains visiteurs est inférieur à 13 ans, il ne doit pas obligatoirement afficher le label pour les enfants. Cependant, il doit respecter les exigences liées à ce label quand il rassemble et utilise des données provenant de ces visiteurs.

Par contre, tous les sites qui visent directement des enfants dont l'âge est inférieur à 13 ans et qui souhaitent obtenir une licence de TRUSTe doivent non seulement adhérer aux dispositions du

programme standard de TRUSTe mais également aux exigences supplémentaires du label pour les enfants. En effet, si un site vise directement des enfants de moins de 13 ans ou dont il sait que l'âge du visiteur est inférieur à 13 ans, il **NE PEUT** :

- collecter des données « de contacts » en ligne de ces enfants sans l'accord préalable des parents ou un avertissement direct des parents de l'utilisation qui en sera faite, ce qui implique que les parents puissent empêcher l'utilisation des données et leur participation dans l'activité. Si l'accord préalable des parents n'est pas obtenu, les données « de contacts » en ligne seront seulement utilisées pour répondre directement à la demande de l'enfant mais ne pourront être utilisées pour re-contacter l'enfant pour d'autres buts ;

- collecter des données personnelles « de contacts » off-line sans l'accord préalable des parents ;

- distribuer ce type de données à des tiers sans l'accord préalable des parents ;

- donner la possibilité aux enfants de moins de 13 ans d'afficher publiquement ou de distribuer de toute autre manière des données personnelles « de contacts » sans l'accord préalable de parents, et tout faire pour interdire aux enfants d'afficher de telles données ;

- convaincre un enfant de moins de 13 ans, par le biais de jeux ou prix spéciaux ou d'autres activités, de divulguer plus d'informations que nécessaire pour participer à l'activité.

Si des données personnelles sont collectées, le site doit également afficher un avertissement à un endroit bien visible par lequel on demande à l'enfant de demander la permission à ses parents pour pouvoir répondre aux questions.

3. – LA PROCEDURE D'ATTRIBUTION DU LABEL

Lorsque le responsable d'un site contacte TRUSTe, on lui propose de désigner un coordinateur de site afin de vérifier que la déclaration relative à la vie privée est en conformité avec les pratiques d'information loyale, que le label y renvoie par un hyperlien et qu'il est correctement placé sur le site (en général, la déclaration principale se situe sur la page d'accueil). TRUSTe approuvera la déclaration (rédigée au départ par le responsable du site, une page permet à ce dernier de l'aider dans cette tâche : http://www.truste.org/wizard) et vérifiera qu'elle contient au moins les assertions présentées au point 2.2.

La page suivante indique comment faire partie du programme TRUSTe et obtenir le label : http://www.truste.org/webpublishers/pub_join.html

Avant d'obtenir le label, TRUSTe doit approuver la déclaration et recevoir l'accord de licence TRUSTe signé ainsi que le paiement du droit de licence annuel.

La démarche à suivre est la suivante :

- rédiger au préalable une déclaration (cela n'est pas obligatoire mais si on ne le fait pas, la procédure sera plus longue) ;
- lire et signer 2 copies de l'accord de licence TRUSTe ;
- payer les droits ;
- envoyer ces documents à TRUSTe ;
- un représentant TRUSTe prend contact, vérifie la déclaration et rédige un document d'auto évaluation ;
- si tout est en règle, le label est délivré.

Le coût du label attribué par TRUSTe est fonction du chiffre d'affaires annuel de la société :

-	299 $	pour un chiffre d'affaires annuel	inférieur à 1 million de dollars ;
-	399 $		entre 1 et 5 millions de dollars ;
-	499 $		entre 5 et 10 millions de dollars ;
-	1.499 $		entre 10 et 25 millions de dollars ;
-	2.499 $		entre 25 et 50 millions de dollars ;
-	3.499 $		entre 50 et 75 millions de dollars ;
-	4.999 $		supérieur à 75 millions de dollars.

4. - PROCESSUS DE GESTION DU LABEL ET SECURISATION DU LABEL

4.1.- La surveillance de TRUSTe et la procédure de résolution des plaintes

Tous les sites qui affichent le label TRUSTe marquent leur accord pour se soumettre à la surveillance de TRUSTe et à la procédure de résolution des plaintes. TRUSTe contrôle que les sites licenciés se conforment effectivement aux principes du programme et affichent leurs pratiques relatives à la vie privée au moyen d'une variété de mesures :

a. Contrôles initial et périodiques par TRUSTe : après avoir complété et signé un formulaire pour obtenir la licence, un représentant de TRUSTe vérifie la conformité du site aux principes du programme TRUSTe, à la déclaration et à l'utilisation du label. Ce même contrôle sera effectué périodiquement et notamment en cas de changement des pratiques. Ce contrôle s'effectue notamment par test ou sondage ;

b. Encourager les utilisateurs à vérifier qu'un site respecte sa politique de vie privée déclarée : préalablement, les sites acceptent de fournir aux utilisateurs des moyens simples et effectifs pour soumettre leurs réclamations directement au site Web. De plus, la déclaration relative à la vie privée doit au moins contenir les données pour pouvoir contacter TRUSTe. Si le site Web ne répond pas ou ne fournit pas une réponse satisfaisante, l'utilisateur peut contacter TRUSTe, qui jouera le rôle d'intermédiaire ;

c. Prise en compte des réactions et réclamations des utilisateurs : en effet, la vigilance de l'utilisateur est requise. En fait, on encourage ce dernier à contacter directement TRUSTe pour dénoncer une violation de la politique de vie privée affichée, un usage abusif du label ou tout autre problème lié à la vie privée. Une page a été créée sur le site pour effectuer ce type de réclamation, dénommée « Watchdog » (http://www.truste.org/users/users_watchdog.html). Cette page contient aussi un hyperlien qui permet d'accéder à la liste des sites licenciés par TRUSTe ;

d. Mise en place d'un label « click-to-verify » pour dissuader le piratage du label : tous les sites licenciés doivent afficher le label « click-to-verify » sur leur déclaration relative à la vie privée. Si on clique sur le label, on arrive sur le serveur sécurisé de TRUSTe et on vérifie ainsi que le site est effectivement licencié par TRUSTe ;

e. Le cas échéant, contrôle de conformité par une firme d'audit (PriceWaterHouseCoopers ou KPMG).

Afin de résoudre les réclamations des utilisateurs ou de TRUSTe, les sites licenciés acceptent de se soumettre à tout contrôle ou demande de renseignements de la part de TRUSTe. Si cela ne suffit pas pour atteindre une solution satisfaisante, une enquête plus poussée est menée. En fonction de la gravité de la violation, cette procédure peut mener à un contrôle de conformité du site par une firme d'audit (et éventuellement une modification de la déclaration), à une révocation du label, à la

cessation du programme TRUSTe, à une procédure de résolution du contrat, ou à un renvoi à l'autorité fédérale compétente (Attorney General's office, FTC ou Consumer Protection Agency).

4.2. - Authentification du label

Il existe plusieurs éléments pour vérifier l'authenticité du label TRUSTe.

Premièrement, un label TRUSTe est toujours lié à une déclaration vie privée. Si ce n'est pas le cas, le label est un faux. De plus, l'utilisateur peut vérifier l'authenticité du label en consultant la liste des sites licenciés par TRUSTe actuellement. Malheureusement, il n'y a pas de garantie à 100 pour cent que le label n'a pas été piraté ou n'a pas fait l'objet d'un usage abusif. Toutefois, des mesures ont été prise pour éviter cela, telles que par exemple le label « click-to-verify ». Lorsqu'on clique sur ce dernier, on arrive à la page du site qui affiche le label de TRUSTe, qui renvoie au site de TRUSTe. Sur ce dernier, on trouve une liste de l'ensemble des sites licenciés et une déclaration authentique que le site Web d'origine est effectivement un participant au programme (cette déclaration est faite en mode sécurisé).

2. Initiatives de labellisation en projet

Globalsign – Price Waterhouse Coopers : projet labellisation.

Contact : ***Samoera Jacobs***
GlobalSign NV
Kunstlaan 1-2, 1210 Brussels, Belgium
tel:02/209 05 93
samoera@belsign.be

Date de réunion : mardi 13 avril 1999.

Compte rendu de la réunion :

Globalsign n'a pas encore mis au point un projet opérationnel en matière de labellisation.

Elle est toutefois vivement intéressée par ce sujet et compte jouer un rôle dans ce nouveau marché. A cet égard, elle devrait relancer et concrétiser dans un avenir proche le projet initié en janvier 1998 en collaboration avec Coopers & Lybrand (devenu Price Waterhouse Coopers), projet qui n'a pas évolué depuis cette date.

Selon nos informations, Coopers & Lybrand avait développé en janvier 1998 une liste très complète de critères à vérifier et à respecter pour obtenir le label. Ces critères portaient notamment sur les prescrits légaux (vie privée, protection du consommateur, fiscalité, etc.) ainsi que sur des aspects de sécurité informatique. Cette liste n'est pas disponible.

Globalsign devrait rencontrer à nouveau PWC pour remettre le projet sur les rails et le concrétiser. Il semble qu'il existe manifestement une demande du marché pour ce genre de produit. Le rôle de PWC serait, d'une part, de déterminer la ***liste de critères*** à respecter au niveau belge (dans la perspective d'étendre cette liste à une échelle européenne en tenant compte par exemple des directives européennes) et, d'autre part, d'effectuer l'audit des sites Web afin de vérifier que les critères définis dans la liste sont scrupuleusement respectés. Cette étape débouchera sur un ***rapport d'audit***. Si l'audit est concluant, PWC donnera alors l'aval à Globalsign de certifier le label. Ce label serait signé par Globalsign et pourrait être apposé sur le site Web.

Parallèlement à la signature du label, Globalsign délivrera également un ***certificat***, afin que ce label puisse être vérifié par tout utilisateur. Un hyperlien permettra d'accéder au rapport d'audit. Ce certificat attestera que le site Web existe (contrôle d'identité), a effectivement été audité et a obtenu le label. Il aurait une validité de maximum 6 mois. Un contrôle devra donc être effectué tous les 6 mois. Si ce n'est pas le cas ou si le contrôle est négatif, le label sera retiré ou plus exactement le certificat sera révoqué et enregistré dans la liste de révocation (liste noire). En effet, il semble techniquement difficile pour Globalsign de retirer le label du site Web car il s'agit d'une image (gif, jpeg ou autre) dont elle n'a pas le contrôle (c'est la société qui gère le site Web qui a ce contrôle), mais si le certificat est révoqué, on constatera que le label ne vaut plus rien lors de la procédure de vérification du label.

Il est question de créer des ***labels modulaires*** (label minimum, label complet (au prix de 100.000 BEF), label vie privée, label protection du consommateur, label sécurité, etc.) afin d'une part,

de pouvoir répondre aux besoins précis des clients et, d'autre part, d'offrir des labels à moindre coût (les PME doivent pouvoir aussi obtenir un label).

En certifiant le label, Globalsign est conscient qu'en cas de problèmes les réclamations vont directement lui être adressées. Toutefois, elle n'entend pas prendre toute la ***responsabilité*** de la délivrance du label. Elle se limite à endosser la responsabilité liée à son activité (délivrance d'un faux certificat, non révocation d'un certificat, usurpation de sa clé privée, etc.). Pour ce qui est du non respect par le site Web des critères ayant fait l'objet de l'audit, cela relève de la responsabilité de l'auditeur (PWC).

La réflexion ne semble pas avoir été poussée plus au-delà. De nombreuses questions restent sans réponse :

- comment répartir les responsabilités ?
- qui peut demander la révocation du certificat associé au label, à quelles conditions, selon quelle procédure, dans quels délais, etc. ?
- comment assurer une sécurité effective du label contre une falsification ou une utilisation frauduleuse ?

Fedma - Federation of European Direct Marketing

Contact : ***Asucion Capparos***
Fedma
439 avenue de Tervueren
1150 Bruxelles
http://www.fedma.org
acaparros@fedma.org

Date de réunion : jeudi 15 avril 1999

Compte rendu de la réunion :

La Fedma fait part de deux expériences en matière de labellisation : l'une espagnole dont la mise en pratique a débuté fin 1998, et l'autre qui est un projet de labellisation à l'échelle européenne.

- ***Le label espagnol***

La fédération espagnole de marketing direct, membre de la Fedma, a créé un label '***privacy***' basé sur un code de conduite. Ce label est effectif depuis novembre 1998 (site : http://www.aece.org/corporativo/sello.htm). Son champ d'activité est limité d'une part à la protection de la vie privée et des données personnelles, et d'autre part aux sites espagnols.

Le ***code de conduite*** qui sert de fondement au label a été rédigé par l'association espagnole de marketing et, dans un souci d'indépendance, en collaboration avec trois associations de consommateurs espagnoles : une association des utilisateurs des moyens de communication, et deux associations membres du BEUC (Bureau Européen des Unions de Consommateurs).

Le label est attribué aux sites espagnols qui respectent le code de conduite en matière de protection de la vie privée. Un ***Comité de contrôle***, composé pour moitié de membres de la fédération de marketing et pour l'autre moitié de membres d'associations de consommateurs, effectue un contrôle aléatoire des sites qui possèdent le label et du respect de code de conduite. Un autre type de contrôle est effectué par un logiciel ad hoc, dit *logiciel spider*, dont la tâche est de rechercher sur le Web tous les sites sur lesquels le label est apposé. Cette recherche permet de vérifier si des sites ne se sont pas frauduleusement attribué le label, sans engagement préalable à respecter le code de conduite. Il semble que ce logiciel soit également capable d'effectuer un contrôle de l'application par le site de la politique décrite dans le code de conduite, et de déceler d'éventuelles infractions.

Les utilisateurs ont la possibilité de dénoncer des pratiques qui leur sembleraient illicites. Ces plaintes donnent également lieu à des contrôles.

- ***Le projet de label européen***

La Fedma a l'intention de créer un label au niveau européen, en reprenant le concept développé par la fédération espagnole, mais en étendant le champ d'application à toute l'Europe et à d'autres domaines que la protection des données personnelles. Le projet est encore à l'état d'ébauche, son contenu exact reste encore à définir. L'orientation actuelle se dirige vers un label à ***quatre composantes*** :

1. protection des données personnelles, avec une partie spéciale vis à vis des enfants,
2. communications commerciales, également avec une partie spécialement ciblée sur les mineurs,
3. identification du site (adresse physique, adresse de contact) : par référence à la Proposition de directive sur le commerce électronique,
4. vente à distance : dispositions de la directive contrats à distance.

Ces quatre composantes seraient, a priori, proposées en un seul 'package'. La Fedma envisage également d'offrir un logiciel de sécurisation des paiements effectués en ligne aux sites qui participent à la labellisation, ou à tout le moins de conseiller l'emploi d'un logiciel assurant une sécurité des paiements.

Le label serait développé suite à la rédaction d'un code de conduite prenant pour fondement les ***directives européennes***. Il est probable que la Fedma étende le concept à ses membres d'Europe centrale et orientale, notamment la Pologne, la République Tchèque, la République Slovaque et la Russie.

La Fedma est actuellement à la recherche de partenaires, à la fois au sein de ses propres membres, notamment techniques, mais aussi auprès d'associations de consommateurs aux niveaux européen et national. Une collaboration avec une autorité de certification est envisagée.

Elle se penche également sur la possibilité de proposer aux sites qui adhèrent à la labellisation un ***service à valeur ajoutée***, déjà développé dans le cadre de l'OCDE : le *Data Privacy Policy Generator*. Ce logiciel permettrait aux sites titulaires du label de s'engager plus en avant et de développer une politique de protection des données plus poussée.

Le contrôle de la bonne mise en œuvre du code de conduite serait effectué, d'une part, suite aux plaintes éventuelles des utilisateurs, et, d'autre part, par un contrôle régulier. L'idée d'un ***ADR*** en ligne est même envisagée, comme suite logique des engagements des sites à respecter le code de conduite.

Ready – initiative d'auto-labellisation

Contact : Dominique Morleghem
General Manager
Tel: 02/255 31 20
E-mail: d.morleghem@ready.be
http://www.ready.be

Réunion téléphonique : le mercredi 21 avril 1999

Compte rendu :

Le site de Ready propose une initiative ***d'auto-labellisation*** : sur base du *contrat de confiance* diffusé sur le site, Ready a demandé à une société de consultants de vérifier les engagements pris dans ce contrat de confiance.

Le contrat de confiance reprend les éléments suivants :

- Choix, qualité et service ;
- Satisfait ou non débité ;
- Protection de la vie privée ;
- Sécurité ;
- Garanties.

C'est cette dernière partie 'garanties' qui introduit l'auto-labellisation : « Ready fera vérifier deux fois par an par un organisme extérieur indépendant reconnu la bonne application des points du contrat concernant la *protection de la vie privée* et la *sécurité*. Les conclusions de ce rapport seront communiquées sur le site Ready.be ».

L'organisme extérieur indépendant auquel il est fait référence est la société Ernst & Young. Les consultants de Ernst & Young établiront un premier rapport sur le respect des engagement pris par Ready dans le contrat de confiance, avec d'éventuelles recommandations quant à des modifications à apporter. Suite à ce rapport et aux recommandations, les modifications nécessaires seront apportées par Ready. Ernst & Young contrôlera alors la bonne application des recommandations, et émettra un second rapport qui sera disponible sur le site de Ready.

La question de savoir si le logo de Ernst & Young figurera sur le site de Ready est encore à l'étude.

Ready envisage de recourir aux services d'un notaire pour garantir le sérieux de la procédure. A terme, l'audit sera probablement étendu à d'autres domaines comme les pratiques commerciales.

Institut des Réviseurs d'Entreprise (IRE) : projet de labellisation

Contact : André Kilesse
Société BDO
Rue Waucomont, 51
4651 BATTICE
andre_kilesse@bdo.be (à éviter, car problème avec le serveur de mails)
Tél . : 087/69.30.00
Fax. : 087/67.93.58

Réunions : divers entretiens téléphoniques

Compte-rendu des entretiens téléphoniques :

Au départ, l'IRE belge a développé une liste de « standards de travail » (+/- 60 pages) en matière de labellisation. L'IRE a essayé de convaincre ses collègues européens d'adopter cette liste mais sans succès. L'échelon européen préfère reprendre le label « WebTrust ». Dès lors, des négociations sont actuellement en cours avec WebTrust pour pouvoir utiliser leur label, tout en permettant aux membres de l'IRE d'utiliser un autre label (Truste ou autre) dans un souci de respect de la concurrence. Une réunion s'est tenue à Edimbourg le 26 avril sur cette question.

Au niveau belge, l'IRE élabore un projet de normes sur la labellisation des sites et vient de l'envoyer à ses membres (900 personnes) à la mi-avril. Ce projet est accompagné de quelques questions pour connaître l'avis des réviseurs sur la question (ex. : faveur pour un ou plusieurs labels, admet-on un rapport d'audit sans label, etc.).

Compte-rendu de la réunion du 30 avril 1999 :

L'Institut des Réviseurs d'Entreprise (IRE) s'intéresse à la labellisation depuis plus d'un an. Le rapport annuel de l'IRE de 1998 présente d'ailleurs la position officielle de l'Institut sur ce sujet[4]. Une ***Commission de Travail « labellisation des sites Web »*** a été crée au sein de l'IRE. Cette commission est présidée par André KILESSE et composée des membres suivants : Karel De BAERE, le principal responsable du commerce électronique chez PriceWaterhouseCoopers, H. CROSIERS d'Ernst & Young, L. CARIS d'un cabinet anversois, S. LELEUX, associé du président de l'IRE (J.F. CATS), et K. De BRABANDER, associé d'André Kilesse.

Le rôle de la commission de travail se divise en deux parties :

- d'une part, rédiger une ***norme*** énonçant les principes à suivre par les réviseurs pour labelliser un site Web (la manière dont le travail de contrôle doit s'effectuer et le contenu du rapport) : un projet[5] a été rédigé et envoyé récemment aux membres qui ont 3 mois pour réagir, envoyer

[4] Un extrait de ce rapport se trouve en annexe.

[5] Le *projet de norme* se trouve en annexe. Ce document est relativement **confidentiel** (nous avons toutefois obtenu l'autorisation de vous le transmettre). Le Conseil de l'IRE approuvera (ou non) le caractère définitif de ce rapport en septembre ou en octobre.

leurs commentaires et répondre aux 4 questions posées. Les réponses sont attendues pour fin juin ;

- d'autre part, négocier le ***contrat de licence WebTrust***. La décision d'opter pour le label WebTrust a en effet été prise il y a 6 mois environ.

L'idée de la *Commission* est de proposer aux réviseurs d'entreprise la norme comme standard minimum, en leur laissant le choix de proposer le label de WebTrust tout comme d'autres labels. On aurait donc un label WebTrust dont le contenu serait différent de celui utilisé au Canada ou aux Etats-Unis.

Le choix du label de WebTrust résulte de longues discussions au niveau européen. Dans un premier temps, l'idée dominante était de développer un programme de labellisation entièrement européen, différent du standard américain, en regroupant tous les instituts européens de réviseurs d'entreprise. La FEE, Fédération Européenne des Experts Comptables, a été contactée dans ce but, mais a préféré attendre qu'un produit fini lui soit proposé avant de contacter ses membres. Ce produit fini lui a été présenté quelques mois plus tard : un programme standard de travail de 50 pages[6] élaboré par les sociétés PriceWaterhouseCoopers et Ernst & Young.

ECWAT (European Consortium for Web Assurance and Trust) a été créé afin de donner un pendant européen à WebTrust, et d'essayer de bénéficier d'un financement de la Commission européenne. Trois pays se sont particulièrement engagés dans ce projet : la France, la Belgique et les Pays Bas, qui apparaissent comme leaders du consortium, à côté des autres pays européens et d'universitaires.

Un premier projet ECWAT a été présenté à la Commission européenne en vue d'un financement mais a été refusé. Or, dans le même temps, d'autres instituts de réviseurs négociaient avec les américains et canadiens, créateurs de WebTrust, notamment les anglais avec qui les négociations étaient très avancées. Devant cette position devenue dominante de préférer le modèle américain à un modèle européen, un nouveau projet ECWAT a été élaboré. Cet ECWAT II se concentre désormais sur l'analyse de l'impact de l'apposition d'un label sur un site Web quant à la confiance des utilisateurs.

Du côté des négociations avec WebTrust, deux points ont été formulés par les réviseurs belges et français : ils ne souhaitent s'engager dans ce label qu'à la double condition que les spécificités nationale et européenne soient décidées par l'Europe et non par les américains ; et qu'il soit possible de collaborer avec plusieurs autorités de certification (et non une seule comme c'est la position de WebTrust vis-à-vis de Verisign). C'est cette seconde condition qui retarderait la réponse des américains. L'IRE attend donc la position des américains avant de s'engager plus en avant.

De leur côté, les anglais ont signé avec WebTrust il y a 6 mois, tandis que les hollandais seraient sur le point de s'engager.

Pour le reste, l'IRE travaille toujours sur ECWAT II.

---

6 Document confidentiel non communiqué.

CRC – Centre Régional de la Consommation

Contact : Madame Magalie COSSU
Centre Régional de la Consommation
47 bis, rue B. Delespaul
59000 Lille
France
Tel (+33) 28 82 89 59
e-mail : mcossu@crc-conso.com
http://www.crc-conso.com/note/com/part4.html

Le contexte

Les principaux freins au développement du commerce électronique sont identifiés comme étant principalement le paiement en ligne, l'identification et le degré de confiance des sites Web visités par les internautes. Une plus grande transparence est apparue nécessaire, notamment en ce qui concerne l'authenticité des sites marchands.

A partir de ce constat, un groupe de travail interne au CRC-Consommation a mené une réflexion qui a abouti à un projet *d'identifiant qualitatif* qui permettrait au consommateur :

- d'une part, de mesurer la réalité économique de l'entreprise dont il visite le site ;
- d'autre part, de consulter ses droits et devoirs en terme de protection juridique, en fonction des textes régissant la vente à distance ;
- enfin, d'avoir la certitude que l'entreprise a rédigé une convention avec une structure consumériste, précisant qu'elle a parfaitement connaissance du droit applicable en matière de vente à distance.

L'identifiant qualitatif

L'idée d'un identifiant qualitatif, c'est-à-dire d'un logo pointant vers une page d'information, a ainsi été développée. Le principe est qu'un consommateur arrivant sur la page d'accueil d'un site Web marchand qu'il ne connaît pas, souhaite certainement obtenir toutes les informations nécessaires sur son identité, les caractéristiques de l'offre, des modes de paiement, des délais, etc. Pour avoir la certitude que ces informations sont réelles, il faut également que celles-ci soient « vérifiées » par un organisme indépendant.

Le rôle d'organisme indépendant pourrait être celui du CRC-Consommation : ce dernier hébergerait sur ses propres pages les informations inhérentes au site Web marchand. Pour atteindre les informations sur le site, le consommateur n'aurait qu'à cliquer sur un logo apposé sur la page d'accueil dudit site[7].

[7] Au-delà du logo, on peut également imaginer la réalisation d'une bannière animée, solution qui permet de délivrer un message clair, mais plus difficile à intégrer au sein d'une page Web originale. Le message suivant défilerait : « Si vous vous posez des questions sur l'achat via Internet, vérifiez l'engagement qualité de ce site sur le serveur du CRC-Consommation ».

L'information du consommateur

Chaque entreprise ainsi « partenaire » du CRC-Consommation aurait ainsi ses informations détaillées disponibles sur une page hébergée par le CRC, les consommateurs y arrivant en cliquant sur le logo précédemment présenté.

Les informations suivantes seraient présentées :

- Dénomination légale,
- Adresse du siège social,
- n° du Registre du Commerce et des Sociétés,
- Date de création,
- Statut Juridique,
- Capital social,
- Numéro de téléphone,
- Existence de surface(s) de vente physique(s),
- Nombre de magasins,
- Surface de vente moyenne par magasin (m^2),
- Surface de vente totale (m^2),
- Détail de l'activité Internet,
- Date de lancement de la vente en ligne,
- Nom et e-mail du responsable commercial,
- Types de produits proposés,
- Les prix pratiqués sont-ils les mêmes qu'en magasin ?
- Modes de paiement proposés,
- Technique de sécurisation des paiements,
- Mode de livraison des produits,
- Les produits sont-ils en stock ou commandés ?
- Délai moyen de livraison pour un produit en stock (valeur non contractuelle),
- Délai moyen de livraison si produit à commander (valeur non contractuelle),
- Nom et adresse de la banque de l'enseigne,
- Nom et adresse de l'assurance de l'enseigne.

La possibilité pour un consommateur d'avoir un accès simple et direct à toutes ces informations, plus la garantie de leur validité, est certainement un élément qui pourra le conforter dans sa démarche d'achat.

Rappel du droit applicable à la vente à distance

Au-delà de ces simples informations descriptives, le consommateur aurait également accès aux dispositions légales régissant la vente à distance. Par le biais de liens hypertextes, le consommateur aurait accès, d'une part, à une page d'informations juridiques « connaître ses droits en tant que consommateur sur Internet » ; et d'autre part, au texte de la convention régissant le partenariat entre le CRC-Consommation et le site marchand « lire le texte de la convention ».

La disponibilité en ligne de l'ensemble de ces textes est un nouvel élément permettant de conforter le consommateur dans son acte d'achat.

La démarche et ses limites

Les professionnels désirant participer à cette démarche s'engagent, via une convention passée avec le CRC-Consommation, d'une part à vérifier et mettre à jour de façon spontanée les informations diffusées aux consommateurs, et reconnaissent, d'autre part, être en parfaite connaissance du droit

applicable en matière de vente à distance. Il s'agit donc bien d'une véritable démarche préventive dans l'intérêt à la fois des consommateurs, mais aussi des professionnels, notamment des entreprises qui se lancent dans l'aventure sans « existence physique » préalable.

Toutefois, cette démarche a également ses limites, et ne doit en aucun cas être considérée comme un « Label » au sens strict du terme.

Seule la réalité économique de l'entreprise peut être appréciée, et non la qualité des prestations de vente, de livraison, de service après vente et des produits vendus. A ce titre, le CRC-Consommation ne peut pas être considéré comme responsable ni comme "médiateur" en cas de litige entre consommateur et distributeur. En cas de litige, il appartiendrait aux consommateurs de se rapprocher des associations de consommateurs et/ou d'un avocat. La mise en place d'un tel partenariat devrait cependant éviter la survenance de litiges qui, à coup sûr, ruinerait les efforts de crédibilisation mis en place par les distributeurs.

3. Annexes

Institut des Reviseurs d'Entreprises

Monsieur Didier GOBERT
FUNDP Namur
Faculté de Droit - CRID
Rempart de la Vierge 5
5000 NAMUR

le 19 avril 1999

Cher Monsieur,

Comme promis lors d'un entretien, je vous fais parvenir le projet de norme élaboré par la Commission Certification des sites internet de l'Institut des Reviseurs d'Entreprises. Ce projet de norme a été envoyé aux membres pour consultation. Ceux-ci disposent d'un peu plus d'un mois pour réagir.

Bien que ce document ne soit pas encore définitif, je vous transmets à titre confidentiel le document pour information. Dans la mesure où vous souhaitez réagir au contenu de ce projet de norme, je serais heureux d'en faire part aux autres membres de la commission.

Je vous souhaite bonne réception de ce document et vous prie d'accepter, Cher Monsieur, l'expression de mes sentiments les meilleurs.

André KILESSE
Président de la Commission "Certification des sites internet"

Institut des Reviseurs d'Entreprises

LE PRESIDENT

12 avril 1999

Cher Confrère,

Objet: Avant-projet de norme sur la déclaration de fiabilité relative aux opérations commerciales effectuées de façon électronique

Le document qui vous est soumis est un avant-projet de norme adopté par le Conseil de l'Institut en matière de déclaration de fiabilité relative aux opérations commerciales effectuées de façon électronique. Les travaux de la Commission «Certification des sites internet» découlent de travaux du dernier forum du revisorat qui s'est tenu à Genval et des travaux actuellement en cours au sein de l'*International Federation of Accountants* (IFAC).

Les commentaires relatifs à cet avant-projet sont attendus au plus tard le 15 juin 1999.

Cette proposition de norme de révision fait partie de ce que l'on appelle les «*assurance services*», en d'autres termes des missions devant aboutir sur un avis de professionnel non assimilable à une certification. Il s'agit de la première proposition de normes en matière informatique soumise par le Conseil pour commentaires. Différentes orientations stratégiques font l'objet plus particulièrement de la consultation des membres.

Le Conseil est conscient de la nécessité d'adopter rapidement une norme en matière d'opérations commerciales effectuées de façon électronique (Rapport annuel IRE 1998, p.133). En effet, un nombre sans cesse croissant d'entreprises utilise le réseau électronique dans le cadre de leurs activités. Certaines se limitent à la recherche d'informations, d'autres effectuent des opérations commerciales d'achat ou de vente de biens ou services par l'intermédiaire de ce réseau électronique.

./..

Ces activités commerciales ne peuvent connaître un essor que dans la mesure où les utilisateurs du réseau électronique ont confiance dans les personnes qui proposent des biens ou des services.

En dehors des opérations effectuées dans un réseau fermé, les personnes qui souhaitent effectuer des opérations commerciales au travers d'un réseau électronique ouvert auquel tout intervenant peut accéder (tel que le réseau internet) sans prendre de risques majeurs doivent exiger que le cocontractant s'engage à respecter certains principes fondamentaux assurant le bon déroulement de l'opération commerciale effectuée de façon électronique.

A l'étranger, certains auditeurs délivrent des sceaux donnant aux utilisateurs de réseaux électroniques ouverts l'assurance du respect effectif des engagements pris par les dirigeants des sociétés qui proposent des biens ou des services via ces réseaux. Ce nouveau type de mission devrait déboucher sur la délivrance d'une déclaration de fiabilité et de sécurité des opérations effectuées de façon électronique en cas de respect des engagements pris par les dirigeants de ces entreprises. L'Institut communiquera ultérieurement le programme de formation qui sera associé à cette nouvelle mission.

Les reviseurs d'entreprises ne peuvent rester indifférents à cette évolution parallèle à leur domaine traditionnel d'activités.

Je vous remercie pour les commentaires que vous ferez parvenir à l'Institut et vous prie d'agréer, Cher Confrère, l'expression de mes salutations confraternelles.

Jean-François CATS

Institut des Reviseurs d'Entreprises

AVANT-PROJET DE NORME

NORME SUR LA DECLARATION DE FIABILITE RELATIVE AUX OPERATIONS COMMERCIALES EFFECTUEES DE FAÇON ELECTRONIQUE

Questions posées par la Commission Certification des sites internet

Le Conseil souhaite recueillir l'avis des membres sur cet avant-projet.
Les commentaires doivent lui parvenir avant le 20 juin 1999.

- *Question 1 - Rapport obligatoirement (ou non) accompagné d'un sigle*

Dans son paragraphe 1.1.1. la norme impose une identification des sites présentant les garanties requises par l'apposition d'un sigle délivré par une autorité de certification sur instruction d'un reviseur d'entreprises. L'autorité de certification donne la garantie que le sigle est réel et infalsifiable.
Faut-il exiger qu'un sigle doive toujours être associé à une déclaration de fiabilité et de sécurité délivrée par un reviseur d'entreprises ou est-il concevable qu'une déclaration de fiabilité et de sécurité soit délivrée sans qu'un sigle n'apparaisse à l'écran?
Dans la mesure où la deuxième solution est acceptable, faut-il exiger une protection de la déclaration du reviseur par l'intermédiaire d'une autorité de certification donnant aux tiers l'assurance que la déclaration est réelle et n'a pas été falsifiée?

- *Question 2 - Sigle unique ou multitude de sigles?*

Pour pouvoir délivrer une déclaration de fiabilité et de sécurité, le paragraphe 1.1.2. de la norme impose le respect de conditions à différents niveaux:
- la sécurité des systèmes informatiques
- l'intégrité des opérations
- la transparence des pratiques commerciales et le respect des règles légales et fiscales y relatives.

Cela signifie qu'un seul type de sceau est affiché et ce dans la mesure où la norme dans son ensemble est rencontrée.
Faut-il envisager la création d'autres sceaux dont la portée se limiterait à une partie des principes généraux (par exemple affichage d'un sceau lié à la délivrance d'une déclaration de fiabilité relative à la sécurité des systèmes informatiques)?
Dans la mesure où un sceau «partiel» est considéré comme acceptable, quel est le critère à prendre en considération pour déterminer la pertinence de la portée d'un sceau?

- *Question 3 - Accréditation?*

Le paragraphe 1.4.1. de la norme rappelle le principe général selon lequel un reviseur d'entreprises ne peut accepter une mission que s'il dispose préalablement des capacités, des collaborations et du temps requis pour son bon accomplissement.
Ce principe général est-il suffisant ou faut-il prévoir un système d'accréditation étant donné la forte technicité et l'évolution rapide de la technologie sous-jacente aux opérations commerciales effectuées de façon électronique?
Dans la mesure où une accréditation est préconisée, doit-elle être délivrée à une personne physique ou peut-elle être délivrée à un cabinet de révision?

- *Question 4 - Extension de la portée de la norme?*

La portée de la norme (paragraphe 1.1.) est limitée aux opérations proposées par des entreprises à des consommateurs (appelées opérations «Business to consumers»).
Faut-il étendre le champ d'application de la norme aux opérations entre entreprises (appelées opérations de «Business to business»)?
Dans l'affirmative, faut-il postposer l'adoption de cette norme de manière à rédiger une norme commune ou est-il acceptable de publier ultérieurement un second document traitant des opérations «Business to business»?

AVANT-PROJET DE NORME

NORME SUR LA DECLARATION DE FIABILITE RELATIVE AUX OPERATIONS COMMERCIALES EFFECTUEES DE FACON ELECTRONIQUE

Schéma

Chapitre 1er : principes généraux

Chapitre 2 : principes d'exécution de la mission

Chapitre 3 : Rapports

❑

❑ ❑ ❑

CHAPITRE 1er : PRINCIPES GENERAUX

1.1. CHAMP D'APPLICATION DE LA NORME

Une démarche révisorale peut être mise en oeuvre dans le but de contribuer à la fiabilité et à la sécurité du commerce électronique. Par commerce électronique, on entend le recours à une infrastructure fondée sur un réseau électronique ouvert dans le but de conclure des opérations commerciales. L'objet de la présente norme est limité aux missions d'opinion relative aux opérations commerciales ou assimilées, à l'exclusion des services financiers, offertes aux consommateurs par le réseau Internet. Elle détermine les modalités des contrôles à mettre en oeuvre et la portée de la déclaration qui peut être délivrée à l'issue des contrôles.

1.1.1. L'identification des sites présentant les garanties requises peut être réalisée par l'apposition d'un sigle délivré sur instruction d'un reviseur d'entreprises pour une durée limitée et reconnaissable par tout utilisateur.

Le sigle doit être délivré par une autorité de certification dûment reconnue (conformément à la loi du .....) qui pourra garantir que le sigle est réel et infalsifiable. La gestion du sigle est effectuée par cette autorité de certification sur instruction du reviseur.

Le sigle est délivré lorsque les garanties qualitatives requises sont réunies. Le sigle doit donner accès aux *management assertions* (engagements pris par l'entreprise vis-

à-vis des consommateurs) et au rapport du reviseur établi selon les règles déterminées au chapitre III.

Les garanties qualitatives requises doivent répondre aux objectifs mentionnés au paragraphe 1.1.2. L'annexe 1 à la présente norme détermine les garanties minimales requises pour les opérations commerciales avec un consommateur réalisées par l'intermédiaire du réseau Internet.

La durée de validité d'un sigle ne peut en aucune manière dépasser 3 mois. Un mécanisme d'effacement en cas de non renouvellement express doit être prévu. La durée de validité peut être réduite par convention entre le reviseur et l'entreprise cliente.

1.1.2. Pour atteindre les objectifs de fiabilité et de sécurité nécessaires à la bonne exécution des pratiques commerciales, certaines conditions doivent être réunies en ce qui concerne notamment :

- la sécurité des systèmes informatiques;
- l'intégrité des opérations;
- la transparence des pratiques commerciales et le respect des règles légales et fiscales y relatives.

Par *sécurité des systèmes informatiques*, il y a lieu d'entendre pour les besoins de la présente norme l'ensemble des éléments du contrôle interne de la fonction informatique en ce qu'ils sont liés aux activités de commerce électronique. Sont notamment visés : l'environnement de contrôle, l'analyse des risques par les dirigeants, les contrôles du fonctionnement des opérations (en ce compris les contrôles d'accès, la protection contre les virus, les procédés de backup et recouvrement, etc.), la circulation appropriée de l'information et le contrôle de qualité.

Par *intégrité des opérations*, il faut entendre l'assurance que l'entreprise a mis en oeuvre des contrôles appropriés destinés à garantir un enregistrement des commandes, leur bonne exécution et leur facturation conformément aux conditions prévues pour le contrat. Les mêmes conditions seront réunies en ce qui concerne le paiement, notamment par carte bancaire et le service après-vente.

En ce qui concerne *la transparence des pratiques commerciales*, l'entreprise doit se conformer aux règles légales relatives aux pratiques du commerce et fournir l'assurance qu'elle a mis en place des contrôles efficaces dans le but d'éviter toute pratique contraire aux usages honnêtes en matière commerciale. Les règles légales concernées portent notamment sur les pratiques du commerce, la protection de la vie privée, les droits d'auteur, les droits de douane et la fiscalité indirecte (TVA), la signature électronique.

1.1.3. Par opération commerciale ou assimilée, on entend la conclusion d'un contrat de vente, de louage de chose, de prestation de service, de concession d'un droit d'exploitation ainsi que toute relation contractuelle similaire.

1.2. RESPONSABILITES DES PARTIES EN PRESENCE

Le reviseur d'entreprises ne peut délivrer une déclaration de fiabilité des pratiques commerciales que dans les cas où la direction a préalablement reconnu sa responsabilité sur les différents éléments faisant l'objet de l'examen de fiabilité. Le reviseur ne peut s'immiscer dans la gestion de l'entreprise ni modifier les conditions dans lesquelles s'exercent les pratiques commerciales.

1.2.1. L'organe d'administration de l'entreprise est responsable au plus haut niveau de l'organisation de l'entreprise et du bon déroulement de ses activités. En particulier, en matière de commerce électronique, ils doivent veiller :

- à la mise en oeuvre d'un contrôle interne adapté à la nature et à l'étendue des activités de commerce électronique, garantissant la sécurité des systèmes informatiques et l'intégrité des opérations;
- au respect des conditions légales et contractuelles dans la bonne exécution de toute opération commerciale à laquelle elle est partie.

1.2.2. Lorsque le reviseur d'entreprises est appelé à remettre une déclaration de fiabilité relative aux pratiques commerciales électroniques d'une entreprise, sa responsabilité ne peut dépasser l'objet de sa mission, à savoir donner une assurance raisonnable de la fiabilité des pratiques commerciales aux engagements souscrits par l'entreprise.

En aucune façon, l'intervention du reviseur d'entreprises ne peut avoir pour but de garantir la bonne fin d'une opération commerciale ni de garantir la qualité du produit livré ou du service presté. Le reviseur ne peut souscrire à un tel engagement, même contractuellement. Il doit exclure expressément cette responsabilité tant dans ses relations avec l'entreprise concernée qu'avec les clients de cette dernière. Une mention en ce sens figurera dans son rapport.

1.3. OBJET DE LA MISSION DU REVISEUR

L'objectif de la mission est de faire rapport sur la crédibilité de l'engagement souscrit par l'entreprise vis-à-vis de sa clientèle en évaluant l'information donnée par rapport aux critères fixés par la présente norme.

1.3.1. La mission du reviseur n'est pas une mission de révision d'une information financière au sens des normes générales de révision. Il s'agit d'une mission distincte par sa nature, par son objet et par la portée du rapport délivré.

La mission est différente *par sa nature* car il ne s'agit pas d'une mission d'attestation d'informations comptables. Elle porte d'une part sur l'existence de systèmes d'information et de traitement présentant les contrôles internes nécessaires pour satisfaire aux assertions prédéfinies auxquelles les dirigeants ont souscrit en matière de commerce électronique.

La mission est différente *par son objet* car les assertions de contrôle ne concernent pas une information comptable mais le respect notamment de certains principes légaux et contractuels et des usages honnêtes en matière commerciale.

La mission est différente *par la portée du rapport* délivré par le reviseur. Il ne comporte aucune attestation de la fiabilité d'une information mais il a pour but de donner une assurance raisonnable sur la fiabilité des systèmes d'information et de traitement en matière de commerce électronique.

1.3.2. La démarche du reviseur a pour objectif de confirmer que les engagements souscrits par l'entreprise vis-à-vis de sa clientèle (assertions qualitatives) ont été respectés en pratique. Ces assertions qualitatives sont déterminées à l'avance et rendues publiques vis-à-vis de l'utilisateur. Le reviseur ne peut délivrer un rapport sans réserve si les assertions minimales prévues par l'annexe 1 de la présente norme ne sont pas respectées.

Le reviseur mettra en oeuvre des procédures de contrôle destinées à identifier les écarts par rapport aux assertions qualitatives des dirigeants, que le reviseur juge assez importants, pris individuellement ou cumulés, pour avoir une influence sur la décision d'un consommateur, de traiter avec l'entreprise.

1.4. PRINCIPES DEONTOLOGIQUES

Dans l'exécution de cette mission, le reviseur d'entreprises doit respecter les principes déontologiques découlant notamment de l'arrêté royal du 10 janvier 1994 en ce compris son chapitre III relatif aux règles particulières relatives à l'indépendance dans l'exercice d'une mission révisorale.

1.4.1. Le reviseur d'entreprises et les autres personnes qui participent à la mission doivent avoir une compétence professionnelle appropriée à l'exécution de ce type de mission. Conformément à l'article 18ter de la loi du 22 juillet 1953 portant création de l'Institut des Reviseurs d'Entreprises, le reviseur ne peut accepter une telle mission que s'il dispose préalablement des capacités, des collaborations et du temps requis pour son bon accomplissement.

1.4.2. Par rapport à l'entreprise concernée, le reviseur d'entreprises doit justifier du respect des mêmes règles d'indépendance que celles requises pour l'exécution d'une mission de révision des états financiers.

1.4.3. Lorsqu'un autre reviseur d'entreprises exerce des fonctions de commissaire dans la société qui désire obtenir une déclaration de fiabilité relative à ses opérations commerciales sur Internet, les règles usuelles de confraternité, en ce compris la prise de contact écrite, sont d'application.

1.4.4. Avant d'entreprendre une mission conformément à la présente norme, le reviseur doit être raisonnablement fondé à croire qu'il pourra fournir une conclusion à l'issue de ses travaux. Avant d'accepter un nouveau client, le reviseur doit s'assurer que celui-ci fournit des éléments raisonnables relatifs à sa réputation et son intégrité. Si, de l'avis du reviseur, les pratiques commerciales suivies par l'entreprise n'offrent pas les garanties normalement requises, il préférera refuser l'exécution de la mission.

1.4.5. Le commissaire-reviseur ne peut communiquer librement avec le reviseur qui effectuerait une mission de contrôle de la fiabilité du commerce électronique. Le commissaire-reviseur demeure tenu au secret professionnel sauf si l'organe d'administration de l'entreprise consent par écrit à la communication entre les deux reviseurs. Il est recommandé de solliciter cet accord.

La lettre de mission relative à la mission de contrôle de la fiabilité du commerce électronique (ci-dessous, paragraphe 1.4.6.) comprendra en tout cas une autorisation du reviseur de communiquer ses constatations au commissaire-reviseur. Lorsque ces constatations sont importantes pour le contrôle des états financiers, le reviseur en fera part à son confrère qui exerce les fonctions de commissaire.

1.4.6. Dans toute mission visée à la présente norme, le reviseur d'entreprises devra veiller à la conclusion d'un contrat (lettre de mission) dans lequel les mentions suivantes seront nécessairement reprises :

- description et étendue de la mission;
- contacts qui auraient éventuellement été pris avec un confrère pour exécuter la même mission;
- responsabilité de l'organe d'administration sur les engagements pris vis-à-vis de la clientèle en matière d'intégrité des opérations, de sécurité des systèmes, de transparence des pratiques commerciales et de respect des règles légales et fiscales y relatives;
- responsabilité de l'organe d'administration de l'entreprise pour permettre au reviseur d'effectuer toutes les vérifications qu'il estime nécessaires;
- autorisation donnée au reviseur de faire, le cas échéant, appel à un expert;
- autorisation de communiquer avec le commissaire-reviseur;
- engagement du reviseur d'exécuter sa mission conformément à la présente norme;

- portée de la déclaration qu'il délivrera à l'issue de sa mission, à savoir une assurance raisonnable du respect des engagements souscrits par la direction vis-à-vis de sa clientèle;
- règles relatives à la durée de validité et aux droits d'attribution et de révocation du sigle;
- engagement de l'organe d'administration de l'entreprise de ne pas apporter des modifications majeures aux structures et au fonctionnement du site sans en informer le reviseur;
- engagement de renoncer à l'utilisation du sigle lorsque le reviseur a retiré le droit d'utilisation conformément au paragraphe 3.1.4. ci-dessous ou lorsque la durée contractuelle de validité est expirée sans avoir été renouvelée;
- modalités de calcul, de facturation et de paiement des honoraires;
- clause pénale pour utilisation abusive d'un sigle dont l'autorisation a été retirée.

Si la lettre de mission ne remplit pas les conditions mentionnées ci-avant, le reviseur déclinera la mission. Un exemple de contrat de mission est donné en annexe 2 à la présente norme.

❑❑❑

CHAPITRE 2 : PRINCIPES D'EXECUTION DE LA MISSION

2.1. IDENTIFICATION DE LA MISSION

Toute mission de contrôle de la fiabilité des opérations de commerce électronique suppose l'acquisition d'une connaissance suffisante de l'entreprise cliente, des systèmes électroniques utilisés ainsi que des assertions des dirigeants dont le reviseur doit vérifier la fiabilité.

2.1.1. Le reviseur doit acquérir une connaissance suffisante de l'entreprise. Il doit réunir des informations relatives aux personnes responsables de sa gestion, à sa forme juridique, au groupe dont il fait, le cas échéant, partie, à sa situation financière et à l'objet des activités.

L'objectif de la vérification de la situation financière est de déterminer dans quelle mesure l'entreprise pourra poursuivre ses opérations pendant la durée de validité du sigle.

2.1.2. Le reviseur doit analyser les systèmes informatiques et les systèmes de télécommunication utilisés par l'entreprise. Il doit obtenir une connaissance suffisante des matériels et des logiciels utilisés en relation avec le commerce électronique.

2.1.3. La déclaration de fiabilité porte sur un certain nombre d'engagements de l'entreprise (ou assertions qualitatives) vis-à-vis des consommateurs en ce qui concerne :

- la sécurité des systèmes informatiques;
- l'intégrité des opérations;
- la transparence des opérations commerciales et le respect des règles légales et fiscales y relatives.

Le reviseur doit identifier ces assertions qualitatives. Si certaines assertions essentielles ne font pas l'objet d'un engagement ou si certaines pratiques relatives à la gestion du website ne sont pas conformes aux règles légales et fiscales, le reviseur devra évoquer la question avec les dirigeants. Le cas échéant, il préférera ne pas poursuivre sa mission.

2.2. ORGANISATION ET DEROULEMENT DE LA MISSION

Le reviseur exécute sa mission conformément à un programme de travail approprié. Il veille à ce que le travail des autres personnes qui participent à sa mission soit convenablement effectué et supervisé. L'organisation de la mission tiendra compte des besoins spécifiques du client et du niveau d'assurance requis par la présente norme. L'annexe 5 définit les diligences normales de contrôle.

2.2.1. Le programme de travail comprend la description des travaux de contrôle à effectuer en vue de délivrer la déclaration de fiabilité relative au commerce électronique. Il comporte les étapes suivantes :

- évaluation des risques de l'organisation;
- l'évaluation des sécurités du système informatique;
- collecte d'éléments probants relatifs aux différentes assertions des dirigeants en matière d'intégrité des opérations, de protection de la vie privée et de transparence des pratiques commerciales;
- évaluation générale du résultat des travaux et établissement du rapport.

2.2.2. Dans l'organisation de ses travaux, le reviseur devra envisager en outre la nécessité de recourir aux travaux d'un expert (ci-dessous 2.5.).

2.3. EVALUATION DU RISQUE

Dès la phase préliminaire de sa mission et tout au long de celle-ci, le reviseur doit identifier les domaines qui présentent des risques généraux et spécifiques susceptibles d'orienter l'organisation de sa mission.

2.3.1. Le risque de révision comprend trois types de risques :

supprimer la mention sur le certificat digital et prendra les mesures nécessaires pour éviter toute confusion du public.

3.1.4. Lorsque l'entreprise a modifié ses engagements ou ses pratiques commerciales de façon significative sans en informer le reviseur, contrairement à l'engagement qu'elle avait pris, le reviseur peut mettre fin sans préavis au droit d'utiliser le sigle et demander à l'autorité de certification de retirer son rapport figurant sur le certificat digital de l'entreprise.

3.1.5. S'il est consulté par un confrère qui est invité par l'entreprise à effectuer une mission conforme à la présente norme, à propos des motifs pour lesquels il a mis fin aux relations avec l'entreprise cliente, il est autorisé à en donner le motif.

3.1.6. Si le reviseur est amené à retirer le droit d'utiliser le sigle, il doit s'assurer que l'entreprise ne prolonge pas abusivement l'usage du sigle. La vérification doit être opérée après un délai de grâce de 3 jours ouvrables et au plus tard, dans les 10 jours calendrier après le retrait du droit. Si l'usage se prolonge après le délai de grâce, une lettre recommandée doit être envoyée mettant en demeure de cesser l'usage illicite du sigle. Le reviseur examinera l'opportunité de faire appel à la clause pénale figurant au contrat. Il en informera l'Institut des Reviseurs d'Entreprises.

3.2. Contenu du rapport

Le rapport du reviseur (dont un exemple figure en annexe 4) doit comprendre un titre, le nom du destinataire, une description de l'objectif du rapport, une déclaration relative aux responsabilités, la référence aux engagements souscrits par les dirigeants ainsi que des normes de contrôle, l'adresse du site (URL) ayant fait l'objet d'une révision, une conclusion sur la fiabilité et la sécurité du système, la durée de validité du droit d'utiliser le sigle, la date du rapport et le lieu où il est émis ainsi que la signature manuelle ou digitale du reviseur.

3.2.1. Bien que le rapport concerne le respect des engagements souscrits par l'entreprise au cours d'une période passée, l'usage du sigle a pour but de donner confiance aux utilisateurs du site pendant une période postérieure à la délivrance du rapport. Le reviseur accepte ainsi une responsabilité implicite pour la durée d'utilisation du sigle.

Afin de ne pas engager sa responsabilité à la légère, le reviseur doit s'assurer que les modifications significatives du site seront portées à sa connaissance. Il prêtera attention aux changements susceptibles de remettre son rapport en cause.

3.2.2. La description de l'objet de la mission mentionnera les éléments figurant au paragraphe 1.1.2. de la présente norme.

3.2.3. Le rapport doit se référer aux engagements souscrits par l'entreprise vis-à-vis de sa clientèle. Ces engagements doivent être accessibles pour tout utilisateur ou contrepartie commerciale, sur le site électronique. Cette accessibilité doit être clairement identifiée, facilement exécutable et comprendre au moins les éléments mentionnés en annexe 1 à la présente norme.

3.2.4. Le rapport du reviseur mentionnera que les dirigeants de l'entreprise sont responsables des engagements rendus publics en matière de commerce électronique. La responsabilité du reviseur est d'exprimer une opinion sur le respect de ces engagements à l'issue de travaux de révision menés en conformité avec les normes de l'Institut des Reviseurs d'Entreprises relatives à la déclaration de fiabilité relative aux opérations commerciales effectuées de façon électronique.

3.2.5. Le rapport doit décrire la façon dont le reviseur a effectué ses contrôles. Cette description fera expressément référence aux présentes normes. Il doit préciser que les travaux de révision ont été planifiés et exécutés de façon à fournir une base raisonnable suffisante pour l'expression de l'opinion du reviseur.

Le rapport décrira les travaux de révision en précisant qu'ils consistent à :

- identifier les pratiques de commerce électronique de l'entreprise, les systèmes informatiques concernés et les contrôles mis en place pour s'assurer que les opérations sont traitées conformément aux engagements souscrits par la direction;

- vérifier par sondages que les opérations sont exécutées conformément aux engagements souscrits par la direction;

- vérifier et évaluer l'efficacité des contrôles mis en oeuvre par la direction en vue de garantir les engagements qu'elle a souscrits.

3.2.6. Le rapport doit mentionner avec précision l'adresse du site Internet (URL) ayant fait l'objet de la révision et contenir une conclusion consistant dans une déclaration de fiabilité établie conformément au paragraphe 3.3. ci-dessous.

3.3. CONCLUSION DU RAPPORT

Le rapport du reviseur doit contenir l'expression claire de sa conclusion relative à la fiabilité et à la sécurité du commerce électronique sur le site Internet. Dans cette conclusion, le reviseur doit préciser la période de l'examen du fonctionnement du site électronique et déclarer dans quelle mesure, au cours de cette période, l'entreprise s'est conformée aux assertions qualitatives définies

à garder de manière fidèle la trace de l'exécution de sa mission. Ces documents de travail doivent être conservés pendant cinq ans.

2.6.1. Les principes généraux développés dans la recommandation du 5 janvier 1987 relative aux documents de travail du reviseur d'entreprises sont d'application.

2.6.2. La conservation des dossiers sur un support électronique est jugée appropriée à condition que les mesures nécessaires aient été prises pour protéger ce support contre toute altération.

2.7. EVALUATION GENERALE DES RESULTATS DES TRAVAUX DE VERIFICATION ET CONTROLE DE QUALITE.

A l'issue de ses travaux, le reviseur doit contrôler la qualité des travaux effectués par les collaborateurs ou experts auxquels il aurait fait appel et effectuer une évaluation générale des travaux de vérification.

2.7.1. Le contrôle de la qualité des travaux de révision s'effectue en conformité avec la recommandation du 16 janvier 1998 relative au contrôle de la qualité des travaux de révision.

2.7.2. L'évaluation générale des travaux de vérification doit faire l'objet d'un mémorandum dans lequel le reviseur réunit toutes les informations pertinentes concernant les assertions des dirigeants relatives à :

- la sécurité des systèmes informatiques;
- l'intégrité des opérations;
- la transparence des opérations commerciales et le respect des règles légales et fiscales.

2.7.3. Cette évaluation générale sera complétée par une lettre de déclaration des dirigeants (dont un exemple figure en annexe 3) par laquelle ceux-ci confirment leur engagement sur les points suivants :

- reconnaissance par la direction du fait qu'elle est responsable du site électronique et de son contenu;
- reconnaissance par les dirigeants de leurs responsabilités de communiquer au reviseur tous les éléments significatifs qui pourraient avoir un effet sur l'étendue de sa mission;
- caractère complet des informations fournies au reviseur;
- confirmation de l'engagement des dirigeants de souscrire aux principes qui justifient la délivrance du sigle;

- existence d'instructions formelles adressées au personnel d'agir en conformité avec les principes développés dans les engagements souscrits par l'entreprise vis-à-vis de sa clientèle;
- obligation d'informer le reviseur en cas de modification majeure apportée aux structures ou au fonctionnement du site.

❑❑❑

CHAPITRE 3 : RAPPORTS

3.1. RELATIONS ENTRE LE SIGLE ET LE RAPPORT

Le sigle est une marque distinctive approuvée sur le website. L'authenticité du sigle peut être vérifiée moyennant la mention figurant sur le certificat digital du website. Ce certificat est délivré par une autorité de certification dûment reconnue sur instruction du reviseur.

L'opinion du reviseur s'exprime exclusivement par son rapport et aucune autorisation d'apposition d'un sigle ne peut être donnée si ce sigle ne donne pas accès, de façon automatisée, à une copie du rapport qui a autorisé son utilisation.

3.1.1. La durée de validité d'un rapport dépendra de la nature et de l'étendue des activités de l'entreprise qui pratique le commerce sur Internet. Cette durée sera fixée à 3 mois au plus à dater de la signature du rapport mais le reviseur pourra convenir avec l'entreprise de mises à jour plus fréquentes. L'émission plus rapprochée de rapports est recommandée dans l'hypothèse où l'entreprise procéderait à des modifications fréquentes de ses pratiques commerciales ou de ses systèmes informatiques. Il en va de même si l'activité de l'entreprise est dans une phase de développement.

3.1.2. Lorsque le reviseur n'a pas renouvelé sa déclaration de fiabilité à l'issue de la période de trois mois, soit que sa mission n'ait pas été renouvelée par le client, soit qu'il ait constaté des problèmes l'empêchant de renouveler sa déclaration, il devra en informer l'autorité de certification. Il demandera de supprimer la mention figurant sur le certificat digital et il demandera à son client d'enlever le sigle sur le website.

3.1.3. Même si le rapport a une durée théorique de trois mois, il est nécessaire de convenir avec l'organe d'administration de l'entreprise cliente que celle-ci s'engage à informer le reviseur entre deux rapports afin de lui communiquer les changements significatifs intervenus dans ses pratiques de commerce électronique (ci-dessus 1.4.6.). Si le reviseur estime que ces modifications doivent l'amener à modifier les conclusions de son dernier rapport, il doit le révoquer et demander à l'autorité de certification de

- les risques sur lesquels ni la direction ni le reviseur n'ont de prises (risques inhérents),
- les risques sur lesquels la direction peut avoir prise (risques de contrôle interne),
- le risque sur lequel le reviseur peut également avoir prise (risque de non détection).

Ces risques peuvent être approchés comme dans une mission de révision des états financiers. Le reviseur peut se reporter en cette matière à la recommandation du 3 décembre 1993 relative aux risques de révision.

2.4. PROCEDES DE VERIFICATION

Le reviseur décide de la nature et de l'étendue des travaux de contrôle à effectuer. Il a le choix des techniques à appliquer mais doit toujours être en mesure de motiver ses conclusions.

2.4.1. Les éléments probants peuvent être obtenus selon les techniques usuelles de la révision, comprenant notamment :

- l'examen approfondi des fichiers, documents et pièces justificatives;
- l'analyse des procédures;
- la confirmation d'informations auprès de tiers;
- la confirmation d'informations par la direction;
- la confirmation d'informations par le commissaire-reviseur;
- l'observation personnelle par le reviseur;
- les analyses et discussions avec les personnes intéressées.
- l'utilisation d'un logiciel d'audit.

2.4.2. Les éléments probants obtenus de tiers et les constatations personnelles du reviseur sont normalement plus fiables que les documents internes. Les documents internes seront d'autant plus fiables que le système de contrôle est de bonne qualité.

Les éléments probants de diverses origines ou de nature différente qui se corroborent offrent une plus grande certitude. Au contraire, s'ils se contredisent, ils feront l'objet d'un examen approfondi.

Le niveau de confirmation externe de ce type de mission sera normalement moindre que pour une mission de révision des états financiers.

2.4.3. La recherche des éléments probants portera au moins sur les éléments suivants :

- identification des pratiques de commerce électronique de l'entreprise et systèmes informatiques concernés;
- environnement de contrôle et autres éléments de contrôle interne;
- portée des contrôles mis en place pour assurer que les opérations conclues par la voie électronique sont traitées dans le respect des engagements légaux et contractuels;
- vérification des contrôles destinés à garantir que les pratiques commerciales de l'entreprise sont conformes aux usages honnêtes.

2.5. RECOURS AUX TRAVAUX D'UN EXPERT

Le reviseur doit s'assurer que toutes les personnes qui participent à la mission ont une expertise suffisante. Selon ce qui est prévu au paragraphe 2.2., il devra faire appel aux services d'un spécialiste possédant les compétences, les connaissances et l'expérience voulue dans un domaine autre que celui qui est propre aux reviseurs.

2.5.1. En ce qui concerne l'utilisation des travaux d'un expert, le reviseur peut se reporter aux principes généraux exprimés dans la recommandation du 6 septembre 1996 relative à l'utilisation des travaux d'un expert dans le cadre de la révision des comptes annuels.

2.5.2. Lorsque le reviseur estime qu'il devra recourir aux travaux d'un expert au cours de sa révision, il doit s'assurer de l'accord préalable des dirigeants en ce qui concerne l'objet de la mission de l'expert et la personne à laquelle il a l'intention de recourir.

2.5.3. Le reviseur qui fait appel à la collaboration d'un expert ne peut déléguer à ce dernier les éléments essentiels de la mission. Sous sa propre responsabilité, il doit se forger une opinion sur :

- la sécurité des systèmes informatiques;
- l'intégrité des opérations;
- la transparence des opérations commerciales et le respect des règles légales et fiscales.

2.6. DOCUMENTATION

Le reviseur d'entreprises est obligé de consigner ou de faire consigner par écrit les travaux de contrôle effectués en personne ou par ses collaborateurs de façon

par les dirigeants et couvrant au minimum les domaines décrits au paragraphe 1.1.1.

3.3.1. Un rapport de refus d'octroi devra être émis lorsque :

- le reviseur est d'avis que tout ou partie des engagements de l'entreprise en matière de commerce électronique ne sont pas conformes aux minima fixés en annexe 1 à la présente norme; ou

- l'entreprise ne s'est pas conformée d'une manière significative aux engagements qu'elle avait pris en matière de commerce électronique au cours de la période sous revue; ou

- le reviseur n'a pas été à même de rassembler des éléments probants suffisants pour évaluer dans quelle mesure l'entreprise s'est conformée aux engagements qu'elle avait souscrits dans l'exécution du commerce électronique; ou

- les systèmes informatiques de l'entreprise ne comprennent pas les garanties suffisantes en matière de contrôle interne pour garantir la sécurité et l'intégrité des opérations de commerce électronique; ou

- lorsque les dirigeants n'ont pas permis au reviseur d'effectuer toutes les vérifications nécessaires à l'expression de son opinion ou fixent des limitations inacceptables pour la mise en oeuvre des vérifications ultérieures aux dates que le reviseur jugerait appropriées.

  Doivent notamment être considérées comme une limitation dans l'exercice des travaux :

  - l'impossibilité de communiquer avec le fournisseur d'accès Internet de l'entreprise; et

  - l'impossibilité d'obtenir des informations que le reviseur jugerait nécessaires sur les systèmes informatiques de l'entreprise.

3.3.2. Lorsque le reviseur a délivré un rapport de refus d'octroi, il ne peut autoriser l'autorité de certification à greffer une quelconque déclaration de fiabilité quelconque sur le certificat digital du website tant que l'entreprise n'aura pas effectué les démarches nécessaires pour lui permettre de délivrer un rapport sans réserve.

3.3.3. S'il existe des faiblesses dans le contrôle interne, le reviseur pourra juger utile d'adresser à l'entreprise une lettre circonstanciée relatant ses constatations et recommandant éventuellement des améliorations nécessaires.

Annexe 1

Garanties minimales à offrir par toute entreprise aux consommateurs pour les opérations commerciales proposées dans le cadre du commerce électronique

Pour atteindre les objectifs de fiabilité et de sécurité nécessaires à la bonne exécution des pratiques en matière de commerce électronique, la direction de l'entreprise doit prendre des engagements vis-à-vis des consommateurs et effectuer les opérations conformément aux engagements pris.

Ces engagements relatifs aux pratiques en matière de commerce électronique (*management assertions*) sont décrits sur le site internet et couvrent au minimum les matières suivantes:

1. *la sécurité des systèmes informatiques*

   La direction de l'entreprise doit assurer qu'elle a mis en oeuvre un contrôle interne adapté à la nature et à l'étendue des activités de commerce électronique permettant d'assurer la sécurité des systèmes informatiques.

   La direction de l'entreprise veillera notamment à mettre en place une stratégie en matière de protection des données: contrôles d'accès (cryptographie, Fire Wall), protection contre les intrusions de tiers ou les virus, copies de sauvegarde et de récupération. En outre, un plan d'urgence doit permettre d'assurer les services en cas de panne.

2. *l'intégrité des opérations*

   La direction de l'entreprise doit décrire quelles sont les garanties offertes aux consommateurs en matière:
   - d'enregistrement des commandes, de leur bonne exécution et de leur facturation
   - de paiement, notamment par carte bancaire
   - de service après vente.

   La direction de l'entreprise mentionnera qu'elle a mis en oeuvre des contrôles appropriés destinés à garantir l'intégrité des opérations et le respect des engagements pris vis-à-vis des consommateurs.

3. *la transparence des pratiques commerciales et le respect des règles légales et fiscales y relatives*

   La direction de l'entreprise doit:
   - fournir l'assurance qu'elle a mis en place des contrôles efficaces dans le but d'éviter toute pratique contraire aux usages honnêtes en matière commerciale
   - assurer qu'elle se conforme aux règles légales applicables au commerce électronique (les pratiques du commerce, la protection de la vie privée, les droits d'auteur, les droits de douane et la fiscalité indirecte (TVA), la signature électronique).

Annexe 2

Exemple de lettre de mission

Lettre adressée au Président du conseil d'administration, au gérant ou au collège de gestion

Monsieur le Président,

Par la présente, j'ai l'honneur de vous confirmer que je suis disposé à effectuer la mission d'examen des conditions dans lesquelles s'effectuent les opérations commerciales proposées par votre entreprise au travers de son site internet (URL: (à compléter)).

Dans le cadre des opérations de commerce électronique proposées, votre entreprise a pris des engagements vis-à-vis de la clientèle en matière d'intégrité des opérations, de sécurité des systèmes, de transparence des pratiques commerciales et de respect des règles légales et fiscales y relatives. Le site internet au travers duquel vous proposez des opérations de commerce électronique reprendra ces engagements qualitatifs pris vis-à-vis des clients potentiels.

Cette mission vise à confirmer que les engagements souscrits par votre entreprise vis-à-vis de sa clientèle en matière de commerce électronique ont été respectés en pratique. Celle-ci ne débouchera cependant sur aucune garantie de bonne fin des opérations commerciales ou de la qualité des produits livrés ou des services prestés.

Il ne faut pas s'attendre à ce que cette mission permette de détecter les erreurs, irrégularités ou actes illégaux, y compris les fraudes ou les détournements de biens, qui pourraient exister. Toutefois, nous vous informerons de toutes les erreurs importantes et de toutes les irrégularités ou actes illégaux que nous pourrions découvrir, à moins qu'ils ne soient manifestement négligeables.

Nos contrôles seront effectués conformément aux normes de l'Institut des Reviseurs d'Entreprises. Ceci suppose que les responsables de votre société me communiquent les informations indispensables, me donnent les explications nécessaires et m'accordent toute possibilité d'effectuer les vérifications utiles pour le bon accomplissement de ma mission.

En outre, les dirigeants de votre entreprise m'informeront de tout changement qui pourrait être apporté aux structures et au fonctionnement du site Web, afin que je puisse déterminer si une mise à jour de mes procédés est nécessaire.

Le cas échéant, je ferai appel à un spécialiste en informatique pour effectuer les contrôles du système informatique: les honoraires dus à cet expert sont couverts par les honoraires fixés ci-après.

Au terme de cet examen, je vous demanderai de confirmer par l'intermédiaire d'une lettre de déclaration un certain nombre d'engagements, tels que:

- la reconnaissance par les dirigeants de votre entreprise du fait qu'ils sont responsables du site électronique et de son contenu;
- la reconnaissance par les dirigeants de leurs responsabilités de communiquer au reviseur tous les éléments significatifs qui pourraient avoir un effet sur l'étendue de sa mission;
- le caractère complet des informations fournies au reviseur;
- la confirmation de l'engagement des dirigeants de souscrire aux principes qui justifient la délivrance du sigle;
- l'existence d'instructions formelles adressées au personnel d'agir en conformité avec les principes développés dans les engagements souscrits par l'entreprise vis-à-vis de sa clientèle;
- l'obligation d'informer le reviseur en cas de modification majeure apportée aux structures ou au fonctionnement du site.

Conformément aux normes de l'Institut des Reviseurs d'Entreprises, la déclaration de fiabilité et de sécurité ne peut couvrir une période supérieure à trois mois. Comme convenu lors de notre entretien, dans la mesure où l'examen devait être concluant, la déclaration de fiabilité et de sécurité de votre site internet couvrira une période de xxx mois (à compléter).

Compte tenu de l'évolution constante du commerce électronique sur Internet, je me réserve le droit de déterminer le choix du moment ainsi que la durée du travail de vérification nécessaire pour la mise à jour et le maintien du sceau.

Selon notre convention, le résultat de l'examen relatif à la déclaration de fiabilité et de sécurité vous sera remis avant (date à compléter).

La déclaration de fiabilité et de sécurité délivrée doit être accessible à tout utilisateur de votre site internet qui souhaite effectuer des opérations commerciales.

Ce sigle est destiné uniquement à être utilisé par les dirigeants de la société xxxx pour le site Web ayant fait l'objet du service de certification (URL: (à compléter)). Le sigle ne peut être ni copié, ni reproduit ou distribué.

Dans la mesure où la déclaration de fiabilité et de sécurité n'est pas renouvelée ou est retirée avant le terme prévu initialement, vous ne pourrez plus faire usage du sigle à partir du jour où vous aurez reçu la notification du retrait du sigle par l'autorité de certification.

Par ailleurs, si votre site Web fait apparaître un sigle et une déclaration de fiabilité et de sécurité alors que celle-ci n'a pas été obtenue, n'a pas été renouvelée ou a été retirée, une procédure pénale sera entamée pour utilisation abusive du sigle.

Actuellement, la déclaration de fiabilité et de sécurité que je pourrais émettre est libellée comme suit:

(Insérer le rapport approprié)

Mes honoraires sont calculés selon le taux journalier en vigueur au sein de notre cabinet, en fonction du temps requis par l'exercice des contrôles et la rédaction de la déclaration de fiabilité et de sécurité. Selon nos conversations préliminaires, je puis évaluer le coût de mon

intervention à un montant de ... F. hors T.V.A. Dans la mesure où cette évaluation initiale devrait être dépassée de plus de ... %, je ne manquerais pas de vous consulter avant de poursuivre la mission. Une facture de provision d'honoraires représentant ... % de l'estimation précitée vous sera adressée si vous pouvez souscrire au contenu de la présente, le solde étant facturé au moment du dépôt du rapport.

Outre les honoraires mentionnés ci-dessus, vous me verserez une somme 1400 US$ pour la gestion du sceau WebTrust. Je suis tenu de reverser l'intégralité cette somme à l'Institut des reviseurs d'entreprises. Il va de soi que vous ne devrez verser ce montant de 1400 US$ que dans la mesure où cette mission devait se solder par l'émission d'un rapport sans réserve.

J'ai pris note du fait qu'aucun confrère reviseur d'entreprises n'exerce des fonctions de commissaire dans votre société, ni n'a été précédemment invité à effectuer la même mission de déclaration de fiabilité et de sécurité.
ou
Comme mentionné lors de notre entretien, vous m'autorisez à prendre contact avec mon confrère, M....., reviseur d'entreprises qui exerce des fonctions de commissaire dans votre société. De même, vous me permettez de prendre contact avec MM....., les confrères auxquels vous avez proposé d'effectuer la même mission de déclaration de fiabilité et de sécurité.

Je vous remercie vivement de m'avoir consulté pour la réalisation de cette mission et si vous marquez votre accord sur ce qui précède, vous seriez bien aimable de me retourner la copie ci-jointe de la lettre, signée pour accord. Par votre signature, la présente lettre sera considérée comme un ordre de mission.

date
X reviseur d'entreprises
représentant la société civile de reviseurs d'entreprises XYZ

Annexe 3

Exemple de lettre de déclaration des dirigeants

A l'attention du reviseur d'entreprises. Monsieur .....; date ....

La présente lettre vous est adressée dans le cadre de votre mission portant sur l'examen de la fiabilité des opérations commerciales effectuées de façon électronique. En exécution du contrat souscrit en date du ...

1. La gestion du site internet et les opérations commerciales effectuées dans le cadre de ce site électronique (URL: (à compléter)) relèvent de notre responsabilité. Nous vous confirmons, compte-tenu de notre meilleure connaissance :

   - que les engagements de notre société en matière de sécurité des systèmes informatiques, d'intégrité des opérations, de transparence des pratiques commerciales et de respect des règles légales et fiscales y relatives sont mis à la disposition des consommateurs sur le site internet;

   - que ces pratiques commerciales ont été appliquées de manière continue et qu'aucun changement significatif dans ces pratiques commerciales n'est intervenu sans qu'il n'ait été porté à votre connaissance;

   - qu'aucune infraction aux lois et règlements n'a été constatée qui puisse avoir un effet significatif sur les opérations commerciales effectuées de façon électronique par notre société;

   - que nous avons donné des instructions formelles aux membres du personnel de notre société d'agir en conformité avec les principes développés dans les engagements souscrits par l'entreprise vis-à-vis de sa clientèle;

   - que nous n'avons retenu aucune information importante qui, à notre connaissance, aurait pu influencer l'exécution de votre mission.

2. Nous vous confirmons que des vérifications ultérieures peuvent être effectuées pendant toute la durée au cours de laquelle le contrat prévoit le droit d'utiliser le sigle. Pendant toute cette période, nous nous engageons à vous communiquer les modifications importantes que nous serions amenés à apporter à nos systèmes informatiques ou à nos pratiques commerciales relatives aux opérations effectuées de façon électronique.

3. Nous vous confirmons l'engagement de l'entreprise de maintenir les principes généraux qui vous ont permis d'autoriser l'apposition du sigle de fiabilité, dans ses relations avec sa clientèle utilisant les procédés de commerce électronique. Nous renouvelons notre

acceptation de renoncer immédiatement à l'utilisation du sigle dans la mesure où vous seriez amené à constater des faits contredisant la portée du présent engagement.

L'administrateur-délégué ou le directeur général.

Annexe 4

Déclaration de fiabilité délivrée par le reviseur d'entreprises

Déclaration de fiabilité délivrée par le reviseur d'entreprises

Au Président du conseil d'administration de la Société ABC.

Nous avons vérifié les assertions qualitatives des dirigeants de la Société ABC relatives aux opérations de commerce électronique proposées sur son site Web (URL: à compléter), pour la période du XXX au XXX (à compléter).

Les dirigeants sont responsables des assertions qualitatives arrêtées [**lien hypertexte avec les assertions des dirigeants**]. Celles-ci couvrent la sécurité des systèmes informatiques, l'intégrité des opérations, la transparence des pratiques commerciales et le respect des règles légales et fiscales y relatives. Notre responsabilité consiste à exprimer une opinion sur les assertions qualitatives des dirigeants en nous fondant sur nos travaux de contrôle.

Nos travaux ont été effectués conformément aux normes belges relatives aux missions de déclaration de fiabilité et de sécurité des opérations commerciales effectuées de façon électronique, adoptées par l'Institut des Reviseurs d'Entreprises. Conformément à ces normes, les travaux ont été planifiés et exécutés de manière à obtenir un niveau d'assurance raisonnable pour fonder notre opinion. Nos travaux consistent à:

- identifier les pratiques de commerce électronique de l'entreprise, les systèmes informatiques concernés et les contrôles mis en place pour s'assurer que les opérations sont traitées conformément aux engagements souscrits par la direction;
- vérifier par sondages que les opérations sont exécutées conformément aux engagements souscrits par la direction;
- vérifier et évaluer l'efficacité des contrôles mis en oeuvre par la direction en vue de garantir les engagements qu'elle a souscrits.

Nous estimons que nos travaux donnent un fondement raisonnable à notre opinion.

À notre avis, pour la période du XXX au XXXX (à compléter), la direction de ABC s'est conformée, à tous les égards importants, aux assertions qualitatives auxquelles elle s'était engagée.

Compte tenu des limites intrinsèques des contrôles, il est possible que des erreurs ou des fraudes puissent se produire sans être détectées. En outre, toute extrapolation qui aurait pour effet d'étendre à des périodes futures les résultats d'une évaluation des contrôles présente un risque, puisqu'il est possible que les contrôles deviennent inadéquats en raison de nouvelles circonstances ou que l'efficacité de ces contrôles diminue.

Le sigle affiché sur le site Web de commerce électronique de ABC (URL: à compléter) est a priori valable jusqu'au XXXX (à compléter) et constitue une représentation symbolique du contenu du présent rapport. Il n'a pas pour objet, ni ne doit être interprété comme ayant pour objet, de mettre à jour ce rapport ou de fournir une quelconque assurance additionnelle.

Bruxelles, le ...
Société XYZ, représentée par M. X., Commissaire-reviseur

Quelques sources d'information complémentaires

1. Documents relatifs au commerce électronique actuellement en discussion.

- **Au niveau européen**

Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électronique, JOCE du 23 octobre 1998, C 325, COM(1998), 297 final, pp. 5-11.

Proposition de directive du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur, JOCE du 5 février 1999, C 30, COM(1998), 586 final, pp. 4-16.

- **Au niveau belge**

Projet de loi modifiant la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, Chambre des Représentants (SO 1998/99), 2050/1 & 2, mars 1999 (voir en particulier l'article 20).

2. Quelques sites internet intéressants à consulter:

- **E-commerce (généralités)**

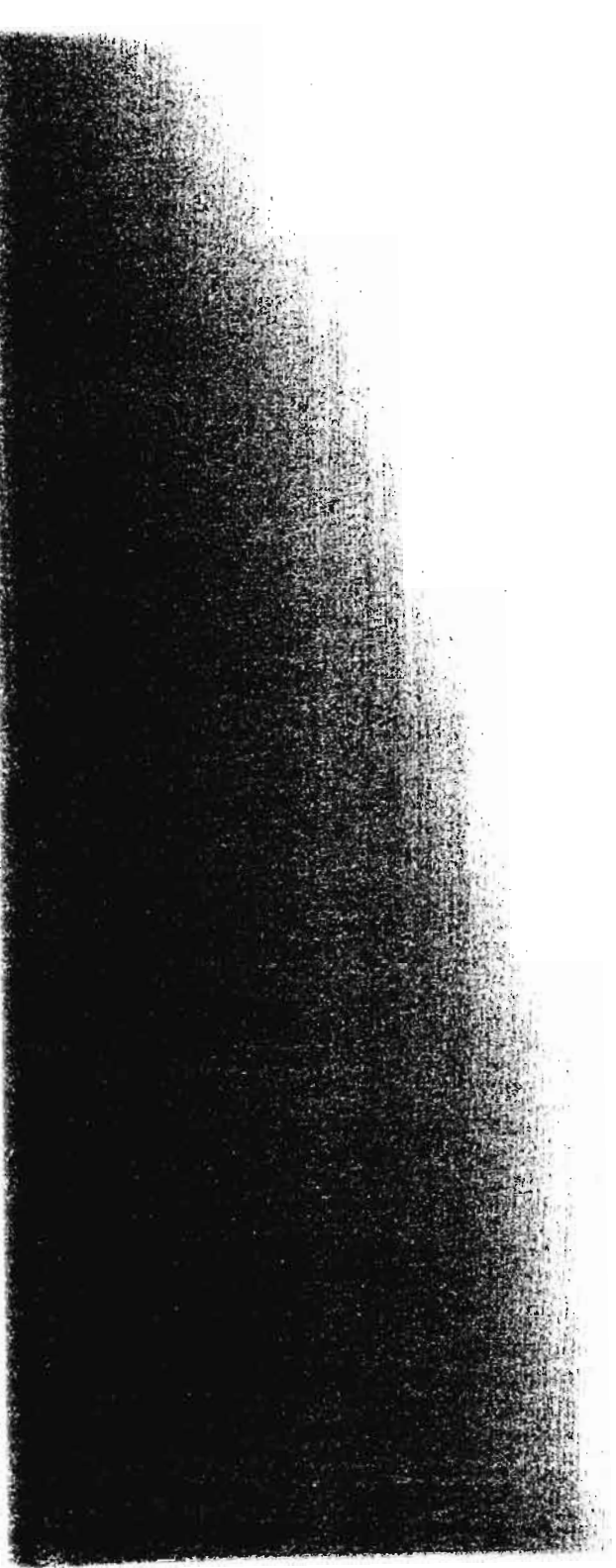
Union européenne:	www.ispo.cec.be/ecommerce/ www.europa.eu.int/comm/dg15/
OCDE:	www.ottawaocdeconference.org/
OMC:	www.wto.org/
E-Business:	www.ebusiness-europe.com/
CommerceNet:	www.commerce.net
France: (Voir notamment le rapport Lorentz)	www.finances.gouv.fr/commerce_electronique/
Etats-Unis:	www.ecommerce.gov
Actualité:	www.journaldunet.com

- **Sites universitaires (nombre important de liens utiles)**

CRID:	www.droit.fundp.ac.be/
ICRI:	www.law.kuleuven.ac.be/

- **Certification de sites**

CPA WebTrust:	www.cpawebtrust.org
Trust-e	www.etrust.org
Better business bureau:	www.bbbonline.org
VeriSign	www.verisign.com



INSTITUT DES REVISEURS D'ENTREPRISES
Créé par la loi du 22 juillet 1953

—

Avenue Marnix 22
1000 Bruxelles

Rapport annuel 1998

Conformément à l'article 12 de la loi du 22 juillet 1953, modifiée par les lois du 10 juillet 1956 et du 21 février 1985, le Conseil a l'honneur de vous faire rapport sur son activité au cours de l'année 1998.

11. AGREMENT DE CONSEILLERS D'ENTREPRISES

Le *Moniteur belge* du 4 février 1998 publie l'arrêté du 9 décembre 1997 du Gouvernement flamand relatif à l'octroi d'une aide financière aux petites entreprises faisant appel à des conseillers d'entreprises extérieurs agréés et à l'agrément de ces conseillers d'entreprises. L'objectif de cet arrêté est de subventionner les conseils dans les domaines suivants: faisabilité d'un plan d'entreprise, gestion financière et comptable, gestion commerciale, gestion industrielle, organisation, management et gestion du personnel, gestion de la télématique.

L'entreprise qui souhaite subsidier son activité choisit le conseiller d'entreprise extérieur qu'elle souhaite consulter sur une liste de conseillers d'entreprises agréés mise à sa disposition par le VIZO (Vlaams Instituut voor Zelfstandig Onderneming). Pour obtenir l'agrément de conseillers d'entreprises extérieurs, il faut être porteur d'un diplôme d'enseignement universitaire et avoir au moins trois années complètes d'expérience professionnelle en tant que conseiller de PME dans le domaine pour lequel l'agrément est demandé. Les reviseurs d'entreprises peuvent demander un agrément dans le domaine «Organisation générale d'entreprise, stratégie, faisabilité d'un plan d'entreprise» qui comprend les aspects suivants: faisabilité d'un plan d'entreprise, aspects de rentabilité, équilibre financier, coût, prix, contrôle budgétaire, gestion de la production, de la distribution, des débouchés, de l'organisation des ventes.

Il y a lieu de rappeler qu'un système similaire existe en Région wallonne par application de l'arrêté de l'Exécutif régional wallon du 9 juillet 1992 portant exécution de l'article 32.11 de la loi du 4 août 1978 de réorientation économique[1].

(1) Rapport annuel IRE 1992, p. 54.

12. LABELLISATION DES SITES WEB

Par commerce électronique, on entend l'ensemble des échanges sur un réseau électronique ouvert (Internet) dans le but de conclure des opérations commerciales. Le développement très rapide de l'Internet fait apparaître des perspectives exceptionnelles de croissance des activités commerciales électroniques mais suscite également des inquiétudes sur la sécurité des transactions et la protection des parties impliquées.

Si le commerce électronique n'est pas un phénomène nouveau, son développement est de plus en plus stimulé en Europe par le cadre du marché unique et, à partir de 1999, par la possibilité de conclure des opérations en euros.

Pour assurer un développement cohérent du commerce électronique, certaines conditions doivent être remplies. La confiance des intervenants et la sécurité des transactions requièrent dans une certaine mesure l'intervention du législateur, notamment dans le but de résoudre les problèmes de preuve, d'originalité de l'écrit ainsi que les éléments liés à la cryptographie. La profession de reviseur d'entreprises peut aussi jouer un rôle en qualité d'intermédiaire de confiance.

Les organismes de certification des sites Internet ont notamment pour mission l'authentification des parties à la transaction, la certification de la signature électronique et la certification des paiements, c'est-à-dire la garantie de la sécurité des systèmes de paiement. Ces organismes s'appuient sur d'autres professionnels dont le but est de répondre aux besoins des parties en présence en matière, par exemple, de protection du consommateur, protection de la vie privée, application régulière des lois commerciales et fiscales, etc. C'est dans ce domaine principalement que la profession peut intervenir, forte de sa compétence en matière de contrôle des systèmes d'information financière.

Dans les autres pays, notamment les Etats-Unis et le Canada, ayant déjà étudié la problématique, il est apparu nécessaire de différencier nettement les deux missions décrites ci-avant, à savoir d'une part la mission d'authentification des parties en cause, au travers par exemple d'une signature électronique, mission confiée à une autorité de certification et d'autre part, la mission dénommée «labellisation du site» qui consiste non pas en une certification, mais en une affirmation «d'assurance raisonnable».

L'approche distincte de ces deux missions a également été suivie par les Communautés européennes.(1)

Dès le début de l'année 1998, le Conseil de l'Institut a fait examiner dans quelle mesure les reviseurs d'entreprises peuvent contribuer au développement attendu de la «labellisation des sites Web». Constatant l'existence d'une expérience, principalement Outre-Atlantique, la Commission européenne est rapidement arrivée à la conclusion qu'une initiative s'imposait au niveau européen et qu'une prise de position au niveau national était indispensable en vue de confirmer l'intérêt de la profession pour cette activité.

Après avoir entendu un rapport intermédiaire de la Commission, le Conseil de l'Institut a décidé de mettre tout en œuvre pour élaborer dans le plus bref délai une norme et un programme détaillé de contrôle permettant aux reviseurs d'entreprises de se positionner sur le marché de la labellisation des sites. Ces travaux ont été menés tout au long de l'exercice et ont débouché sur des documents préparatoires qui seront soumis au Conseil dans les premières semaines de l'exercice prochain.

Toutefois, pour aboutir à l'objectif poursuivi, plusieurs conditions doivent être remplies et notamment le développement de contacts avec des organismes de certification disposés à accepter le label délivré par un membre de l'Institut et la reconnaissance internationale de ce label. Dans ce contexte, les initiatives purement nationales revêtent peu d'intérêt. En effet, l'Internet est un réseau mondial et la labellisation de sites n'a aucun sens si le marché auquel elle s'adresse est trop limité.

L'Institut a dès lors pris des initiatives dès le printemps 1998 pour susciter une concertation entre les Instituts professionnels européens au sein de la Fédération des Experts-comptables Européens. Ces réunions ont rapidement révélé qu'une préférence serait donnée à une discussion immédiate avec les Instituts américains et canadiens qui ont développé et appliquent depuis peu un programme de labellisation de sites Web sous le nom WebTrust. Parallèlement à sa première initiative, le Conseil a noué des contacts avec les représentants de WebTrust en vue de permettre aux membres de l'Institut qui le souhaitent de rendre des services basés sur la méthodologie développée Outre-Atlantique.

(1) Voyez par exemple la proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques (*J.O.C.E.*, 23 octobre 1998, C 325, pp. 4-11).

Ces discussions, dont les implications financières sont significatives, devront se poursuivre en 1999. Un socle commun de vérification s'impose quel que soit le lieu où le service de labellisation est donné tandis que des spécificités apparaissent au plan européen notamment en ce qui concerne le respect des directives relatives à la protection du consommateur, au respect de la vie privée et aux réglementations douanières et TVA.

Par ailleurs, le Conseil a également pris une part active dans la réflexion menée au sein du projet Agora 98 «Commerce électronique: vers le confiance!». Cet atelier convoqué par le Vice-Premier Ministre, Ministre de l'Economie, des Télécommunications et du Commerce extérieur avait pour but de créer un consensus visant à la compatibilité des infrastructures de clés publiques permettant la signature digitale mais le projet s'étend également à des aspects annexes tels que la reconnaissance des autorités de certification et la labellisation des sites. La présence des représentants de l'Institut au sein de l'atelier Agora 98 est donc indispensable pour faire valoir l'investissement en cours de réalisation au sein de l'Institut et assurer le droit des reviseurs d'entreprises de délivrer des labels de qualité. Il faut que des exigences minimales soient fixées pour pouvoir effectuer ce type de missions:

- offrir des garanties d'indépendance et d'impartialité;
- avoir des connaissances et des compétences suffisantes;
- être tenu à un code de déontologie reconnu;
- être astreint au secret professionnel;
- avoir souscrit une assurance qui couvre sa responsabilité professionnelle.

Les membres de l'Institut répondent à ces conditions ou du moins, pourront répondre à ces conditions dans la mesure où les programmes de formation permanente nécessaires leur permettront de justifier de la compétence exigée dans le contexte de ces missions.

Le Conseil est convaincu de l'importance des initiatives qui ont été prises en 1998. Il a tout mis en œuvre pour sensibiliser les Instituts membres de la FEE à l'urgence d'une initiative dans ces domaines technologiques nouveaux. Il espère que ces initiatives aboutiront très prochainement. Les reviseurs d'entreprises doivent développer d'urgence leur compétence dans les domaines technologiques tels que la labellisation de sites qui peuvent devenir un des domaines par excellence où la profession de reviseur d'entreprises peut se développer dans le XXI^e^ siècle.

VII. ETUDES ET PUBLICATIONS

1. COMMISSION D'ETUDES TECHNIQUES

1.1. Problématique de l'an 2000

Président: M. Luc Toelen
Membres: MM. P. Augusteijns, B. Dubois et D. Timmerman, assistés par M. H. Olivier
Représentants de l'IEC: Mme M. Claes et M. M. Verschelden

Comme exposé dans la première partie de ce rapport (p. 86 et suivantes), le passage à l'an 2000 sera source de nouveaux risques de contrôle. Il a dès lors semblé important aux membres du Conseil de mettre sur pied une commission traitant de la problématique de l'an 2000.

Les travaux effectués par cette commission s'intègrent dans le projet Forum Millésime 2000, mis sur pied par le Cabinet du Premier Ministre. Ce Forum Millésime 2000 a pour but de sensibiliser tous les acteurs, aussi bien publics que privés, à l'urgence d'un traitement rigoureux économique du problème.

Les membres de la Commission ont rédigé différents documents, rassemblés en décembre 1998 dans une brochure de la série Etudes IRE:

- une proposition de lettre à envoyer par les reviseurs d'entreprises aux dirigeants d'entreprise de manière à les sensibiliser au problème du changement de millénaire ainsi qu'un programme d'action à entreprendre par ces dirigeants;
- une note technique relative à l'implication du problème de l'an 2000 en matière de révision;
- une note technique relative à l'impact du problème de l'an 2000 sur les missions d'expertise comptable, en collaboration avec l'Institut des Experts-Comptables;
- un programme de contrôle des comptes annuels de l'exercice 1998.

Le Président de la Commission a également joué un rôle important dans les débats qui se sont déroulés au sein du Forum Millésime 2000, organisé par le Cabinet du Premier Ministre. A l'occasion de ces réunions, le confrère Toelen a pu mettre en évidence le rôle à jouer par les reviseurs d'entreprises, mais également les limites de la mission des reviseurs d'entreprises dans le cadre de leur mission de contrôle légal des comptes annuels.

1.2. Labellisation des sites web

Président: M. A. Kilesse
Membres: MM. L. Caris, H. Crosiers, K. De Baere, K. De Brabander et S. Leleux, assistés par Mme C. Dendauw et M. H. Olivier

Le Conseil de l'Institut a souhaité créer une commission «Labellisation des sites web», chargée d'élaborer une norme et un programme détaillé de contrôle permettant aux reviseurs d'entreprises de se positionner sur le marché de la labellisation des sites Internet.

Une description générale des travaux effectués par la Commission de l'Institut est donnée dans la première partie du présent rapport.

La norme élaborée par la Commission Website énoncera les principes généraux applicables aux différentes missions potentielles des reviseurs d'entreprises dans le cadre du commerce électronique. Seront annexés à cette norme, un exemple de lettre de mission, une lettre de déclaration des dirigeants et une déclaration de fiabilité à émettre par le reviseur d'entreprises au terme de sa mission.

Un programme de contrôle sera également mis à la disposition des membres de manière à assurer une cohérence au niveau des contrôles relatifs aux opérations de commerce électronique proposées par les entreprises et par conséquent une homogénéité des conditions d'apposition de labels.

La Commission a par ailleurs développé des contacts au niveau européen avec les autres organisations professionnelles d'auditeurs de manière à harmoniser les positions au niveau européen.

Les membres de la Commission ont aussi examiné les positions prises Outre-atlantique par l'AICPA et l'ICCA de manière à déterminer dans quelle mesure les options prises au niveau américain et canadien en matière de labellisation des sites Internet sont transposables au niveau européen. Une première rencontre avec les représentants de WebTrust s'est déroulée en décembre 1998. Cette prise de contact devrait déboucher sur des discussions dans le courant de l'année 1999 visant à adapter le contrat de licence WebTrust au contexte européen.

1.3. Audit et environnement

Président: M. L. Hellebaut
Membres: Mme R. Van Maele, MM. T. Buteneers, B. De Klerck, M.J. De Samblanx, V. De Wulf, M. Doumen, D. Kroes, L. Ruysen et L. Stammen, assistés par M. C. Hendrickx

Après avoir rédigé une note technique relative au contrôle de conformité au contrat signé avec Fost Plus, la Commission a élaboré une seconde note technique visant à permettre aux reviseurs d'entreprises d'effectuer un contrôle de la conformité des conventions conclues avec BEBAT.

La note technique relative à Fost Plus a par ailleurs fait l'objet d'une adaptation aux modifications dans les clauses du contrat. En même temps, l'Institut a mis à la disposition de ses membres les documents relatifs au contrôle sur la contribution au Point Vert au Grand-Duché du Luxembourg.

Actuellement, la Commission «Audit et environnement» prépare un projet de note technique concernant le contrôle des obligations de contribution dans le cadre du Val-I-Pac. Ces documents devraient être finalisés au début de l'année 1999. De cette manière, le contrôle en vue d'un premier rapport pourrait s'effectuer cette année encore, dans la mesure où cette recommandation serait applicable.

Les membres de la Commission font également partie d'un jury chargé de la sélection du lauréat du «Prix du meilleur rapport environnemental». Cette initiative, décrite dans la première partie du rapport annuel (p. 43), a une portée nationale mais également une portée européenne.

1.4. Evolution de la doctrine comptable

Membres: MM. P. Fivez et H. Van Passel, assistés par Mme C. Dendauw
Représentants de l'IEC: MM. G. Delvaux et J. Van Wemmel

Le Conseil de l'Institut estimait dans le courant de l'année 1998 qu'il serait utile qu'un groupe de réflexion se penche sur l'évolution attendue par la profession en matière de doctrine comptable.

Un groupe a dès lors été mis sur pied, en collaboration avec l'Institut des Experts-Comptables, de manière à développer quelques thèmes essentiels que les professionnels jugent prioritaires dans le développement de la doctrine comptable.

Il va de soi que les suggestions qui découleront de cette réflexion traduiront certaines difficultés rencontrées par les professionnels dans le cadre de leurs activités courantes mais également des sujets que la doctrine comptable belge n'a pas encore traité jusqu'à ce jour. Ce document a également pour objectif de montrer quels sont les changements nécessaires aux yeux des professionnels pour que les tiers obtiennent des états financiers pertinents.

Les travaux de ce groupe de réflexion devraient être publiés dans le courant de l'année 1999.

2ème Partie :

Recommandations en matière de labellisation

Auteurs : Didier GOBERT et Anne SALAÜN

Sous la direction du Professeur Yves POULLET

Plan

La labellisation a pour but de donner une meilleure visibilité à un site Web et aux pratiques que ce site applique dans les relations avec ses clients. Elle représente un argument commercial visant à faire mieux vendre les produits et les services du site. Surtout, la labellisation montre la volonté du site à montrer un engagement, vis-à-vis de ses clients, à respecter certains critères, et à prendre en compte leurs intérêts.

Un site qui développe une activité économique sur Internet peut donc trouver un intérêt à participer à une initiative de labellisation. Tel est le cas du WIN dont le site pourrait bénéficier de la technique de la labellisation afin de mieux se positionner par rapport à ses clients et de mieux vendre ses services.

Le but du développement qui suit est de déterminer de quelle façon le WIN peut s'engager dans une initiative de labellisation. Après un rappel des initiatives législatives en lien avec la labellisation (Partie 1), une classification des différentes formes de labellisation est proposée (Partie 2). Cette classification est ensuite appliquée au WIN (Partie 3). Enfin, des recommandations sont proposées en conclusion (Partie 4).

PARTIE 1 – INITIATIVES LÉGISLATIVES EN LIEN AVEC LA LABELLISATION

Le législateur belge, tout comme le législateur européen, s'est récemment engagé dans la promotion de la labellisation. De la même manière, plusieurs initiatives promouvant l'auto-réglementation sont à mentionner.

1.1. PROMOTION DE LA LABELLISATION

i) Le Projet de loi belge

Le projet de loi belge[1] visant à transposer la directive européenne relative aux contrats à distance[2] introduit la labellisation dans son article 80 : le paragraphe 3 interdit au vendeur *d'exiger* un acompte ou paiement quelconque du consommateur avant la fin du délai de renonciation de 7 jours. Or, cette interdiction « est levée lorsque le vendeur apporte la preuve qu'il respecte les règles fixées par le Roi en vue de permettre le remboursement des sommes versées par le consommateur ».

Le but de cette disposition est d'assouplir la règle pour les vendeurs qui présentent des garanties pour le remboursement des sommes par le consommateur. Les commentaires de l'article 80 parlent de « système de cautionnement, de blocage transitoire des sommes versées, d'assurance ou de labellisation – notamment des sites de commerce électronique ».

La labellisation des sites de commerce électronique est donc explicitement visée par le projet de loi comme l'une des techniques qui permet au vendeur de lever l'interdiction d'exiger un paiement avant l'expiration du délai de renonciation. Une fois la loi adoptée, un Arrêté Royal devrait définir les règles applicables et les critères à respecter.

Il est donc intéressant de voir, d'une part, que la labellisation est envisagée par le législateur comme une technique présentant des garanties certaines puisqu'elle permet de lever une interdiction légale ; et, d'autre part, que le gouvernement sera amené à s'engager davantage dans cette voie par le biais d'un Arrêté Royal.

ii) Le Projet de loi luxembourgeois

Le projet de loi luxembourgeois relatif au commerce électronique[3] introduit lui aussi la labellisation dans son titre III sur « les contrats conclus par voie électronique ». L'article 66 traite de la charge de la preuve relative à l'existence d'une information préalable, d'une confirmation écrite des informations, du respect des délais et du consentement du consommateur. Le paragraphe 2 précise que « la preuve des éléments énumérés au § 1 peut notamment être apportée par un mécanisme de certification de qualité du professionnel, dont les modalités seront fixées par règlement grand-ducal ».

Là aussi, la labellisation – ou certification de qualité – du vendeur vient assouplir les obligations qui sont imposées à ce dernier.

---

1 Document de la Chambre des Représentants, session ordinaire, 10 mars 1999, projets n°2050/1 et 2051/1– 98/99, disponible sur le site Web de la Chambre.

2 Directive 97/7/CE du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance, *JOCE* L 144 du 4 juin 1997.

3 Projet disponible à : http://www.droit.fundp.ac.be/textes/EcoLU.pdf

1.2. PROMOTION DE L'AUTO-REGLEMENTATION

La promotion de l'auto-réglementation participe également à la promotion de la labellisation : le développement de codes de conduite aux niveaux européen et national participe en effet au développement d'initiatives de labellisation dans la mesure où les codes de conduite peuvent servir de base aux critères que les sites s'engagent à respecter dans le cadre d'une labellisation.

i) La Proposition de Directive commerce électronique

La Proposition de directive du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur[4] encourage dans son article 16 l'adoption de codes de conduite par les Etats membres. Elle souligne l'importance des codes de conduite élaborés au niveau communautaire par des organisations ou associations professionnelles destinés à contribuer à la bonne application des articles 5 à 15 de la Proposition[5]. L'article 16 souligne également que les associations de consommateurs doivent être impliquées dans le processus d'élaboration et de mise en œuvre des codes pour les matières les concernant.

ii) Le code de conduite néerlandais

Les Pays Bas ont récemment publié la première version d'un code de conduite[6] relatif au commerce électronique. Cette initiative fait suite à une conférence organisée aux Pays Bas en juin 1998 sur le thème « The legal framework for electronic commerce: selfregulation? ».

Toutefois, ce code de conduite ne semble pas être, à l'heure actuelle, dans une version suffisamment complète pour pouvoir être utilisé comme référence.

iii) La directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[7]

Le Chapitre V de la directive, intitulé « Codes de Conduite », encourage « l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales prises par les Etats membres en application de la directive ».

---

4 Proposition du 18 novembre 1998, disponible à : http://www.ispo.cec.be/ecommerce/legal.htm

5 C'est-à-dire les articles relatifs aux informations à fournir, aux communications commerciales, aux contrats conclus par voie électronique, à la responsabilité des intermédiaires.

6 Voir les sites : http://www.ecp.nl ; ou : http://www.ediforum.nl

7 *JOCE L* du 23 novembre 1995 p. 281.

PARTIE 2 – LES DIFFÉRENTES FORMES DE LABELLISATION

2.1. CLASSIFICATION

Une initiative de labellisation peut prendre plusieurs formes. Principalement, on peut distinguer deux formes de labellisation que l'on peut définir comme suit :

- ***la labellisation interne:*** elle s'entend comme l'initiative de marquer ses propres services d'un niveau de qualité par un engagement à respecter certains critères, sans toutefois que le respect de ces critères fasse l'objet d'un contrôle a priori et périodique par un organisme tiers indépendant[8] ;

- ***la labellisation externe*** : elle s'entend comme l'initiative de faire contrôler a priori et périodiquement par un organisme tiers indépendant le respect effectif d'un ensemble de critères prédéfinis. Le résultat de ce contrôle peut s'exprimer par l'affichage du rapport effectué par un vérificateur indépendant et/ou d'un label.

Le critère déterminant pour distinguer la *labellisation interne* de la *labellisation externe* est l'intervention préalable[9] et périodique d'un organisme tiers indépendant dans le contrôle du respect des critères prédéfinis (que ceux-ci soient définis par le candidat à la labellisation, par le tiers qui effectue le contrôle ou par un autre tiers)[10].

Afin d'éviter toute confusion par la suite, il faut noter que l'intervention d'un tiers peut se situer à deux niveaux :

- soit pour la détermination des critères[11] (c'est-à-dire un contrôle de la qualité des critères),
- soit pour le contrôle du respect effectif par le site Web des critères prédéfinis (c'est-à-dire un contrôle de conformité aux critères).

Par contre, les éléments suivants ne sont pas déterminants pour distinguer ces deux types de labellisation :

- **l'origine de l'initiative :** qu'elle soit interne ou externe, la labellisation résulte généralement d'une initiative volontaire du candidat à la labellisation (celui qui entend marquer son engagement). Toutefois, il est vrai que dans certains cas, la labellisation (interne ou externe) pourrait apparaître comme forcée, soit contractuellement (par exemple, si le WIN n'accepte d'héberger des sites que s'ils s'engagent à respecter des critères prédéfinis[12]), soit réglementairement.

---

8 Cette labellisation « interne » correspond en quelque sorte à la notion d'auto-labellisation.

9 Préalable à l'affichage du label et/ou du rapport de vérificateur ou, à tout le moins, à la diffusion de l'information selon laquelle un tiers est intervenu pour effectuer la vérification.

10 Par exemple, relèveraient de la labellisation « interne » l'initiative AECE (même s'il se rapproche de la labellisation « externe » car le *Comité de Contrôle* AECE effectue un audit périodique et aléatoire) et l'initiative Ready actuelle. Par contre, relèveraient de la labellisation « externe » les initiatives WebTrust, TRUSTe et BBBOnLine (Ready ferait également partie de cette catégorie dans le futur si Ernst&Young effectuait un audit du site). Voir sur ce point le développement dans la Partie 2.

11 En pratique, les critères peuvent être soit directement rédigés par un tiers, soit un projet peut être rédigé par le WIN et être revu et avalisé par un tiers. Dans une certaine mesure, c'est ce qui se fait dans l'initiative TRUSTe.

12 Il n'empêche néanmoins que dans cette hypothèse, c'est le site lui-même et non le WIN qui s'engage à respecter les critères, le WIN ne s'engagerait qu'à l'exercice de certains moyens de contrôle.

- **la détermination des critères par un tiers :** le fait que les critères que l'on entend respecter soient déterminés par le candidat à la labellisation ou par un tiers n'apparaît pas comme un élément qui permettrait de distinguer la labellisation interne de la labellisation externe. Dans ces deux types de labellisation, les critères peuvent être prédéfinis par les responsables du site (sous la forme d'un contrat de confiance comme Ready, de conditions générales ou sous la forme d'une déclaration telles que dans BBBOnLine[13]) ou par un tiers (tel que c'est le cas pour les principes et critères WebTrust ou TRUSTe, le code de conduite AECE et dans une certaine mesure, dans l'initiative du CRC). De plus, même si les critères sont déterminés par un tiers, ceux-ci apparaissent souvent comme minimaux. Dès lors, rien n'empêche le site de prendre l'initiative de s'engager à plus[14]. Toutefois, l'intervention d'un ou plusieurs tiers (un centre de recherches universitaire, une ou plusieurs association(s) de consommateurs ou d'utilisateurs d'Internet, une société d'audit indépendante et compétente, etc.) pour la détermination des critères est de nature à renforcer la crédibilité de ces derniers;

- **le contrôle a priori de la détermination des critères par un tiers :** on peut répéter ce qui a été présenté dans le point précédent. En effet, que les critères soient directement rédigés par un tiers ou qu'un projet soit préparé par le candidat puis revu, corrigé et avalisé par un tiers ne change rien au problème (dans le cadre de TRUSTe par exemple, un responsable de TRUSTe peut demander que la déclaration initiale faite par le responsable du site soit modifiée) ;

- **l'affichage d'un label :** l'affichage d'un label (comme dans WebTrust, TRUSTe, BBBOnLine ou le logo CRC) n'est pas nécessairement obligatoire dans la labellisation externe[15]. L'important réside dans l'extériorisation (une preuve visible) de l'intervention d'un tiers quant au respect effectif des critères par le site : que cette extériorisation prenne la forme d'un label, de l'affichage du rapport du vérificateur ou une autre forme a peu d'importance. A l'inverse, un label peut être utilisé dans le cadre de la labellisation interne (le label AECE par exemple) pour renvoyer aux critères prédéfinis. L'affichage d'un label ne permet donc pas de distinguer les deux formes de labellisation, et risque d'ailleurs de créer une confusion entre les deux.

- **le renvoi à des critères prédéfinis :** le renvoi aux critères prédéfinis se retrouve dans les deux formes de labellisation. En effet, il est peu probable qu'un site s'engage à respecter des critères qu'il ne rend pas accessibles à l'utilisateur.

- **le renvoi à un rapport de vérification d'un tiers indépendant :** cet élément ne se retrouvera en principe que dans la labellisation externe. En effet, il s'agit de la concrétisation la plus visible de l'intervention d'un tiers pour la vérification de la conformité aux critères (le rapport du vérificateur WebTrust par exemple). Même si l'hypothèse est théorique, on peut imaginer qu'aucun renvoi ne soit fait à un éventuel rapport d'un vérificateur (cela semble être le cas pour les labels Privacy et Kid's Privacy de BBBOnLine)[16];

- **la sécurisation du label :** étant donné que l'affichage d'un label ne constitue pas un critère permettant de distinguer la labellisation interne de la labellisation externe, a fortiori le fait que ce

---

13 Notons d'ailleurs que pour le label Privacy de BBBOnLine, aucun critère précis n'est défini. Le site s'engage simplement par une déclaration « à dire ce qu'il fait et à faire ce qu'il dit ». C'est uniquement le respect effectif de cette déclaration qui est vérifié par BBBOnLine.

14 Notons d'ailleurs que pour WebTrust, les principes et critères apparaissent non seulement comme minimaux mais aussi uniquement comme une *base de référence* pour le vérificateur, qui dispose d'une certaine liberté dans l'appréciation de ceux-ci. On peut faire la même réflexion pour TRUSTe puisque il appartient à chaque responsable de site Web de faire une déclaration personnalisée en fonction de ses besoins, qui peut d'ailleurs offrir un plus haut niveau de protection que celui offert par les principes et critères TRUSTe.

15 Notons toutefois qu'en pratique, un label sera généralement utilisé dans la labellisation externe.

16 Pour ce qui est de TRUSTe, on renvoie uniquement à la déclaration initiale faite par le responsable du site, qui elle renvoie à une page de TRUSTe qui confirme que le site participe à son programme.

label soit sécurisé (juridiquement, par le dépôt d'une marque par exemple, et/ou techniquement, par un certificat comme WebTrust ou le renvoi à une page sécurisée ou un moteur de recherche comme pour TRUSTe) ou non ne constitue pas plus un critère de distinction.

La distinction entre labellisation interne et externe étant faite, il est possible d'envisager une gradation, c'est-à-dire des sous-catégories à l'intérieur de la labellisation interne et de la labellisation externe.

2.2. LA LABELLISATION INTERNE

Rappelons que la *labellisation interne* suppose l'absence de contrôle par un tiers du respect des critères. Au sein de cette catégorie, on peut envisager plusieurs niveaux.

- Niveau 1

Relève du niveau 1, la labellisation interne qui présente les caractéristiques suivantes :

- détermination des critères par le WIN sans intervention d'un tiers,
- affichage des critères sur le site du WIN.

A noter que le renvoi à ces critères peut se matérialiser par un label de type « WIN Trust ».

- Niveau 2

Relève du niveau 2, la labellisation interne qui présente les caractéristiques suivantes :

- détermination des critères par un tiers, ou par le WIN mais revus et avalisés par un tiers ;
- affichage des critères sur le site du WIN ou du tiers (avec un hyperlien sur le site du WIN).

A noter que le renvoi à ces critères peut impliquer l'affichage du label du tiers (en plus du label du WIN).

- Niveau 3

Relève du niveau 3, la labellisation interne qui présente les caractéristiques suivantes :

- détermination des critères par un tiers, ou par le WIN mais revus et avalisés par un tiers ;
- affichage des critères sur le site du WIN ;
- mise en place d'un mécanisme de réception des plaintes et de contrôle a posteriori du respect des critères par le site (sanctions possibles).

2.3. LA LABELLISATION EXTERNE

Rappelons que la *labellisation externe* suppose un ***contrôle a priori*** par un tiers du respect des critères. Suite à ce contrôle qui détermine l'octroi du label, des ***contrôles a posteriori*** ont lieu, soit de façon périodique, soit suite à une plainte d'un utilisateur.

Au sein de cette catégorie, on peut également envisager plusieurs niveaux.

- Niveau 4

Relève du niveau 4, la labellisation externe qui présente les caractéristiques suivantes :

- détermination des critères par le WIN sans intervention d'un tiers,

- intervention préalable et périodique[17] d'un tiers pour la vérification du contrôle de conformité (le tiers ne vérifie ni le contenu ni la qualité des critères),
- affichage des critères sur le site du WIN,
- affichage du rapport du tiers vérificateur,
- *option*[18] : possibilité de sécuriser l'identification et/ou l'intégrité de :
    - la page des critères,
    - la page du rapport,
    - le cas échéant, le label.

▪ Niveau 5

Relève du niveau 5, la labellisation externe qui présente les caractéristiques suivantes :

- détermination des critères par un tiers, ou par le WIN mais revus et avalisés par un tiers ;
- intervention préalable et périodique d'un tiers pour la vérification du contrôle de conformité ;
- affichage des critères sur le site du WIN,
- affichage du rapport du tiers vérificateur,
- *option* : possibilité de sécuriser l'identification et/ou l'intégrité de :
    - la page des critères,
    - la page du rapport,
    - le cas échéant, le label.

17 Cette intervention se fait soit d'initiative et régulièrement soit sur base d'une plainte.

18 Il convient de préciser que cette partie « sécurisation », qui est de nature technique, est en théorie susceptible de s'appliquer aux 5 niveaux. Toutefois, d'un point de vue pratique, elle sera essentiellement exploitée (pour des raisons de coûts, contraintes de mise en œuvre et complication du système) dans les niveaux 4 et 5. L'utilisation de cette option « sécurité » est de nature à renforcer la fiabilité du niveau en question, sans toutefois l'élever à un niveau supérieur. Ce n'est donc pas en soit un critère susceptible de distinguer un niveau d'un autre (c'est la raison pour laquelle il se trouve en italique dans le tableau qui suit).

Les différents niveaux de labellisation

		Détermination des critères		**Affichage des critères**	**Vérification de conformité par un tiers**			**Affichage du rapport du tiers vérificateur**	***Sécurisation***
		Par le WIN	Par un tiers (rédaction ou révision et aval)		Contrôle a priori	Contrôle a posteriori périodique	Contrôle a posteriori suite à une plainte		
Labellisation interne	Niveau 1	X		X					*Optionnelle mais théorique*
	Niveau 2		X	X					*Optionnelle mais théorique*
	Niveau 3		X	X			X		*Optionnelle mais théorique*
Labellisation externe	Niveau 4	X		X	X	X	(X)	X	*Optionnelle*
	Niveau 5		X	X	X	X	(X)	X	*Optionnelle*

2.4. APPLICATION DES NIVEAUX DE LABELLISATION AUX INITIATIVES OPÉRATIONNELLES ET EN PROJET[19]

2.4.1. WebTrust

On se situe ici dans un ***niveau 5*** de labellisation :

- les critères sont dégagés par WebTrust (par l'ICCA et l'AICPA) : tout site qui souhaite recevoir le label WebTrust doit impérativement respecter la liste des critères ;
- tout site labellisé doit renvoyer aux critères WebTrust par un lien depuis son site ;
- un auditeur accrédité par WebTrust effectue un contrôle a priori du respect des critères par le site avant d'octroyer le label ;
- une fois le label obtenu, un auditeur accrédité par WebTrust effectue des contrôles périodiques de l'application des critères par le site labellisé ;
- le label WebTrust est sécurisé par un certificat géré par une autorité de certification (Verisign) qui permet d'authentifier le label – en limitant ainsi les risques d'utilisation frauduleuse – de mieux gérer l'expiration du label et de le révoquer si nécessaire.

2.4.2. BBB OnLine

On se situe ici dans un ***niveau 5*** de labellisation :

- les critères sont définis par BBB OnLine ;
- les sites labellisés font un renvoi aux critères de BBB OnLine ;
- des contrôles a priori et a posteriori sont effectués ;
- un mécanisme de plainte est mis à disposition des visiteurs à l'encontre des sites labellisés qui ne respecteraient pas les critères BBB OnLine ;
- les résultats du contrôle sont affichés sur le site labellisé.

2.4.3. AECE

On se situe ici dans un ***niveau 3*** de labellisation :

- le code de conduite est déterminé par un comité composé pour moitié de représentants de la fédération espagnole de marketing direct et pour moitié de représentants d'associations de consommateurs ;
- le label est affiché sur le site labellisé (sans que l'AECE ne procède à un contrôle a priori) ;
- un mécanisme de réception des plaintes est organisé à l'encontre des sites qui ne respecteraient pas le code de conduite.

Remarque : l'AECE précise qu'un contrôle aléatoire est effectué par le Comité de Contrôle. Etant donné qu'aucune indication suffisante n'est donnée quant à la périodicité de ce contrôle et à son

[19] Renvoi aux initiatives décrites dans l'état des lieux du 3 mai 1999.

caractère systématique, il est difficile de le considérer comme un contrôle préalable et périodique qui classerait l'initiative de l'AECE dans le niveau 5 de labellisation.

2.4.4. TRUSTe

On se situe ici dans un ***niveau 4*** de labellisation :

- TRUSTe définit un standard minimum de règles à respecter, mais ce qui est véritablement déterminant c'est la déclaration que fait chaque site sur sa propre politique de protection de la vie privée ;
- un renvoi est fait vers les standards TRUSTe et vers les critères propres au site ;
- TRUSTe réalise un contrôle a priori du respect des standards minimaux ;
- un mécanisme de réception et de traitement des plaintes est mis en place ;
- TRUSTe effectue des contrôles réguliers de conformité avec les standards.

2.4.5. Ready

- ***Ready actuel : niveau 1 de labellisation***

- les critères (le « contrat de confiance ») sont déterminés par Ready sans qu'un tiers n'intervienne ni dans le choix des critères, ni dans l'aval de ces critères ;
- le contrat de confiance est disponible sur le site de Ready ;
- aucun tiers n'intervient dans le contrôle a posteriori du respect de ce contrat de confiance.

- ***Ready futur : niveau 4 de labellisation***

A l'avenir, le contrat de confiance sera révisé par un tiers et le rapport de ce tiers sera disponible sur le site de Ready. On sera alors en présence d'une labellisation de niveau 4, c'est-à-dire :

- détermination des critères par Ready sans intervention d'un tiers[20] ;
- affichage des critères sur le site de Ready ;
- contrôle périodique du respect des critères par un tiers ;
- affichage du rapport du tiers sur le site Ready.

[20] Remarque : si le tiers intervient également dans la détermination des critères, on passera alors dans un niveau 5 de labellisation.

PARTIE 3 – APPLICATION AU WIN DES NIVEAUX DE LABELLISATION

La distinction entre la labellisation interne et externe ainsi que la détermination des différents niveaux ayant été opérés, il convient désormais de mettre en œuvre ces niveaux au cas particulier du WIN.

Cette mise en œuvre peut s'opérer dans deux hypothèses distinctes. En effet, il apparaît que le sujet de la labellisation n'est pas unique. Dans le cadre du WIN, on peut envisager :

- la labellisation du WIN (ou plus exactement de ses services), et

- la labellisation des clients du WIN.

3.1. LABELLISATION DES SERVICES DU WIN

L'idée est de labelliser les services offerts par le WIN. Ces services sont les suivants :

- les accès individuels à l'Intranet et/ou l'Internet ;
- l'hébergement de sites Internet : hosting ;
- l'hébergement du serveur du client : housing ;
- le support aux transactions en ligne ;
- l'e-business.

Accessoirement, les services tels que l'interconnexion de réseaux et la visioconférence peuvent être inclus dans le processus de labellisation des services du WIN.

La question se pose de savoir si le WIN doit labelliser la totalité de ses services – dont la publicité est d'ailleurs faite sur son site Web – ou s'il doit se limiter à labelliser les services offerts et conclus par le Web (tel que l'accès à l'Intranet et/ou l'Internet par exemple) ?

Les deux solutions sont possibles et le choix entre l'une et l'autre revient au WIN.

Notons toutefois que si l'état des lieux présenté dans le rapport intermédiaire démontre que la labellisation virtuelle s'applique essentiellement aux services virtuels (c'est-à-dire au moins conclus via le Web), rien n'interdit que cette labellisation virtuelle s'applique également aux produits ou services offerts, conclus, livrés ou prestés dans l'environnement physique (et dont le site Web se limite à en faire de la publicité)[21]. Cela présente certains avantages par rapport au label « papier » (les deux labels n'étant d'ailleurs pas incompatibles) en termes de visibilité[22], de transparence[23], d'accessibilité[24] et de vérifiabilité[25].

---

21 En d'autres mots, on vend ou on preste physiquement mais on labellise virtuellement.

22 Les techniques informatiques offrent plus de souplesse et de possibilités que le papier.

23 On peut facilement connaître la signification d'un label virtuel en cliquant dessus, ce qui n'est pas possible pour le label papier qui exige une bonne information du public sur le label et sa signification et une bonne mémoire !

24 La technique des hyperliens ainsi que les moteurs de recherches permettent de trouver rapidement les différents labels ainsi que les sites labellisés.

25 Les techniques de sécurité informatique permettent de vérifier presque instantanément l'authenticité d'un label.

Les services du WIN peuvent être labellisés suivant les niveaux présentés précédemment.

3.1.1. La labellisation interne

Rappelons que la labellisation interne suppose l'absence d'intervention d'un tiers quant à la vérification du respect des critères par le site.

- **Niveau 1**

Dans le niveau 1, le WIN marque ses services d'un niveau de qualité en déclarant qu'il s'engage à respecter certains critères. Cela prendra la forme d'une déclaration faite sur son site, comme le fait le site ready.be actuellement.

Dans ce 1er niveau, le WIN se charge de rédiger lui-même les critères[26] qu'il entend respecter, en les adaptant aux services qu'il propose à ses clients.

Limitons nous à dire que cette liste[27] devrait prendre en compte le respect de certaines législations (telles que la loi sur les pratiques du commerce et sur l'information et la protection du consommateur – dite LPC – du 14 juillet 1991[28] ; la loi relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données du 11 décembre 1998[29]) ; soit d'une manière vague (« Nous appliquons la LPC et la loi sur la vie privée », « Nous protégeons vos données personnelles », « Nous protégeons le consommateur », etc.) soit d'une manière plus précise (en énumérant l'ensemble des droits des consommateurs consacrés par ces législations).

Notons cependant que ces critères doivent rester *visibles* (mis en évidence sur le site), *accessibles* facilement et rapidement, *compréhensibles* (l'internaute moyen n'est pas un juriste !) et *convaincants*. Pour le reste, le WIN peut s'engager à respecter des obligations supplémentaires, non imposées par la loi, qui offrent un plus à la qualité du produit ou du service (du type par exemple, « satisfait ou remboursé »).

Le WIN localiserait cette liste de critères sur son site. Le renvoi à ces critères peut se faire de manières diverses :

- soit ils sont clairement affichés sur la page d'accueil (ce qui est difficile d'un point de vue pratique car la liste peut être longue) ou sur une autre page du site ;

- soit on renvoie à une page consacrée à cette liste via un hyperlien qui lui, idéalement, doit se trouver sur la page d'accueil (on montre ainsi l'importance accordée à cette liste et à son respect).

---

26 Nous ne pouvons nous permettre de proposer une liste idéale de critères car cela représente une charge de travail considérable et nécessite un analyse très poussée, ce qui dépasse largement le cadre de cette convention (cette remarque vaut également pour les niveaux 2 à 5). Toutefois, il est indéniable qu'une telle liste présente un intérêt non négligeable.

27 Des standards minimums devraient en toute hypothèse être mentionnés dans la liste des critères, notamment :
- la protection de la vie privée et des données personnelles ;
- la bonne information des clients sur les services proposés ;
- la qualité des services proposés ;
- l'adoption de mesures techniques de sécurité adéquates ;
- le respect des réglementations en vigueur ;
- des services après-vente de qualité ;
- etc.

28 *M.B.* du 29 août 1991.

29 *M.B.* du 3 février 1999 p. 3049.

Cet hyperlien peut prendre la forme d'un label (image) et/ou d'une phrase (« Notre contrat de confiance », « Nos engagements », « Nous respectons les droits des consommateurs », etc.).

L'adoption du niveau 1 par le WIN présente les *avantages* et *inconvénients* suivants :

Avantages :

- une grande flexibilité pour le WIN : il est libre dans le choix des critères qu'il adopte, il peut faire évoluer ces critères à tout moment, etc. ;

- une facilité de mise en œuvre ;

- une solution peu onéreuse : elle nécessite uniquement la mobilisation de quelques ressources internes pour rédiger les critères et les afficher sur le site ainsi qu'un espace mémoire très faible sur le serveur ;

- nonobstant le 3ème inconvénient décrit ci-après, le fait de déclarer que l'on respecte telle ou telle législation est de nature à informer le consommateur qu'il dispose de certains droits ainsi que de possibilités de recours (pour autant que cette déclaration soit suffisamment précise. On peut imaginer un renvoi vers la loi visée, vers le site du Ministère des Affaires Economiques[30], vers le site du Ministère de la Justice, etc.). D'autre part, les engagements supplémentaires peuvent constituer un acte juridique unilatéral, dont le non respect peut être sanctionné.

Inconvénients :

- l'absence d'intervention d'un tiers – soit dans la rédaction en tant que telle des critères, soit dans l'entérinement a posteriori des critères – risque de limiter la portée de l'initiative et sa crédibilité ;

- la flexibilité pour le WIN risque de constituer un facteur d'instabilité aux yeux de l'internaute (surtout si le WIN modifie régulièrement ses engagements) et de poser des problèmes de preuve lorsqu'un internaute désire se prévaloir des engagements déclarés ;

- l'absence d'intervention préalable d'un tiers pour vérifier , non plus les critères, mais le respect effectif des critères par le site limite la crédibilité de l'initiative. En effet, en quoi le consommateur est-il plus protégé lorsque le WIN se limite à prétendre qu'il respecte la LPC qui, par définition, est impérative et à ce titre doit être respectée ?

En résumé, la labellisation de niveau 1 impliquerait pour le WIN :

→ définir lui-même une liste de critères ;

→ afficher les critères sur son site.

[30] Et notamment à un éventuel vade-mecum à destination des utilisateurs d'Internet qui pourrait être hébergé sur le site Web du Ministère des Affaires Economiques.

- **Niveau 2**

Le niveau 2 est relativement comparable au niveau 1. On peut donc renvoyer en partie à ce qui a été dit précédemment.

Il présente toutefois une différence fondamentale : un tiers intervient dans la détermination des critères.

L'intervention du tiers peut se faire à deux niveaux (non cumulatifs) :

- soit le tiers est chargé par le WIN de rédiger l'ensemble des critères en fonction des exigences du WIN[31] ;

- soit l'intervention du tiers se limite à vérifier les critères rédigés préalablement par le WIN, éventuellement à les modifier, et à les entériner[32].

Pour que l'intervention d'un tiers soit efficace et reconnue comme crédible aux yeux du public, ce tiers doit présenter les caractéristiques suivantes :

- il doit être indépendant du WIN afin d'accomplir sa mission en toute objectivité, et être reconnu par le public en cette qualité ;
- il doit disposer des compétences appropriées (c'est-à-dire une bonne connaissance des législations concernées ainsi que des besoins réels des utilisateurs d'Internet) et, idéalement, une expérience dans le domaine afin de proposer une solution suffisamment protectrice des intérêts des utilisateurs (et des consommateurs en particulier) sans toutefois qu'elle se situe en marge de la réalité du marché ;
- dans la mesure du possible, le tiers doit s'adjoindre la participation d'associations concernées (consommateurs, utilisateurs d'Internet, etc.) pour la rédaction de ces critères.

Une fois la liste établie, le WIN hébergerait la liste des critères soit sur son site soit sur le site du tiers[33]. De la même manière qu'au niveau 1, le renvoi à ces critères pourrait se faire par un hyperlien. Notons cependant que le tiers exigera probablement qu'il soit présenté comme auteur de la liste et que son nom, voire son logo, soit affiché. De plus, ceci est dans l'intérêt du WIN puisqu'il s'agit du moyen le plus aisé d'avertir l'Internaute qu'un tiers est intervenu pour la détermination des critères.

L'adoption du niveau 2 par le WIN présente les *avantages* et *inconvénients* suivants :

Avantages :

- l'intervention d'un tiers dans la détermination des critères est de nature, d'une part, à offrir une liste de critères de grande qualité et, d'autre part, à renforcer la crédibilité de l'initiative ;

- étant donné que la liste ne peut être modifiée unilatéralement par le WIN mais nécessite chaque fois l'intervention du tiers, cela constitue pour l'internaute une garantie de stabilité et de sérieux ;

---

31 Peu importe la forme que peuvent prendre ces critères. Soit ils sont présentés sous la forme d'une liste ad hoc créée exclusivement pour le WIN. Soit ils prennent la forme d'un code de conduite existant auquel renvoie le WIN, de la même manière que le ferait éventuellement d'autres entreprises. La première solution présente l'avantage d'être précise et adaptée à la situation du WIN alors que la seconde présente l'avantage d'être plus largement diffusée et donc connue du public, surtout si le code de conduite résulte d'une initiative publique ou est appuyé par une administration.

32 Cette solution est en principe moins onéreuse que la première tout en offrant une efficacité et un niveau de crédibilité équivalent.

33 La seconde solution est préférable dans la mesure où c'est le meilleur moyen de montrer qu'un tiers est intervenu pour la rédaction des critères.

- l'intervention d'un tiers évite de devoir mobiliser les ressources internes du WIN pour effectuer cette lourde tâche ;

- si la liste est hébergée sur le site du tiers, il sera plus aisé pour l'internaute d'en faire la preuve en cas de contestation étant donné qu'elle ne se trouve plus sous la maîtrise du WIN ;

- cette solution est moins onéreuse et plus facile à mettre en œuvre que les niveaux 3, 4 et 5.

Inconvénients :

- l'intervention d'un tiers pour la détermination des critères ne garantit pas nécessairement à l'utilisateur que ces critères sont effectivement respectés par le WIN[34]. Dès lors, l'absence d'intervention préalable d'un tiers pour vérifier le respect effectif des critères par le site limite la crédibilité de l'initiative. ;

- l'intervention d'un tiers présente des difficultés pour le WIN en termes de coût, de flexibilité et de sélection de ce tiers.

En résumé, la labellisation de niveau 2 impliquerait pour le WIN :

→ définir la liste des critères avec l'intervention d'un tiers ;

→ afficher les critères sur son site ;

→ éventuellement afficher le logo du tiers.

- **Niveau 3**

Le niveau 3 est comparable au niveau 2. On peut donc renvoyer à ce qui a été dit précédemment.

Il présente toutefois une élément supplémentaire : le WIN s'engage à mettre en place un mécanisme de réception des contestations ou plaintes, à essayer de régler le problème à l'amiable et, en cas d'échec, à se soumettre à un système de résolution alternative des litiges (ADR)[35].

L'ADR suppose l'intervention d'un organisme tiers qui se chargerait de traiter en toute objectivité et indépendance la contestation. Le WIN s'engagerait alors à se soumettre à la décision prise par cet organisme.

---

34 Le WIN pourrait toutefois prétendre qu'un de ses services internes, tel que le service juridique, effectue un contrôle du respect effectif de ces critères.

35 L'ADR (Alternative Dispute Resolution) est déjà développé aux Etats-Unis et au Canada avec des initiatives telles que le CyberTribunal, qui propose à la fois la médiation et l'arbitrage (http://www.cybertribunal.org) ; l'Online Ombudsman Office (http://128.119.199.27/center/ombuds) ; le Virtual Magistrate (http://vmag.vcilp.org/). Voir aussi l'article de V. TILMAN publié dans la Revue Ubiquité « Arbitrage et nouvelles technologies : Alternative Cyberdispute Resolution » (numéro 2, p. 47).

L'adoption du niveau 3 par le WIN présente les *avantages* et *inconvénients* suivants :

Avantages :

- la mise en place d'un mécanisme de réception des plaintes et l'engagement d'essayer de trouver une solution à l'amiable démontrent un état d'esprit positif de la part de WIN, qui est de nature à renforcer la confiance des internautes (pour autant que ce système soit effectif !). Le WIN peut même aller plus loin en recourant à l'ADR. Le recours à l'ADR présente un avantage commercial indéniable. En effet, en acceptant de se soumettre à un système d'ADR en ligne, l'utilisateur disposera d'un moyen de recours facile, rapide, relativement efficace et peu onéreux. Ceci constitue une garantie de sérieux de la part du WIN puisqu'il démontre ainsi qu'il entend ne pas profiter du fait que ces avantages n'existent pas pour le recours traditionnel à la justice, ayant pour conséquence que les utilisateurs renoncent à agir en justice et ainsi à leurs droits ;

- les avantages qui sont énumérés pour le niveau 2 sont également applicables ici ;

Inconvénients :

- le recours à l'ADR ne joue pas un rôle préventif comme le joue l'intervention *préalable* d'un tiers pour vérifier le respect effectif des critères par le site ;

- aucun système d'ADR n'est véritablement opérationnel et suffisamment connu sur le marché européen actuellement (mais possibilité de recourir au « CyberTribunal » canadien) ;

- coûts de la mise en place d'un système de réception et de traitement des plaintes, voire du recours à un ADR.

En résumé, la labellisation de niveau 3 impliquerait pour le WIN :

→ définir la liste des critères avec l'intervention d'un tiers ;

→ afficher les critères sur son site ;

→ éventuellement afficher le logo du tiers ;

→ mettre en place une procédure de résolution et de traitement des plaintes.

3.1.2. La labellisation externe

Dans une étape ultérieure, le WIN peut décider d'opter pour une formule de labellisation externe en impliquant pleinement un tiers dans le contrôle préalable et régulier du respect des critères, et/ou dans la détermination ou la révision de ces critères. Un choix entre la labellisation de niveau 4 et la labellisation de niveau 5 s'offre au WIN.

- **Niveau 4**

La différence majeure entre la labellisation interne et la labellisation externe est l'intervention d'un tiers dans le respect de la bonne application des critères par le WIN. Cette intervention donne évidemment davantage de poids à la démarche de labellisation. Dans le niveau 4, la détermination des critères sur lesquels se fonde la labellisation reste de la prérogative du WIN : celui-ci garde la maîtrise de la définition des critères et ne la soumet pas à révision par un tiers. Par contre, le WIN demande au tiers de contrôler la bonne application qu'il fait des critères. Insistons sur le fait que ce tiers n'émettra aucun avis favorable ou défavorable sur la qualité des critères.

Pour ce qui est de la qualité du tiers à qui il est fait appel, on renvoie à ce qui est dit dans le niveau 2 puisque les mêmes critères sont applicables[36] (même si dans le niveau 2 le tiers intervient dans la phase de détermination des critères et non dans la phase de contrôle a posteriori). On peut toutefois ajouter que dans le cadre du contrôle a posteriori, il est important que ce tiers dispose d'une compétence d'audit, puisque le contrôle du respect des critères s'apparente fortement à l'audit d'une société.

La démarche de labellisation de niveau 4 implique l'affichage sur le site du WIN de la liste des critères qui peut se présenter sous forme d'une icône ou d'une phrase expliquant la démarche.

L'intervention du tiers se concrétise à un double niveau de contrôle :

- d'une part un *contrôle a priori* : lors de sa première intervention, le tiers effectuera un contrôle de vérification de l'application des critères par le WIN. Ce contrôle, que l'on peut appeler contrôle a priori, permettra au tiers de se familiariser avec les critères établis par le WIN et d'effectuer une première évaluation ;

- d'autre part un *contrôle a posteriori* : selon une périodicité à déterminer en accord entre le tiers et le WIN, le tiers effectuera des contrôles pour vérifier l'application des critères par le WIN. Les contrôles a posteriori peuvent également résulter de plaintes de visiteurs du site qui dénonceraient une pratique non conforme aux critères.

Il faut noter que l'intervention du tiers se marquera très certainement par l'apposition sur le site du WIN d'un logo ou de tout autre signe distinctif attestant de sa participation. Lors des contrôles de vérification de l'application des critères, le tiers établira un rapport qui attestera du respect des critères par le WIN. Ce rapport pourra soit faire état de la parfaite application des critères par le WIN, soit d'une mauvaise ou imparfaite application des critères. Dans ce dernier cas, le rapport du tiers mentionnera les améliorations à apporter que le WIN devra impérativement respecter : il en va en effet de la crédibilité de l'initiative de labellisation et de l'intervention d'un tiers de se conformer aux recommandations formulées par ce tiers lors de son contrôle d'appréciation. Ensuite, le rapport – qui mentionnera les éventuelles modifications apportées – sera disponible directement sur le site du WIN[37].

---

[36] Rappelons que les qualités professionnelles d'un auditeur sont l'indépendance, l'intégrité, la discrétion et l'objectivité.

[37] A ce sujet, deux options sont possibles : soit le rapport du tiers vérificateur est directement stocké sur une page du site du WIN, soit il est conservé chez le tiers et disponible depuis le site du WIN par le biais d'un lien hypertexte. Sur ce point, voir *infra* le développement sur les aspects « sécurité ».

L'adoption du niveau 4 par le WIN présente les *avantages* et *inconvénients* suivants :

Avantages :

- la liste des critères demeure sous le contrôle du WIN : le tiers n'intervenant pas ni dans la définition des critères ni dans l'aval de ceux-ci, les critères restent stockés sur le site du WIN qui en garde la maîtrise ;

- apposition du logo du tiers : selon toute vraisemblance, le tiers exigera que son logo (ou tout autre signe distinctif) apparaisse sur le site du WIN. Cela n'aura que plus de poids quant à l'initiative de labellisation et renforcera la crédibilité du WIN vis-à-vis de ses clients ;

- le contrôle a priori par le tiers joue un effet préventif indéniable quant à la survenance des litiges ;

- les contrôles a posteriori par le tiers augmentent la crédibilité de l'engagement du WIN ; les éventuelles modifications qui seront apportées suite aux contrôles démontrent également la bonne volonté du WIN.

Inconvénients :

- le principal inconvénient du recours à un tiers est bien entendu la question du coût : en comparaison avec la labellisation interne qui n'implique pas d'investissement conséquent, le coût sera ici élevé, et pourrait être en corrélation avec la notoriété du tiers (plus le tiers sera renommé, plus le prix risque d'être élevé) ;

- l'absence d'intervention du tiers dans le choix ou l'aval des critères risque de diminuer la portée de ceux-ci et d'atténuer la crédibilité de la labellisation ;

- le système est relativement lourd à mettre en place et contraignant.

En résumé, la labellisation de niveau 4 impliquerait pour le WIN :

→ définir la liste des critères sans intervention d'un tiers ;

→ afficher les critères sur son site ;

→ soumettre à un tiers le contrôle du respect des critères ;

→ mettre en place un mécanisme de dépôt et de traitement des plaintes des visiteurs du site ;

→ se conformer aux recommandations du tiers et adopter les modifications nécessaires ;

→ afficher sur le site le rapport du tiers vérificateur ;

→ *en option* : sécurisation de certains éléments (liste de critères, rapport d'audit et label).

- **Niveau 5**

Le niveau 5 se différencie du niveau 4 par l'intervention du tiers dans la détermination des critères, c'est-à-dire soit directement pour la définition des critères, soit seulement pour l'aval de ceux-ci. Il ne faut pas oublier que par *intervention du tiers dans la détermination des critères* on entend également le fait de faire référence à un code de conduite rédigé par une association ou un organisme tiers. Le WIN dispose en effet de la possibilité de faire appel à un tiers pour définir les critères ou de la possibilité de faire référence à un code de conduite existant.

Pour le reste, le niveau 5 fonctionne de la même façon que le niveau 4.

Le choix d'opter pour le niveau 5 de labellisation pourrait se concrétiser par l'adoption de l'initiative ***WebTrust*** telle que reprise par l'Institut des Réviseurs d'Entreprises[38]. Dès que WebTrust sera opérationnel en Europe, on peut imaginer que le WIN y adhère. Dans ce cas, le WIN suivrait la procédure définie par WebTrust : il s'engagerait à respecter les critères définis par WebTrust[39] ; il apposerait sur son site le label WebTrust et ferait un renvoi aux critères ; il se soumettrait à un contrôle de vérification périodique et afficherait le rapport de vérification sur son site. Le choix de WebTrust présenterait l'avantage d'opter pour un mécanisme connu et renommé, et de se soumettre au contrôle de professionnels (c'est-à-dire les principales sociétés de Consulting telles que PriceWaterHouseCoopers, Ernst & Young).

Remarque : les récents développements de WebTrust au niveau européen montrent les évolutions suivantes : le sceau sera revalidé au minimum tous les 90 jours ; le coût fixe du sceau sera de 1.400 EURO auxquels s'ajoutent le coût de l'audit (estimé de 2 à 100 jours/hommes en fonction de la taille de l'entreprise) et le coût de l'audit régulier (estimé de ½ à 10 jours/hommes en fonction de la taille de l'entreprise).

Il faut noter que le choix d'un tiers labellisateur (WebTrust ou autre) peut s'accompagner de la possibilité pour le WIN d'ajouter aux critères du tiers ses propres critères (à l'image de la labellisation proposée par TRUSTe). On se situerait alors entre le niveau 4 et le niveau 5 de labellisation.

L'adoption du niveau 5 par le WIN présente les *avantages* et *inconvénients* suivants :

Avantages :

- à la différence du niveau 4, un tiers intervient dans le choix des critères – ou à tout le moins dans l'évaluation du choix des critères par le WIN – ce qui ajoute en terme de crédibilité puisque le WIN n'est plus seul à déterminer les éléments qui servent de base à la labellisation ;

- pour ce qui est de l'apposition du logo du tiers et les contrôles a posteriori, les mêmes avantages que ceux décrits pour le niveau 4 sont applicables ;

- de toute évidence, cette forme de labellisation est la plus crédible aux yeux des consommateurs. On peut s'attendre à ce que le niveau 5, accompagné d'éléments de sécurité, soit privilégié par le gouvernement dans le cadre de l'article 80 §3 du projet de loi transposant la directive contrats à distance.

---

38 Voir la description du projet d'adapter WebTrust en Europe dans le rapport intermédiaire remis le 3 mai 1999, pp. 34-35.

39 Pour rappel, ces critères sont les suivants : pratiques commerciales, intégrité des informations et protection de l'information.

Inconvénients :

- le seul inconvénient qui demeure est le problème du coût : en plus du coût mentionné au niveau 4 pour l'intervention du tiers dans le contrôle a posteriori, un coût supplémentaire sera certainement demandé par le tiers pour l'évaluation de la qualité des critères.

En résumé, la labellisation de niveau 5 impliquerait pour le WIN :

→ définir la liste des critères avec l'intervention d'un tiers ;

→ afficher les critères sur son site ;

→ soumettre à un tiers le contrôle du respect des critères ;

→ mettre en place un mécanisme de dépôt et de traitement des plaintes des visiteurs du site ;

→ se conformer aux recommandations du tiers et adopter les modifications nécessaires ;

→ afficher sur le site le rapport du tiers vérificateur ;

→ *en option* : sécurisation de certains éléments (liste de critères, rapport d'audit et label).

3.1.3. Remarque concernant l'option sécurisation

Spécialement pour les niveaux 4 et 5, il est possible de renforcer la crédibilité de l'initiative de labellisation en sécurisant certains éléments, à savoir :

- la page des critères ;
- la page du rapport de l'auditeur ;
- le cas échéant, le label.

Cette sécurisation a pour but de vérifier avec une certitude raisonnable les auteurs ou titulaires de ces documents, que leur intégrité n'a pas été compromise et qu'ils ne soient pas usurpés par des personnes non autorisées (par exemple, qu'un faux rapport de vérificateur ne soit simulé ou qu'un label ne soit usurpé par un site non labellisé).

Cette sécurisation peut s'envisager à deux niveaux : d'un point de vue juridique et d'un point de vue technique.

- *D'un point de vue juridique*

La liste des critères ainsi que le rapport du vérificateur sont, pour autant qu'ils présentent un certain degré d'originalité, protégés par le *droit d'auteur*. Leurs auteurs (le WIN ou l'auditeur) pourraient donc s'opposer sur cette base à toute reproduction de ces documents par un tiers (non autorisé). Rappelons que toute atteinte aux droits d'auteur est sanctionnée pénalement (par le délit de contrefaçon par exemple) et/ou civilement (par exemples, par l'action en cessation ou l'action en dommages et intérêts).

Le label (WinTrust par exemple) peut lui aussi être protégé par le droit d'auteur. D'autre part, il pourrait également être déposé comme marque et ainsi protégé par le *droit des marques* pour autant que le label possède un caractère distinctif. Notons que l'article 13, A, 1, d de la Loi Uniforme Bénélux sur les marques (LUBM) permet au titulaire de la marque de s'opposer à « tout usage qui, dans la vie des affaires et sans juste motif, serait fait d'une marque ou d'un signe ressemblant autrement que pour distinguer des produits, lorsque l'usage de ce signe tirerait indûment profit du caractère distinctif ou de la renommée de la marque ou leur porterait préjudice ». Cet article devrait permettre au titulaire de la marque de lutter contre toute usurpation frauduleuse de la marque par un site dans le but de créer une (fausse) apparence de sérieux.

- *D'un point de vue technique*

Différents niveaux de protection sont envisageables. Cette question sera traitée dans le *rapport du Professeur Peeters*. Limitons nous à dire qu'il semble possible :

1. de protéger la liste des critères ainsi que le rapport de l'auditeur en les affichant sur des pages sécurisées (comme le font par exemple, TRUSTe et BBB OnLine) ;

2. de vérifier l'authenticité d'un label en associant celui-ci à un certificat délivré par une autorité de certification. Ce certificat atteste que le label est authentique et qu'il a été délivré à l'entreprise X, et cela suite à une vérification d'un auditeur (comme le fait par exemple WebTrust) ;

3. que l'entité qui octroie le label répertorie dans une base de données sécurisée, accessible grâce à un moteur de recherche, l'ensemble des entreprises auxquelles elle a attribué le label (BBB OnLine ou TRUSTe par exemple). Toute entreprise absente de ces fichiers doit être considérée comme non labellisée ;

4. de mettre en place des moteurs de recherches qui « traquent » les fraudeurs ayant usurpé le label.

3.2. LABELLISATION DES CLIENTS DU WIN

Il ne s'agit plus ici de labelliser les services offerts par le WIN, mais de permettre au WIN d'inciter les clients qu'il héberge (hosting ou housing) d'adopter un système de labellisation (interne ou externe) en leur imposant le respect de critères prédéterminés. On se trouve en présence d'une labellisation « forcée ».

Soit la labellisation est *interne* (niveaux 1, 2 ou 3). Dans ce cas, le WIN se limite à forcer contractuellement ses clients à s'engager au respect de certains critères, avec éventuellement la mise en place d'un mécanisme de réception des plaintes.

Soit la labellisation est *externe* (niveaux 4 ou 5). Dans cette hypothèse, le WIN jouerait le rôle de « labellisateur » à l'instar de WebTrust, TRUSTe ou BBB OnLine[40]. Cela suppose qu'il établisse une liste précise de critères (WinTrust), qu'il effectue l'audit des sites candidats à la labellisation et éventuellement, qu'il fasse appel à une autorité de certification afin d'authentifier le label.

3.2.1. La labellisation interne (niveaux 1, 2 et 3)

Les réflexions qui ont déjà été faites dans le cadre de la labellisation des services du WIN peuvent être répétées dans ce cadre. Nous n'y reviendrons pas. Précisons cependant qu'en ce qui concerne le niveau 1, le fait que les critères soient déterminés par le WIN lui-même ne devrait pas être de nature à enlever toute crédibilité à l'initiative dans la mesure où ceux-ci ne sont plus destinés aux services du WIN mais aux services des clients du WIN. Il n'empêche que le WIN n'apparaîtra jamais comme un véritable tiers car il ne présente pas les caractéristiques développées *infra* (notamment en terme d'indépendance).

Plusieurs questions supplémentaires se posent :

3.2.1.1. Acceptation des critères

L'acceptation du respect des critères est-elle une condition nécessaire pour pouvoir être hébergé comme client par le WIN ? La réponse doit être apportée par le WIN en analysant son intérêt commercial dans l'une et l'autre hypothèse. Si la réponse est négative, le WIN devra être attentif à ce que ses clients labellisés soient bien distingués de ceux qui ne le sont pas pour éviter toute confusion aux yeux du public (le WIN peut tenir une liste des sites labellisés, obliger les sites hébergés et labellisés à l'indiquer clairement voire à afficher un label, interdire aux autres sites de créer une confusion à cet égard, avec une sanction contractuelle en cas de non respect, etc.).

En ce qui concerne le service de support aux transactions en ligne, on peut dire que le WIN assumerait dans une certaine mesure l'engagement (l'auto-labellisation) déclaré par le site hébergé car ce service suppose que le WIN (et non le responsable du site) intervienne techniquement dans la réalisation d'opérations telles que l'acceptation en ligne de l'offre par le client, la transmission en ligne et sécurisée des informations nécessaires à l'exécution de la vente et le traitement sécurisé des paiements en ligne par carte de crédit y afférents. Ceci pose un problème de partage de responsabilités. Le WIN devra préciser la responsabilité qu'il entend assumer dans cette hypothèse.

3.2.1.2. Comment réaliser pratiquement cette labellisation interne ?

→ Le WIN doit avertir ses clients potentiels que la condition (ou la possibilité) pour être hébergé par le WIN est d'accepter le respect de critères prédéfinis. Cette condition (ou cette possibilité) doit

[40] Cette hypothèse ne sera pas développée davantage dans la mesure où il apparaissait clairement lors des réunions que le WIN n'entend pas jouer à court et à moyen terme le rôle de labellisateur.

être clairement indiquée dans la publicité, dans l'offre et doit être rappelée lorsque le client potentiel prend contact avec le WIN.

→ Le WIN doit inclure dans ses contrats d'hébergement (hosting ou housing) une clause par laquelle le client s'engage :

- à respecter les critères prédéfinis ;
- à indiquer sur son site qu'il respecte des critères prédéfinis (il faut trouver un nom attractif) ;
- à renvoyer par un hyperlien à ces critères prédéfinis (soit grâce à un logo tel que par exemple un label « WIN Trust » ou le label du tiers rédacteur des critères soit par un texte).

Si un label est utilisé, celui-ci pourra être sécurisé tant d'un point de vue technique que juridique. Le WIN doit également pouvoir exercer un contrôle afin de déceler toute usurpation du label[41].

→ Idéalement, la page contenant les critères prédéfinis doit se trouver sur le site (et serveur) du WIN ou du tiers pour plusieurs raisons :

- cela permet au WIN ou au tiers de garder la maîtrise de cette page et un niveau de sécurité ;
- cela permet au WIN ou au tiers de recenser les sites qui renvoient à cette page, et ainsi d'exercer un certain contrôle (pour éviter un renvoi abusif à cette page).

→ Le WIN doit indiquer dans le contrat d'hébergement, sur son site (et éventuellement sur le site du client) qu'il se limite à imposer à son client le respect de certains critères mais qu'il n'effectue aucun contrôle *a priori* de ces critères.

→ Toutefois, pour le niveau 3, le WIN doit mettre en place une « hotline » (qui peut prendre plusieurs formes : n° de téléphone (gratuit), fax, e-mail, formulaire sur le site de WIN[42], etc.), dont l'existence et l'accessibilité doivent être clairement indiquées, afin que les utilisateurs puissent faire valoir leurs réclamations ou plaintes (auprès du WIN). Le cas échéant, le WIN doit être en mesure matériellement de répondre à cette demande, il doit se réserver contractuellement le droit et matériellement la possibilité d'effectuer un contrôle, il doit inviter le responsable du site à se mettre en conformité avec les critères et éventuellement sanctionner le site hébergé.

→ Dans le cadre du niveau 3, un recours à l'ADR (Alternative Dispute Resolution, à mettre en place) pourrait être envisagé pour traiter deux cas de figure :

- d'une part, les conflits entre le WIN et le site Web hébergé, en cas par exemple de contestation sur la manière dont le WIN apprécie le respect ou non des critères par le site ;

- d'autre part, les conflits entre les utilisateurs et le site Web : le site Web pourrait s'engager à recourir à l'ADR en cas de réclamation ou de plainte d'un utilisateur. L'ADR se chargerait de traiter en toute objectivité et indépendance la plainte. En fonction de l'appréciation faite par l'ADR, le WIN pourrait éventuellement prendre les sanctions adéquates, sans qu'il n'ait dû se charger du contrôle délicat du respect des critères.

Le recours à l'ADR présente un avantage commercial indéniable pour le site Web. En effet, en acceptant de se soumettre à un système d'ADR en ligne, l'utilisateur disposera d'un moyen de recours facile, rapide, relativement efficace et peu onéreux. Ceci constitue une garantie de sérieux de la part du vendeur. Ces avantages n'existent pas pour le recours traditionnel à la justice, ce qui

---

41 Confer *supra*.

42 Pour la mise en place d'un formulaire permettant aux utilisateurs de dénoncer au WIN une violation par le site des critères qu'il s'était engagé à respecter, un usage abusif du label ou tout autre problème, celui-ci peut s'inspirer du formulaire « Watchdog » mis en place par TRUSTe : http://www.truste.org/users/users_watchdog.html.

incite les utilisateurs à renoncer à agir en justice et ainsi à renoncer à leurs droits. Certains vendeurs peu scrupuleux exploitent cet état de fait.

→ Le WIN doit déterminer les sanctions dans le contrat d'hébergement (clause pénale, résiliation du contrat, inscription sur une liste noire du WIN, etc.) en cas de non respect des critères. Pour le reste, les utilisateurs pourraient toujours attaquer directement le responsable du site qui a violé son engagement quant au respect des critères.

3.2.2. La labellisation externe (niveaux 4 et 5)

Dans l'hypothèse de la labellisation *externe*, le WIN jouerait le rôle de « labellisateur » à l'instar de WebTrust, TRUSTe ou BBB OnLine. Cela suppose qu'il établisse une liste précise de critères (WinTrust), qu'il effectue un audit préalable et périodique des sites candidats à la labellisation, qu'il mette en place un mécanisme de réception et de traitement des plaintes, et éventuellement, qu'il fasse appel à une autorité de certification afin d'authentifier le label.

Comme dit précédemment, cette hypothèse ne sera pas développée davantage dans la mesure où il apparaissait clairement lors des réunions que le WIN n'entend pas jouer à court et à moyen terme le rôle de labellisateur. De plus, nous estimons que l'état des lieux est suffisamment développé et permet d'illustrer (à l'instar de WebTrust, TRUSTe ou BBBOnline) la manière dont le WIN pourrait jouer le rôle de labellisateur. Nous renvoyons donc le lecteur à ce document.

Limitons nous toutefois à préciser que dans une hypothèse bien précise, le WIN pourrait déjà jouer le rôle de labellisateur dans le cadre d'une sorte de labellisation externe sans que cela ne constitue pour lui une grosse contrainte. En effet, si un des services, offert par le WIN et complémentaire au hosting, est la conception de sites Web commerciaux, on peut imaginer que le WIN intègre automatiquement les critères prédéfinis lors de la création de ces sites et de leur gestion ultérieure. Cela renforcerait la crédibilité de cette forme de labellisation puisque le WIN effectuerait en quelque sorte un contrôle a priori, voire a posteriori si le WIN gère le site de son client. Il nous semble que cela doit être promotionné par le WIN et se concrétiser par un signe visible pour que l'utilisateur en prenne connaissance, accompagné éventuellement d'une explication adéquate.

PARTIE 4 – RECOMMANDATIONS

Toute démarche de labellisation doit commencer par le site du WIN lui-même car il est peu concevable que le WIN exige que ses clients soient labellisés s'il ne l'est lui-même. Par ailleurs, la liste des critères pourra être identique dans les deux cas.

Etant donné la situation actuelle, il nous semble que le ***niveau 3 de labellisation*** devrait être adopté par le WIN, à la fois pour son propre site et pour ses clients. A ce titre, le WIN peut s'inspirer de l'initiative de l'AECE.

- *Labellisation du site du WIN*

L'adoption du niveau 3 nous semble être la meilleure pour le WIN pour les raisons suivantes :

- *en terme de crédibilité* : l'intervention d'un tiers dans le choix des critères ainsi que la mise en place d'un mécanisme de réception et de traitement des plaintes renforcent la portée de l'initiative ;

- *en terme de coûts :* les coûts engendrés par l'intervention d'un tiers dans le choix des critères et la mise en place d'une hotline sont nettement inférieurs à ceux résultant des contrôles préalables et périodiques effectués par un auditeur ;

- *en terme de mise en œuvre* : une fois les critères rédigés, l'intervention du WIN se limite à recevoir et à traiter les éventuelles plaintes.

- *Labellisation des clients du WIN*

Là aussi, le niveau 3 de labellisation nous semble le mieux adapté pour les clients du WIN pour les raisons suivantes :

- *en terme de crédibilité* : le fait de proposer – voire d'imposer – le respect des critères par les sites hébergés constitue une garantie de sérieux du WIN, et est de nature à attirer les sites commerciaux respectables ;

- *en terme de visibilité :*

  ⇒ pour le WIN : le renvoi aux critères sur le site du WIN, par exemple par le biais d'un logo, est une manière de faire de la publicité ;
  ⇒ pour les clients : si un logo est placé sur leur site, cela démontre leur volonté et leur engagement à respecter les critères ;
  ⇒ pour les utilisateurs d'Internet : l'initiative est de nature à informer les utilisateurs de leurs droits, et à leur permettre de faire valoir ces droits dans le cadre du mécanisme de réception et de traitement des plaintes.

En résumé, la labellisation de niveau 3 impliquerait pour le WIN :

→ de définir la liste des critères avec l'intervention d'un tiers ;

→ d'afficher les critères sur son site avec un renvoi par le biais éventuellement d'un label ;

→ éventuellement d'afficher le logo du tiers ;

→ de mettre en place une procédure de résolution et de traitement des plaintes ;

→ dans le cadre de la labellisation des clients du WIN, de prévoir des sanctions contractuelles pour les cas où la plainte d'un utilisateur s'avère fondée.