

L'ASBL



**DROIT
&
NOUVELLES
TECHNOLOGIES**

<http://www.droit-technologie.org>

présente :

**LA LABELLISATION DES SITES WEB :
INVENTAIRE DES INITIATIVES EXISTANTES**

Didier GOBERT

assistant à la Faculté de Droit de Namur, Chercheur au CRID

et

Anne SALAÛN

Chercheuse au CRID

<http://crid.fundp.ac.be>

20/02/2000

Avertissement : le recensement qui suit a été effectué en avril 1999, les sites mentionnés peuvent donc avoir évolué depuis cette date. De plus, ce recensement ne doit en aucune façon être considéré comme un jugement critique de la part des auteurs. Il s'inscrit dans le cadre d'une étude plus large, publiée dans la revue DAOR, n° 51, novembre 1999, pp. 83-94, qui vise à élaborer une typologie des différentes formes de labellisation, à déterminer de quelle manière une entreprise peut s'engager dans une initiative de labellisation tant sur la plan de la mise en œuvre que sur celui des avantages et inconvénients, à répertorier les initiatives législatives qui promeuvent la labellisation et enfin à élaborer quelques recommandations.

La présente contribution recense et analyse les principales initiatives de labellisation, c'est-à-dire les labels tels qu'ils existent actuellement aux Etats-Unis et au Canada, ainsi qu'en Espagne. Elle vise également à faire le point sur les projets ayant pour objectif de mettre en œuvre la labellisation en Europe.

1. Initiatives de labellisation opérationnelles

Les labels proposés par WebTrust, BBB OnLine, l'AECE et TRUSTe sont présentés.

1.1. *WebTrust*¹

L'initiative WebTrust part du constat suivant : 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, 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 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 <http://www.cpawebtrust.org>

1.1.1. 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 comptables agréés (CA) et les Certified Public Accountants (CPA) ; le gestionnaire du label : Verisign ; et le demandeur du label.

a) *Les initiateurs des principes et critères WebTrust*

Le 16 septembre 1997, l'ICCA et l'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.

b) *Les 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* sur 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*», et que le CA ou CPA 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.

c) *Le gestionnaire du label*

Verisign, un tiers indépendant, a été désigné comme gestionnaire du label. Il appartient notamment à Verisign de délivrer un certificat numérique *WebTrust*, de fournir un *applet* pour pouvoir afficher le label ainsi que le rapport de l'auditeur et de retirer l'autorisation d'utiliser le label en cas de révocation ou de non renouvellement du rapport.

d) 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.

1.1.2. Les domaines couverts par le label

a) Présentation

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 ».

- Les pratiques commerciales

L'entité candidate à la labellisation doit s'engager 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.

- Intégrité des opérations

Le candidat à la labellisation doit s'engager 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.

- Protection de l'information : vie privée

L'entité doit s'engager 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.

b) 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 précis².

² <http://www.icca.ca/cica/cicawebiste.nsf/public/Aproposdeswebtrust>.

La première version (version 1.0) date du 23 décembre 1997. Une nouvelle version est sortie (version 1.1) le 1^{er} février 1999 et a été soumise à consultation. Celle-ci vise notamment à étendre les exemples afin de couvrir de nouveaux secteurs d'activité (opérations bancaires en ligne et commerce de valeurs).

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. 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 elle a réellement effectué ses opérations conformément aux pratiques de commerce électronique indiquées ; que ses contrôles ont fonctionné efficacement ; qu'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 qu'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*.

1.1.3. Procédure d'attribution du label

a) 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)³. 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.

b) Conditions d'obtention du label

Pour obtenir le label de certification *WebTrust*, l'entité doit respecter tous les principes *WebTrust*.

3 <http://www.icca.ca/cica/cicawebsite.nsf/public/Aproposdeswebtrust>.

L'évaluation se fait par référence aux critères *WebTrust* associés à chacun de ces principes. De plus, l'entité doit, d'une part, 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* ; et d'autre part, obtenir un rapport sans réserve de ce praticien⁴.

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 page⁵ sur son site avec les différentes entreprises qui ont obtenu le label *WebTrust*.

c) 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.

Dans un premier temps, 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 : la nature et la complexité des activités de l'entité, la fréquence des changements importants apportés au site, 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, 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.

Dans un deuxième temps, 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.

1.1.4. Processus de gestion et de sécurisation du label

a) 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.

⁴ Un questionnaire d'auto-évaluation doit aider la direction de l'entité à établir le bien-fondé de sa déclaration : <http://www.icca.ca/cica/cicawebsite.nsf/public/Aproposdeswebtrust>.

⁵ <http://www.verisign.com/webtrust/siteindex.html>

- 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.

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

- Expiration du label

A moins qu'un avis de mise à jour ne soit reçu, l'autorisation d'afficher le label prend fin à sa date d'expiration. 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.

b) 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).

Il est important de préciser qu'en l'absence de ce certificat numérique, le label *WebTrust* ne doit pas être considéré comme valide.

1.2. BBB OnLine⁶

1.2.1. Les intervenants

L'initiative BBB OnLine met en jeu l'initiateur du label, les *Better Business Bureaus*, et les sites Web demandeurs du label.

6 <http://bbbonline.org>

a) L'initiateur du label : les Better Business Bureau

BBB OnLine a été créé aux Etats-Unis en avril 1997 dans le but de répondre au souhait de promouvoir la confiance des consommateurs dans le commerce électronique. 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, la fiabilité des sites et la protection de la vie privée.

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. 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 % estimerait qu'une assurance de la fiabilité du site les inciterait à acheter davantage.

b) Les demandeurs du label

Les sites qui souhaitent bénéficier du label BBB OnLine doivent s'identifier et suivre la procédure ad hoc. 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.

1.2.2. Les domaines couverts

a) 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 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.

b) Privacy label

Le but du label '*privacy*' 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 ».

Les critères à respecter sont les suivants : i) attester l'adoption d'une politique de protection des données et de mesures de sécurité. Cette politique doit être clairement indiquée sur le site ; ii) 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. ; iii) participer au programme de résolution des litiges ; iv) garantir la sécurité des données collectées et se prémunir contre un accès non autorisé par l'adoption de mesures de sécurité adéquates ; v) informer BBB OnLine de tout changement dans la politique à l'égard des données personnelles ; vi) fournir un lien vers la politique à l'égard des données personnelles sur chaque page où des données sont collectées ; vii) informer les tiers vers qui des données sont transférées de la

politique en matière de vie privée ; viii) exiger des tiers qui ont accès à des données qu'ils les gardent confidentielles.

c) 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 critères se basent notamment sur le 'Children's Online Privacy Protection Act' de 1998.

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

1.2.3. La procédure d'attribution

a) 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 ; 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.

b) Privacy label

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 ; 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 label⁷.

c) 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

⁷ A titre d'illustration, BBB OnLine estime que seuls 12 à 15 % des sites audités ont nécessité un réajustement pour obtenir le label

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.

1.2.4. Processus de gestion et de sécurisation du label

a) *Gestion du label*

Le label octroyé au site 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 « BBB OnLine Reliability – Participation Confirmed ». Cette page contient 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'.

b) *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, 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.

c) *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.

1.3. *Sello de Garantía de la Protección de Datos*⁸

1.3.1. Les intervenants

a) *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.

b) *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.

1.3.2. 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 données⁹, et se matérialise par un *code de conduite* que les sites doivent respecter. Les objectifs du label sont d'une part d'assurer le respect par les sites qui affichent le label des principes énoncés dans le code de conduite, et d'autre part d'informer du

⁸ <http://www.aece.org>

⁹ Loi organique de régulation du traitement informatisé des données personnelles.

traitement des données obtenues sur Internet et d'offrir au consommateur la possibilité de s'opposer à un traitement.

1.3.3. L'attribution du label

a) *La procédure*

La procédure se déroule en plusieurs étapes : i) solliciter l'octroi du label auprès de l'association et remplir un formulaire ad hoc ; ii) l'association envoie au demandeur le code de conduite et le contrat par lequel le demandeur doit s'engager à respecter le code ; iii) 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 ; iv) 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 ; v) l'association confirme au demandeur la réception du contrat et l'enregistrement de sa politique de protection des données personnelles ; vi) le demandeur affiche le label sur la page principale de son site et sur toute page où des données personnelles sont demandées.

b) *Le prix*

Une distinction est effectuée entre les sites déjà membres de l'association pour lesquels l'utilisation du label est gratuite ; et les sites non membres qui sont redevables d'une cotisation annuelle dont le montant varie selon leur chiffre d'affaire annuel¹⁰.

1.3.4. Processus de gestion et de sécurisation 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.

1.4. *TRUSTe*¹¹

TRUSTe est une initiative indépendante et sans but de lucre relative à la vie privée, 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 que si l'autorégulation se développe efficacement, aucune initiative législative contraignante ne sera prise).

TRUSTe a été créé par *Electronic Frontier Foundation* (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 *CommerceNet Consortium* (dont la mission est d'accélérer le développement du

¹⁰ Soit un prix qui varie entre 15.000 et 90.000 pesetas.

¹¹ <http://www.truste.org>

commerce électronique global, notamment en travaillant à la suppression des obstacles à ce développement).

L'idée de créer TRUSTe est née aux Etats-Unis 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.

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 en vigueur (depuis octobre 1998) 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'industrie¹². 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 : 1) éduquer 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 fin¹³ ; 2) servir de point de liaison entre les consommateurs et les sites licenciés quand c'est nécessaire ; et 3) encourager le milieu des affaires à afficher leur « déclaration vie privée » et à participer au programme de labellisation surveillé par une tierce partie.

1.4.1. Les intervenants

La 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. 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.

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

¹² Selon une enquête, 88 % de l'ensemble des utilisateurs américains d'Internet visitent tous les mois un site licencié par TRUSTe. De plus, les sites licenciés par TRUSTe représentent 33 % de la totalité du trafic Internet américain.

¹³ Voir : http://www.truste.org/users/users_protect.html

1.4.2. Les domaines couverts par le label

a) *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, accessible généralement via 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. Ils 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.

b) *Les critères retenus*

▪ 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 révélera les informations suivantes : les données collectées sur la personne concernée ; qui collecte ces données ; comment ces données seront utilisées ; avec qui l'information sera partagée ; les 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 l'utilisateur peut mettre à jour ou corriger les erreurs sur ses données.

▪ 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. Dès lors, le site Web qui affiche le label pour les enfants s'engage à obtenir le consentement préalable des parents quand des données sont collectées ainsi qu'à avertir les parents de la manière dont ces dernières sont 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.

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.

1.4.3. la procédure 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 tâche¹⁴).

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 ; 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.

1.4.4. Processus de gestion et de sécurisation du label

a) 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 ;

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

- 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 page¹⁵ a été créée sur le site pour effectuer ce type de réclamation, dénommée « Watchdog ». 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, un contrôle de conformité est effectué par une firme d'audit.

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).

b) 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 prises 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. Les projets de labellisation

Divers projets visant à développer une initiative de labellisation sont actuellement à l'étude en Europe. Certains relatent une label limité à un échelon national, comme c'est le cas pour le Centre Régional de la Consommation en France et pour Ready en Belgique ; d'autres (l'Institut des Réviseurs d'Entreprise) font état d'une volonté de développer un label européen.

2.1. CRC – Centre Régional de la Consommation¹⁶

Un groupe de travail du CRC-Consommation a mené une réflexion qui a abouti à un projet d'identifiant qualitatif qui permettrait au consommateur de mesurer la réalité économique de l'entreprise dont il visite le site ; de consulter ses droits et devoirs en terme de protection juridique, en fonction des textes régissant la vente à distance ; et d'avoir la certitude que l'entreprise a rédigé une convention avec une structure consomériste, précisant qu'elle a parfaitement connaissance du droit applicable en matière de vente à distance.

15 http://www.truste.org/users/users_watchdog.html

16 <http://www.crc-conso.com/>

L'idée d'un identifiant qualitatif, en d'autres termes 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.

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

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 ».

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.

2.2. Ready¹⁷

Ready a pris lui-même l'initiative de la labellisation en diffusant dans un premier temps un contrat de confiance sur son site, et en demandant dans un deuxième temps à un tiers indépendant de vérifier les engagements pris dans ce contrat de confiance. Ce contrat comprend 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 la 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* ».

¹⁷ <http://www.ready.be>

L'organisme indépendant établira un premier rapport sur le respect des engagements 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. L'organisme tiers contrôlera alors la bonne application des recommandations, et émettra un second rapport qui sera disponible sur le site de Ready.

2.3. IRE – Institut des Réviseurs d'Entreprise

L'institut des réviseurs d'entreprises en Belgique s'intéresse à la labellisation depuis plus d'un an. L'option prise au niveau des réviseurs d'entreprise européens a été, plutôt que de créer un propre label, de reprendre et d'adapter WebTrust en Europe.

Une Commission de Travail « labellisation des sites Web » a été créée au sein de l'IRE. Son rôle est, d'une part, de rédiger une norme énonçant les principes à suivre par les réviseurs pour labelliser un site Web ; et, d'autre part, de négocier le contrat de licence WebTrust : la décision d'opter pour le label WebTrust a en effet été prise fin 1998.

L'idée de la Commission de travail 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.

(publié dans *Communications & Stratégies*, 3^{ème} trimestre 1999, n° 35, pp. 229 - 251.)

Didier Gobert

Chercheur au CRID

Assistant à la faculté de droit de Namur – Belgique

Anne Salaün

Chercheuse au CRID

<http://crid.fundp.ac.be>