Le développement du commerce électronique

Antoine, Mireille; Gobert, Didier; Salaun, Anne

Published in:
Droit des technologies de l'information. Regards prospectifs : à l'occasion des vingt ans du C.R.I.D

Publication date:
1999

Document Version
le PDF de l'éditeur

LE DÉVELOPPEMENT DU COMMERCE ÉLECTRONIQUE : LES NOUVEAUX MÉTIERS DE LA CONFIANCE

Mireille ANTOINE, Didier GOBERT et Anne SALAÜN*

INTRODUCTION GÉNÉRALE

1. La récente explosion d'Internet et l'émergence d'un nouveau style de commerce représentent un extraordinaire élargissement des possibilités commerciales offertes aux entreprises et de communications offertes aux administrations. Toutefois, le développement d'un contexte de confiance est un préalable nécessaire en raison de certains risques potentiels relatifs notamment à l'identification des parties, à la transmission des données personnelles, à la sécurisation des paiements, au respect de la législation relative à la protection des consommateurs. Ces risques représentent actuellement un frein au développement des transactions sur Internet.

Afin d'assurer le développement harmonieux du réseau des réseaux, plusieurs techniques permettent de gagner la confiance des utilisateurs d'Internet. Ces techniques impliquent généralement le recours à un tiers (autorité de certification, *labellisateur*, médiateur ou arbitre électronique), dont le métier est précisément d'intervenir afin de créer, d'une autre manière que dans l'environnement traditionnel, un contexte dans lequel les transactions peuvent s'opérer en toute confiance et de manière sécurisée.

L'on voit ainsi se développer non seulement des « métiers de la confiance », tels que ceux de la certification et de la labellisation, mais également de nouveaux modes de règlement des litiges plus proches, plus rapides et moins onéreux.

Cette contribution vise à illustrer les domaines d'intervention de ces tiers ainsi que le régime juridique dans lequel cette intervention devrait s'opérer. Dans un premier temps, nous aborderons le thème de la certification électronique. Ensuite, nous traiterons de la labellisation des sites web. Enfin, nous envisagerons les modes alternatifs de résolution des litiges et proposerons quelques recommandations.

* Chercheurs au CRID-FUNDP.

PREMIÈRE PARTIE. LA CERTIFICATION ÉLECTRONIQUE

2. Le développement des communications en réseau ouvert et plus particulièrement du commerce électronique nécessite non seulement le développement de nouvelles techniques de signatures, mais également leur reconnaissance juridique. Celle-ci passe par l'intervention d'autorités tierces. À cette fin, la Commission européenne a présenté le 16 juin 1998 une proposition de directive sur un cadre commun pour les signatures électroniques. Cette proposition de directive poursuit essentiellement deux objectifs majeurs. Le premier est la reconnaissance juridique des signatures électroniques (1). Le second est la création d'un cadre légal pour le fonctionnement des prestataires de services de certification aussi appelés autorités de certification (2). L'intervention de ces tiers de confiance est indispensable pour garantir une utilisation efficace et fiable de la signature électronique.

La Commission entend donc, à travers cette initiative, favoriser l'utilisation des signatures électroniques et renforcer la confiance des utilisateurs pour l'usage des nouvelles technologies de l'information et des applications qui en découlent.

1. Reconnaissance légale des signatures électroniques

1.1. Reconnaissance légale des signatures électroniques

3. La proposition de directive entend tout d'abord promouvoir la reconnaissance légale des signatures électroniques. Pour parvenir à cette fin, diverses approches étaient possibles[1]. Celle qui a été choisie par la Commission se fonde sur une approche fonctionnelle de la signature, rejoignant sur ce point la loi type sur le commerce électronique adoptée par la CNUDCI[2].

La proposition de directive définit la signature électronique comme étant « une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification ». Cette définition de la signature électronique englobe un ensemble de techniques permettant la réalisation par voie électronique des fonctions de la signature classique, à savoir l'identification du signataire et sa manifestation de volonté d'adhérer au contenu du message auquel la signature se réfère. La proposition de directive suggère une distinction

---

1 M. ANTOINE, D. GOBERT, « Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification », *R.G.D.C.*, juillet-octobre 1998, n° 4/5, pp.285-310.

2 Guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur le commerce électronique (1996), pp. 38 et 39.

entre ce terme générique de signature électronique et une technique plus spécifique de signature électronique qu'elle qualifie de « signature électronique avancée ». En choisissant ce terme, la Commission choisit la voie de la neutralité technologique afin, d'une part d'éviter que la proposition de directive devienne rapidement obsolète et, d'autre part, d'encourager la recherche et le développement de nouvelles techniques de signature. Toutefois, il ne fait pas de doute que, à l'heure actuelle, seule la technique de signature digitale ou numérique fondée sur le mécanisme de cryptographie asymétrique[3] réponde à la définition de la signature électronique avancée donnée par la proposition de directive.

1.2. Effets juridiques de la signature électronique

4. Si la proposition de directive donne une définition de la signature électronique, elle entend également dans un second temps réglementer ses effets juridiques. Tel est l'objet de l'article 5 qui contient deux clauses : l'une d'assimilation et l'autre de non-discrimination[4]. La distinction entre ces clauses est essentiellement fondée sur la qualité de l'intervention de tierces parties, les prestataires de services de certification.

S'agissant tout d'abord de la clause d'assimilation, la proposition de directive entend assimiler les signatures électroniques avancées aux signatures manuscrites pour ce qui est de leurs conséquences juridiques si, toutefois, ces signatures reposent sur un certificat agréé, conformément à l'annexe 1, créé par un dispositif sécurisé de création de signature tel que décrit à l'annexe 3. S'agissant des certificats agréés, la proposition de directive fixe, en son annexe 2, les conditions auxquelles les prestataires de services de certification, tiers de confiance délivrant de tels certificats doivent se conformer. L'intérêt de cette clause est d'assimiler les signatures électroniques avancées aux signatures manuscrites de façon telle à ce qu'elles puissent bénéficier de la même force probante[5] que celle qui est attachée à ces dernières.

En ce qui concerne la clause de non-discrimination, celle-ci vise les signatures ne répondant pas aux conditions requises pour pouvoir être assimilées aux signatures manuscrites, notamment celle relative à la délivrance du certificat par un organisme tiers « agréé ». Le principe énoncé au point 2 de l'article 5 doit être compris comme celui de la recevabilité des signatures électroniques au sens large. En vertu de ce

---

3 Pour une description du fonctionnement de la signature digitale, voy. M. ANTOINE, D. GOBERT, *op.cit.*, p. 292.

4 D. GOBERT, E. MONTERO, « La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle », in *Le consentement électronique*, dans un ouvrage collectif à paraître.

5 Par force probante, on entend « l'intensité quant à la preuve que la loi lui reconnaît et qui s'impose au juge ». F. DUMON, « De la motivation des jugements et arrêts et de la foi due aux actes », *J.T.*, 1978, p. 486.

principe, toute signature électronique est recevable mais, à défaut de répondre aux spécifications de l'article 5.1., il appartient à celui qui s'en prévaut de convaincre le juge de sa valeur probante.

2. Création d'un cadre légal pour le fonctionnement des prestataires de services de certification

5. Les nouvelles techniques de signature permettent au destinataire de données signées électroniquement de vérifier l'origine et l'intégrité des données reçues. Toutefois, la confiance dans un mécanisme de signature électronique, et spécialement dans un mécanisme de signature basé sur la technique de cryptographie asymétrique, dépend de l'intervention de tierces parties de confiance, les prestataires de services de certification, qui pourront certifier le lien entre une personne et son dispositif de vérification de signature par l'émission de certificats.

Le principe posé par la proposition de directive est celui de la liberté de fourniture des services de certification. Les États membres ne peuvent soumettre celle-ci à aucune autorisation préalable, tout comme ils ne peuvent limiter le nombre de prestataires de services de certification. La proposition de directive reconnaît toutefois la possibilité pour les États membres, tout en respectant le principe de la liberté de fourniture de certification, d'édicter des critères « objectifs, transparents, proportionnés et non discriminatoires » pour élever le niveau de service fourni par ces tiers de confiance.

La proposition de directive entend mettre sur pied un mécanisme de certification fiable. Celui-ci s'articule autour de trois points essentiels : tout d'abord celui de la responsabilité des tiers de confiance, prestataires de services de certification, ensuite celui de la protection des données personnelles, enfin celui de la reconnaissance, sous certaines conditions, de certificats émis dans des pays tiers. L'intervention de ce tiers peut perdre toute crédibilité si elle ne se réalise pas dans le respect de ces conditions minimales.

2.1. Responsabilité

6. La proposition de directive ne traite des questions relatives à la responsabilité qu'à propos des certificats émis par les prestataires de services de certification qui délivrent au public des certificats présentés comme agréés ou qui garantissent publiquement de tels certificats. Dès lors, pour les prestataires de services de certification qui délivrent des certificats ordinaires (qui ne sont pas présentés comme agréés), les différentes législations nationales relatives à la responsabilité trouvent à s'appliquer.

7. Pour les certificats agréés, la proposition de directive établit un régime spécifique de responsabilité. Celui-ci tente d'établir un équilibre entre les intérêts des tiers, prestataires de services de certification, et des utilisateurs de certificats, c'est-à-dire « toute personne qui se fie légitimement au certificat ». Notons que la proposition de directive ne traite pas des questions relatives à la responsabilité qui pourraient se poser dans le cadre des relations entre les prestataires de services de certification et les titulaires de certificats. Ici aussi, à défaut de règles spécifiques, le droit commun de la responsabilité trouve à s'appliquer.

En vertu de l'article 6,1 de la proposition de directive, le prestataire de services de certification agréé qui délivre un certificat présenté comme agréé ou qui garantit publiquement un certificat doit garantir :

— l'exactitude des informations contenues dans le certificat agréé à la date où il a été délivré ;

— l'assurance que, au moment de la délivrance du certificat, la personne identifiée dans le certificat agréé détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signatures fournies ou identifiées dans le certificat ;

— dans le cas où le prestataire de services de certification génère les données afférentes à la création de signature et celles afférentes à la vérification de signature, l'assurance que ces deux types de données puissent être utilisés de façon complémentaire ;

— la validité du certificat. Cet élément se dégage du point 1 bis de l'article 6 en vertu duquel le prestataire de services de certification doit être tenu responsable de tout préjudice causé à une personne qui se prévaut légitimement du certificat pour avoir omis de faire enregistrer la révocation dudit certificat.

Les obligations énumérées à l'article 6 visent toutes à assurer l'exactitude des informations mises à la disposition des utilisateurs. En réalité, l'exactitude constitue l'essence même de la fonction de certification : elle conditionne la confiance que les utilisateurs peuvent placer dans un mécanisme de certification.

Le prestataire de services de certification est donc responsable de tout préjudice causé à toute personne qui se fie légitimement au certificat et qui découle du manquement à une des obligations énumérées sauf si elle prouve qu'elle n'a commis aucune négligence.

8. Le prestataire de services de certification peut limiter sa responsabilité. Deux types de clauses relatives à la responsabilité du prestataire peuvent figurer sur le certificat agréé. Le prestataire de services de certification peut tout d'abord fixer des limites à l'utilisation du certificat. Dans cette hypothèse, il ne doit pas être tenu responsable du

préjudice résultant de l'usage abusif du certificat qui contient des limites à son utilisation. Il peut ensuite indiquer dans le certificat la valeur limite des transactions pour lesquelles le certificat peut être utilisé.

9. La formulation des règles relatives à la responsabilité suscite deux commentaires.

Tout d'abord, il est indispensable qu'un régime d'accréditation soit mis sur pied dans chaque État membre. La proposition de directive parle, en son article 6, de certificats présentés comme agréés, ce qui peut laisser entrevoir un régime d'autolabellisation qui n'est pas de nature à renforcer la confiance que la proposition de directive est censée susciter. Il est indispensable que la qualité de prestataire de services de certification agréé soit décernée par un organisme tiers chargé de vérifier que les conditions auxquelles est subordonnée l'agréation sont remplies.

Ensuite, la proposition de directive ne prévoit l'obligation pour le prestataire de services de certification de vérifier la complémentarité des clés que dans l'hypothèse où il génère ces deux types de données. Or cette obligation nous paraît fondamentale pour toute AC qui offre au public le niveau de certificat voulu par la proposition de directive. En effet, en délivrant un certificat, un prestataire de services de certification confirme le lien entre le titulaire d'un certificat et son dispositif de vérification de signature. La certification demeure vide de sens si, certifiant ce lien, le prestataire de services de certification omet de vérifier la complémentarité des données afférentes à la création et à la vérification de signature. En effet, l'assurance que doit avoir le destinataire d'un message signé électroniquement porte sur la garantie que la signature électronique qu'il entend vérifier émane bien du signataire, c'est-à-dire qu'au dispositif de vérification de signature correspond un dispositif de création de signature.

10. Outre les obligations pesant sur les prestataires de services de certification délivrant des certificats présentés comme agréés, la proposition de directive soumet l'activité de ceux-ci au respect des prescriptions énumérées à l'annexe 2 de la proposition de directive. Celles-ci tendent toutes à garantir la sécurité du mécanisme de certification.

2.2. Protection des données à caractère personnel

11. Le prestataire de services de certification, qui est chargé d'établir un certificat, doit être en mesure de vérifier de manière certaine et non équivoque l'identité du candidat titulaire. À cette fin, il est amené à collecter diverses informations à son propos. La proposition de directive entend réglementer la collecte d'informations. Ainsi, elle impose aux États membres de veiller à ce qu'un prestataire de services de certification ne puisse recueillir de données personnelles que directement auprès de la personne concernée ou avec son consentement explicite et uniquement dans

la mesure où cela est nécessaire à la délivrance et à la conservation du certificat (article 8,2°).

Le candidat titulaire ne désirant pas ou n'étant pas légalement obligé de communiquer son identité, peut choisir un pseudonyme qui lui permettra de sauvegarder son anonymat. Ce droit à l'anonymat est consacré par la proposition de directive. En vertu de ce principe, les États membres ne peuvent empêcher le prestataire de services de certification d'indiquer dans le certificat un pseudonyme au lieu du nom du signataire (article 6, 2°).

2.3. Reconnaissance transfrontière des certificats

12. Afin de présenter une réelle utilité, toute infrastructure de certification doit être envisagée dans une perspective internationale. C'est pourquoi la proposition de directive requiert, en son article 7, que les États membres traitent les certificats agréés par un prestataire de services de certification établi dans un pays tiers comme équivalents aux certificats délivrés par un prestataire de services de certification établi dans la Communauté européenne pourvu qu'une des conditions suivantes soit remplie :

— le prestataire de services de certification remplit les conditions visées dans la proposition de directive et a été accrédité dans le cadre d'un régime volontaire d'accréditation établi dans un État membre ;

— un prestataire de services de certification établi dans la Communauté, qui satisfait aux exigences de la proposition de directive, garantit le certificat ;

— le certificat ou le prestataire de services de certification est reconnu dans le cadre d'un accord bilatéral ou multilatéral entre la Communauté et des pays tiers ou des organisations internationales.

Par cette disposition, la proposition de directive entend susciter la confiance des utilisateurs et ouvrir les portes au commerce international.

Quelques réflexions critiques

13. En pratique, la proposition de directive ne revêt d'intérêt et n'est de nature à susciter la confiance que si les États membres, tout en respectant le principe de la liberté d'exercice de l'activité de certification, d'une part, mettent sur pied un régime d'accréditation des prestataires de services de certification, subordonnant l'octroi d'une accréditation au respect des conditions prévues à l'annexe 2 et, d'autre part, soumettent l'activité de ces autorités de certification accréditées au respect des conditions prévues à l'annexe 1 et la création de signatures aux prescriptions de l'annexe 3.

À défaut de modification législative, l'on pourrait craindre que l'objectif visé par la proposition de directive soit manqué puisque, quand bien même celle-ci résoudrait-elle la question de la recevabilité des documents signés électroniquement, le pouvoir discrétionnaire du juge quant à l'appréciation de leur valeur probante serait de nature à rendre l'issue du litige incertaine.

14. D'autre part, il convient d'accroître la protection du consommateur en imposant au vendeur d'utiliser une signature électronique avancée (fondée sur un certificat émis par une autorité de certification accréditée). À défaut d'une telle obligation, un vendeur abusif pourrait refuser de recourir à un système sécurisé, sachant qu'ainsi le consommateur ne bénéficierait pas de la clause d'assimilation.

15. Par ailleurs, si l'on désire réellement renforcer la confiance par l'intervention de tiers, la qualité de « prestataire de services de certification agréé » devrait être octroyée à l'issue d'une procédure d'accréditation menée par un organisme indépendant chargé de vérifier si les conditions fixées à l'annexe 2 de la proposition de directive sont remplies. Or, la formulation de la proposition de directive est ambiguë à ce sujet car elle laisse supposer que l'octroi de cette qualité par un organisme indépendant n'est pas indispensable. On peut en effet déduire de l'article 6 qu'un prestataire de services de certification peut offrir des certificats qu'il qualifie d'« agréés » en dehors de tout contrôle. Cette situation d'apparence n'est pas de nature à renforcer la confiance. Il conviendrait au contraire d'écarter toute ambiguïté en prévoyant une sanction pénale pour les prestataires de service de certification usurpant la qualité de prestataire « agréé ».

16. Enfin, la proposition de directive ne veut pas se limiter à la délivrance et à la gestion de certificats mais couvre également tout autre service et produit utilisant des signatures électroniques ou connexes à celles-ci (services d'enregistrement, services horodateurs, services d'annuaires …). La question s'est dès lors posée de savoir si la labellisation[6] pouvait être qualifiée de connexe à la signature électronique. Si tel avait été le cas la future directive aurait été d'application. Si la réponse est négative eu égard à l'objectif fixé par la proposition de directive, la nécessité d'une réglementation européenne en la matière est ressentie.

6 Voir *infra*, Partie 2 : La labellisation des sites WEB.

PARTIE 2. LA LABELLISATION DES SITES WEB

17. Afin d'assurer le développement harmonieux du réseau des réseaux, plusieurs techniques permettent de gagner la confiance des utilisateurs d'Internet. L'une d'elles est la labellisation des sites Web qui offre des conditions de confiance et de sécurité nécessaires à l'essor du commerce électronique.

La labellisation est le résultat de la combinaison de la technologie et de l'audit. Elle poursuit essentiellement l'objectif de donner une meilleure visibilité à un site Web et aux pratiques que celui-ci applique dans les relations avec ses clients. Elle peut représenter un argument commercial visant à augmenter la vente des produits et des services offerts sur le web. De surcroît, la labellisation atteste la volonté du responsable du site de s'engager, 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 certain à participer à une initiative de labellisation, sans toutefois que cela puisse se faire à n'importe quel prix.

Une analyse des initiatives existantes permet de montrer que la labellisation peut prendre plusieurs formes, présentant chacune des avantages et inconvénients pour le site qui y recoure. Par ailleurs, celles-ci offrent des niveaux de fiabilité différents ou s'inscrivent dans un cadre vide de contenu, ce qui risque parfois de tromper le consommateur.

Après une présentation des initiatives législatives en lien avec la labellisation (1), un essai de classification des différentes formes de labellisation est proposé (2). Enfin, quelques réflexions plus générales relatives à l'intervention d'un tiers dans le cadre de la labellisation sont présentées (3).

1. Initiatives législatives en lien avec la labellisation

18. Les législateurs belge et luxembourgeois se sont récemment engagés dans la promotion de la labellisation. De plus, plusieurs initiatives, notamment européennes, promouvant l'auto-réglementation sont à mentionner.

1.1. Promotion de la labellisation

19. La loi belge du 25 mai 1999[7], qui transpose la directive européenne relative aux contrats à distance[8], introduit la labellisation dans son article

---

7 Loi modifiant la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, *M.B.*, 23 juin 1999, p. 23670.

8 Directive 97/7/CE du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance, *J.O.C.E.*, L 144, du 4 juin 1997.

80. Le paragraphe 3 de cet article 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 de ces sommes. Au titre de garanties, le commentaire de l'article 80 parle de « système de cautionnement, de blocage transitoire des sommes versées, d'assurance ou de labellisation – notamment des sites de commerce électronique »[9].

On constate donc, d'une part, que la labellisation est envisagée par le législateur belge 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, qui fixera les conditions pour pouvoir bénéficier de cette dérogation à l'interdiction d'exiger un paiement anticipé.

20. Le projet de loi luxembourgeois relatif au commerce électronique introduit lui aussi la labellisation dans son titre III sur « les contrats conclus par voie électronique »[10]. 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 ».

Une nouvelle fois, la labellisation — ou certification de qualité — du vendeur vient assouplir les obligations qui sont imposées à ce dernier et apparaît, aux yeux du législateur, comme une technique qui permet de renforcer la confiance.

1.2. Promotion de l'auto-réglementation

21. La promotion de l'auto-réglementation participe également au développement de la labellisation dans la mesure où les codes de conduite qui en émanent peuvent servir de base aux critères que les sites s'engagent à respecter dans le cadre d'une initiative de labellisation.

22. La proposition de directive du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur encourage, dans son article 16, l'adoption de codes de

---

9 Document de la Chambre des Représentants, session ordinaire, 10 mars 1999, projet n°2050/1-98/99, pp. 30-32, disponible sur le site Web de la Chambre : http://www.lachambre.be/documents_parlementaires.html.

10 Texte disponible à : http://www.droit.fundp.ac.be/textes/EcoLU.pdf.

conduite par les États membres[11]. 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[12]. 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.

23. On trouve également dans le Chapitre V de 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[13], un encouragement à adopter des codes de conduite. L'article 27 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 États membres en application de la directive ».

24. Enfin, les Pays-Bas ont récemment publié la première version d'un code de conduite relatif au commerce électronique[14]. Cette initiative, initiée par le Ministre de l'économie néerlandais, fait suite à une conférence organisée aux Pays-Bas en juin 1998 sur le thème « The legal framework for electronic commerce : selfregulation ? ».

2. Les différentes formes de labellisation

25. Étant donné la place privilégiée que le législateur, tant européen que belge et luxembourgeois, accorde directement ou indirectement à la labellisation des sites Web, il nous semble important de définir ce concept et de proposer une classification des différentes formes de labellisation que nous avons pu dégager à la lumière des initiatives existantes[15].

2.1. Définitions et classification

26. Une initiative de labellisation peut prendre plusieurs formes, les deux principales étant la labellisation interne et la labellisation externe. Elles peuvent être définies de la façon suivante :

---

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

12 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.

13 *J.O.C.E.*, 23 novembre 1995, p. 281.

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

15 Mentionnons par exemple les initiatives suivantes : WebTrust (http://www.cpawebtrust.org), BBB OnLine (http://bbbonline.org), TRUSTe (http://www.truste.org), AECE (http://www.aece.org), CRC (http://www.crc-conso.com/) et Ready (http://www.ready.be). Pour un état des lieux approfondi de ces initiatives, voy. Didier GOBERT et Anne SALAUN, « La labellisation des sites web : inventaire des initiatives existantes », *Communications & Stratégies*, septembre 1999.

— ***la labellisation interne :*** elle consiste à 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 préalable et périodique par un organisme tiers indépendant ;

— ***la labellisation externe*** : elle consiste à faire contrôler préalablement 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[16] et périodique d'un organisme tiers indépendant dans le *contrôle du respect de 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).

Afin d'éviter toute confusion, il convient de noter que l'intervention d'un tiers peut se situer à deux niveaux : soit il intervient pour la détermination des critères[17] (c'est-à-dire un contrôle de la qualité des critères) ; soit il intervient pour contrôler le respect effectif par le site Web des critères prédéfinis (c'est-à-dire un contrôle de conformité aux critères).

Par contre, il ne semble pas que l'origine de l'initiative, la détermination ou non des critères par un tiers ou encore la sécurisation ou non du label soient des éléments déterminants pour distinguer ces deux types de labellisation[18].

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

2.2. La labellisation interne

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

Le *premier niveau* de labellisation présente les caractéristiques suivantes : d'une part, les critères sont déterminés par le candidat à la

16 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.

17 En pratique, soit les critères peuvent être directement rédigés par un tiers, soit un projet peut être rédigé par le candidat à la labellisation et être revu et avalisé par un tiers.

18 La sécurisation peut être juridique, par le dépôt d'une marque par exemple, et/ou technique, par un certificat émis par une autorité de certification, par le renvoi à une page sécurisée ou par l'utilisation d'un moteur de recherche « traquant » les fraudeurs.

labellisation sans intervention d'un tiers ; d'autre part, ceux-ci sont affichés sur le site du candidat à la labellisation. Il convient de noter que le renvoi à ces critères peut éventuellement se matérialiser par un label *ad hoc*.

Le *second niveau* de labellisation présente les caractéristiques suivantes : d'une part, un tiers intervient pour la rédaction des critères ou, à tout le moins, pour revoir et avaliser un projet proposé par le candidat à la labellisation ; d'autre part, les critères sont affichés sur le site du candidat ou accessibles sur le site du tiers par un hyperlien. Une nouvelle fois, il faut noter que le renvoi à ces critères peut impliquer l'affichage du label du tiers (en plus éventuellement du label *ad hoc* du candidat).

Enfin, le *troisième niveau* de labellisation présente les caractéristiques du niveau 2, auxquelles il faut ajouter une autre caractéristique : la mise en place d'un mécanisme de *réception* des plaintes et de *traitement* de celles-ci par le déclenchement d'un contrôle du respect des critères par le site, suivi si nécessaire de sanctions.

2.3. La labellisation externe

28. Rappelons que la labellisation externe suppose un *contrôle a priori* par un tiers du respect des critères. Suite à ce contrôle, dont dépendra 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 envisager deux niveaux.

Le *quatrième niveau* de labellisation présente les caractéristiques suivantes : d'une part, les critères sont déterminés par le candidat à la labellisation sans intervention d'un tiers ; d'autre part, ceux-ci sont affichés sur le site du candidat à la labellisation ; ensuite, un tiers intervient préalablement et périodiquement[19] pour vérifier la conformité du site par rapport aux critères[20]. Cette vérification aboutira généralement à la rédaction d'un rapport qui pourra également être affiché sur le site. Enfin, et de manière optionnelle[21], il est possible de sécuriser l'identification et/ou l'intégrité de la page des critères, de la page du rapport et, le cas échéant, du label.

Le *cinquième niveau* de labellisation présente les caractéristiques relevées au niveau 4, avec toutefois la différence fondamentale que les critères ne sont plus déterminés par le candidat à la labellisation, mais par

19 Cette intervention se fait soit d'initiative et régulièrement, soit sur la base d'une plainte.

20 Rappelons toutefois que le tiers ne vérifie ni le contenu ni la qualité des critères.

21 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 soi un critère susceptible de distinguer un niveau d'un autre.

un tiers qui intervient pour la rédaction des critères ou, à tout le moins, pour la révision et l'aval du projet proposé par le candidat à la labellisation.

3. L'intervention d'un tiers dans le processus de labellisation

29. On a vu que dans les différentes formes de labellisation, un tiers pouvait intervenir à plusieurs niveaux. D'une part, il peut jouer le rôle de rédacteur des critères auxquels le site candidat à la labellisation entend se conformer (rôle de rédacteur). D'autre part, il peut effectuer le contrôle de conformité de ces critères par le site (rôle d'audit). Ensuite, un tiers peut être amené à gérer et certifier l'éventuel label délivré par le « labellisateur » au site labellisé (rôle de certificateur). Dans le même ordre d'idée, un tiers peut offrir des produits informatiques dans le but de sécuriser l'un ou l'autre élément de la labellisation (rôle de sécurisation). Enfin, un tiers peut également intervenir en vue d'apaiser ou d'apporter une solution rapide et efficace à un conflit dans le cadre d'un système alternatif de résolution des litiges (rôle de résolution des litiges)[22]. Ces différents rôles ne se retrouvent pas nécessairement dans toutes les formes de labellisation et sont généralement réalisés par des tiers distincts. Toutefois, ils poursuivent tous un objectif commun : renforcer la confiance de l'utilisateur dans l'initiative de labellisation grâce à une sécurisation et une crédibilité accrues résultant de l'intervention de ce(s) tiers. Leur intervention ne produira toutefois réellement ses effets que si elle se réalise dans le respect de certaines conditions.

3.1. Un tiers pour la rédaction des critères

30. Par définition, la labellisation s'entend comme l'initiative de marquer ses propres services d'un niveau de qualité par un engagement à respecter certains critères. Dans ce cadre, il convient de déterminer les critères que le site entend respecter. Pour ce faire, un recours à un tiers peut être envisagé. L'intervention d'un tiers 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.

Pour que l'intervention d'un tiers soit efficace et reconnue comme crédible aux yeux du public, il faut que ce tiers présente les caractéristiques suivantes. D'une part, il doit être indépendant du candidat afin d'accomplir sa mission en toute objectivité, et être reconnu par le public en cette qualité. D'autre part, il doit disposer des compétences appropriées (c'est-à-dire une bonne connaissance des législations concernées et des aspects techniques ainsi que des besoins réels des utilisateurs d'Internet) et, idéalement, d'une expérience dans le domaine afin de proposer une solution suffisamment

22 Voir *infra* Partie 3.

protectrice des intérêts des utilisateurs (et des consommateurs en particulier) sans toutefois que cette solution se situe en marge de la réalité du marché. Enfin, le tiers doit, dans la mesure du possible s'adjoindre la participation d'associations concernées (consommateurs, utilisateurs d'Internet, *etc*.) pour la rédaction des critères.

Quant au contenu des critères, limitons-nous à dire que ceux-ci devraient prendre en compte le respect de certaines législations (telles que les directives européennes relatives aux contrats à distance et à la protection des données personnelles), idéalement d'une manière 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 candidat 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 », offrir une aide à la navigation, mettre en place un mécanisme de réception et de traitement des plaintes, *etc*.).

On pourrait objecter qu'il est inutile de déclarer que l'on respecte l'une ou l'autre législation dans la mesure où celles-ci sont impératives et doivent de toute manière être respectées. Notons néanmoins que cela joue un rôle pédagogique indéniable : le fait de déclarer que l'on respecte les dispositions de 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), dont il ignore peut-être l'existence.

3.2. Un tiers pour l'audit du site candidat à la labellisation

31. On a vu que pour la labellisation externe (niveaux 4 et 5), un organisme tiers indépendant intervient afin de contrôler préalablement et périodiquement le respect effectif par le site web d'un ensemble de critères prédéfinis. Le résultat de ce contrôle peut s'exprimer par l'affichage du rapport effectué par le vérificateur indépendant et/ou d'un label.

Le contrôle effectué par le tiers se concrétise à un double niveau. D'une part, un *contrôle a priori* qui permettra au tiers de se familiariser avec les critères établis par le candidat ou un autre tiers et d'effectuer une première évaluation[23]. D'autre part, un *contrôle a posteriori*, selon une

23 Ce contrôle *a priori* débouchera sur la rédaction d'un rapport destiné à être porté à la connaissance du public, qui attestera du respect des critères par le candidat. On renverra généralement à ce rapport grâce au label.

périodicité à déterminer en accord entre le tiers et le candidat, pour vérifier que le candidat continue à appliquer correctement les critères.

Ce tiers doit idéalement présenter les mêmes caractéristiques que celles qui ont été évoquées dans le point précédent. On peut toutefois ajouter que dans le cadre du contrôle de la conformité aux critères, il est important que le tiers dispose d'une compétence d'audit, puisque le contrôle du respect des critères s'apparente fortement à l'audit d'une société[24].

La combinaison de ces différentes qualités renforce indéniablement la crédibilité de l'initiative et est de nature à prévenir la survenance de certains litiges, et ainsi à accroître la sécurité juridique.

3.3. Un tiers pour la certification

33. Dans certains cas, il est fait appel à un tiers certificateur afin de certifier le label délivré par le tiers labellisateur et ainsi permettre aux visiteurs d'un site labellisé de vérifier l'authenticité de celui-ci. Il s'agit donc de l'adjonction d'un mécanisme technique visant à sécuriser un élément primordial de l'initiative de labellisation, qui renforce une nouvelle fois la crédibilité de cette dernière.

Plus concrètement, avant d'afficher le label, il est parfois nécessaire que le candidat à la labellisation demande et obtienne un certificat spécifique d'un tiers certificateur. Si le candidat reçoit un rapport sans réserve de l'auditeur, celui-ci avise le tiers certificateur 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 tiers certificateur fournit un *applet* (mini-application informatique utilisée sur le Web*)* au candidat. *L'applet* indique à la page Web de communiquer avec le tiers certificateur et, si l'autorisation a été accordée, d'afficher le label et les liens hypertextes associés au rapport de l'auditeur et à toute autre information pertinente.

Pour vérifier l'authenticité d'un label affiché sur 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 spécifique attribué par le tiers certificateur. Ce certificat numérique fournit au client une preuve de la validité du label. Il indique que le label ainsi que le certificat ont été délivrés par le tiers de confiance en question, que le label a été délivré à la suite d'une vérification par l'auditeur, à qui le certificat et le label ont été délivrés, et comment entrer

---

24 Rappelons que les qualités professionnelles d'un auditeur sont l'indépendance, l'intégrité, la discrétion et l'objectivité. De plus, celui-ci se conforme généralement à un ensemble complet de règles de déontologie et de normes professionnelles dans la prestation de ses services.

en communication avec l'entreprise à qui le certificat et le label ont été accordés.

Il est important de préciser qu'en l'absence de ce certificat numérique, le label ne doit pas être considéré comme valide. Cela permet ainsi de prévenir tout risque d'usurpation du label ou autres abus mais également de confirmer qu'un auditeur a effectivement exécuté sa tâche de contrôle du respect des critères par le site.

Le tiers certificateur n'intervient donc pas ici pour certifier l'identité d'une personne, qui utilise ce certificat dans le cadre de la signature d'un acte juridique, mais pour attester que le site Web existe, a effectivement été audité et a obtenu le label. Les enjeux sont donc quelque peu différents. On peut toutefois s'interroger sur l'applicabilité des dispositions contenues dans la proposition de directive sur la signature électronique pour ce nouveau type de certification.

3.4. Un tiers pour la sécurisation des éléments de la labellisation

33. Spécialement pour la labellisation externe (niveaux 4 et 5), il est possible de renforcer la crédibilité de l'initiative de labellisation en sécurisant certains éléments, tels que la page sur laquelle les critères prédéfinis sont affichés, la page sur laquelle le rapport de l'auditeur est hébergé, ou encore le label.

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

Différents niveaux de sécurisation sont envisageables, et impliquent généralement l'intervention d'un tiers. Sans entrer dans une analyse technique, limitons nous à dire qu'il existe plusieurs méthodes de protection. D'une part, il est possible de protéger la liste des critères ainsi que le rapport de l'auditeur en les affichant sur des pages sécurisées et en les hébergeant sur le serveur d'un tiers (le labellisateur par exemple). D'autre part, on peut, comme évoqué précédemment, vérifier l'authenticité d'un label en associant celui-ci à un certificat délivré par un tiers de confiance. Ensuite l'entité qui octroie le label peut répertorier dans une base de données sécurisée, accessible grâce à un moteur de recherche, l'ensemble des entreprises auxquelles elle a attribué le label. Toute entreprise absente de ces fichiers doit être considérée comme non labellisée. Enfin, on peut mettre en place des moteurs de recherches qui « traquent » les fraudeurs ayant usurpé le label.

3.5. Un tiers pour la résolution des litiges

34. L'engagement par un site labellisé de se soumettre à un mode alternatif de résolution des litiges[25] (ARL) démontre un état d'esprit positif de la part du candidat, qui est de nature à renforcer la confiance des internautes. Il est donc judicieux de faire de l'obligation de se soumettre à un ARL une condition d'octroi d'un label.

L'ARL suppose l'intervention d'un organisme tiers chargé de traiter en toute objectivité et indépendance la contestation. Le candidat s'engage alors à essayer de trouver une solution à l'amiable, voire à se soumettre à la décision prise par cet organisme.

Le recours à l'ARL présente un avantage indéniable pour le site labellisé ainsi que pour l'internaute. En effet, en acceptant de se soumettre à un système d'ARL 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 candidat 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, ce qui incite les utilisateurs à renoncer à agir en justice et ainsi à renoncer à leurs droits.

Toutefois, le recours à l'ARL ne peut se faire à n'importe quelle condition. Cette question est traitée dans le point suivant.

Réflexions

35. La labellisation des sites web se développe et apparaît comme une méthode qui permet de gagner la confiance des utilisateurs d'Internet. De surcroît, elle est envisagée par le législateur belge comme une technique présentant des garanties certaines dans la mesure où un site, parce qu'il est labellisé, peut être dispensé d'une interdiction légale (telle que celle relative à l'exigence d'un paiement avant la fin du délai de renonciation). Toutefois, un Arrêté Royal doit encore fixer les conditions relatives à cette labellisation.

En effet, tant le labellisateur, que les tiers qui l'aident dans sa tâche (rédacteur des critères, auditeur, certificateur, *etc*.), ne peuvent se permettre d'exercer leurs activités sans respecter certaines conditions essentielles. Ces dernières sont édictées afin d'offrir un service de qualité. Elles trouvent leur fondement dans le fait que le labellisateur, ainsi que les autres intervenants, doivent assumer la responsabilité de l'apparence de qualité et d'exactitude qu'ils créent au profit des utilisateurs. Il est par exemple inconcevable qu'une autorité de certification délivre un certificat à une

25 Voir le point suivant de cette contribution ainsi que l'article de V. TILMAN publié dans la *Revue Ubiquité*, « Arbitrage et nouvelles technologies : Alternative Cyberdispute Resolution », n° 2, p. 47.

personne physique sans vérifier sur base de documents probants l'identité de celle-ci. On n'imagine pas non plus qu'un « labellisateur » octroie un label vie privée par exemple à un site sans une analyse préalable et minutieuse du respect par ce site de la législation relative à la vie privée. Enfin, dans le cadre de l'ARL, on ne conçoit pas qu'un arbitre remette une décision en dépit du respect des principes de bonne justice, tel que le principe d'indépendance. Dans ces différents cas, le « tiers de confiance » viderait ses obligations essentielles de tout contenu s'il venait à s'exonérer de ses responsabilités pour le produit qu'il délivre (certificat, label, *etc*.). Si certaines conditions essentielles ne sont pas respectées, la confiance affichée par ces tiers ne durerait qu'un temps et prendrait vite la forme d'une apparence trompeuse.

On le voit, un cadre juridique clair s'impose afin d'encadrer les activités des « tiers de confiance ». Celui-ci fixerait les conditions essentielles à respecter. Celles-ci doivent toutefois encore être précisées.

PARTIE 3. LES MODES ALTERNATIFS DE RÉSOLUTION DES LITIGES : APPLICATION À L'ENVIRONNEMENT ÉLECTRONIQUE

36. Si le développement des nouvelles techniques de vente et de prestation de service favorise la multiplication des transactions de consommation, il augmente toutefois le risque de litiges transfrontaliers. Or, dans la plupart des conflits, qu'ils soient nationaux ou transfrontaliers, la valeur limitée de l'enjeu économique du litige rend la durée et le coût d'une procédure judiciaire disproportionné. De ce fait, nombre de consommateurs renoncent à faire valoir leurs droits. L'insécurité qui s'ensuit dans l'esprit des utilisateurs risque à terme de freiner le développement du commerce électronique.

Afin d'offrir une réponse rapide et peu coûteuse aux conflits nés dans l'environnement électronique, il apparaît que l'intervention d'un tiers par le biais d'un mode alternatif de résolution des litiges est de nature à renforcer la confiance des internautes et des professionnels du commerce électronique. La nécessité de pouvoir disposer d'un tel mode de résolution des litiges est également ressentie dans le cadre de la labellisation. Pour atteindre une efficacité réelle, celle-ci doit en effet proposer un mécanisme de réception et de traitement des plaintes liées au respect des engagements pris. Fondé sur la confiance, l'ARL se caractérise principalement par le consensualisme : les parties au litige décident librement de recourir à un mode de résolution autre que les procédures judiciaires devant les tribunaux, soit avant, soit au moment de la naissance du litige.

La présente partie fait tout d'abord état des initiatives européennes en matière de résolution alternative des litiges. Elle traite ensuite des deux voies principales de l'ARL (la médiation et l'arbitrage) en se fondant sur les initiatives existantes.

1. Initiatives européennes

37. La Commission européenne s'est penchée sur les solutions possibles pouvant répondre à la nécessité d'améliorer l'accès des consommateurs à la justice pour la défense de leurs droits. Il en est résulté une Communication sur « la résolution extrajudiciaire des conflits de consommation »[26]. Dans cette Communication, la Commission retient trois voies complémentaires possibles pour répondre aux problèmes soulevés :

1. la simplification et l'amélioration des procédures judiciaires
2. l'amélioration de la communication entre les professionnels et les consommateurs
3. les procédures extrajudiciaires de règlement des conflits de consommation.

Si la première voie se situe dans le cadre traditionnel de règlement des litiges, les deux dernières en revanche se situent en dehors du cadre judiciaire. C'est essentiellement sur celles-ci que la Commission se fonde pour lancer deux initiatives visant à remédier aux problèmes spécifiques résultant des litiges de consommation. La première a trait au lancement d'un formulaire européen de réclamation pour le consommateur. La seconde concerne l'adoption d'une recommandation établissant certains principes minimaux que les organes responsables pour la résolution extrajudiciaire des litiges de consommation devraient respecter.

Outre ces deux initiatives, la « Proposition de Directive relative à certains aspects juridiques du commerce électronique dans le Marché intérieur » aborde la question du règlement extrajudiciaire des différends en invitant les États membres à veiller à ce que leur législation permette l'utilisation effective de mécanismes de résolution extrajudiciaire des litiges.

1.1. Formulaire de réclamation du consommateur [27]

38. En ce qui concerne tout d'abord l'amélioration de la communication entre les consommateurs et les professionnels, la Commission souligne la nécessité d'aider le consommateur à trouver une solution à l'amiable de son différend avec le professionnel afin d'éviter les désagréments tels que

---

26 http://europa.eu.int/comm/dg24/policy/developments/acce_just/acce_just02_fr.html.

27 http://europa.eu.int/comm/dg24/policy/developments/acce_just/acce_just03_fr.html.

décrits ci-dessus, liés à l'ouverture d'une procédure. Dans ce contexte, la Communication propose un « formulaire européen de réclamation pour le consommateur » visant à améliorer le dialogue entre consommateurs et professionnels et, de ce fait, à faciliter le règlement à l'amiable des litiges pouvant survenir. Il s'agit d'un formulaire proposant un choix de réponses multiples pour aider le consommateur à mieux cerner ses problèmes tout en lui offrant la possibilité d'apporter des précisions complémentaires. La combinaison du système de choix multiples et de texte libre est destinée à faciliter la question de la traduction des demandes dans le cas de litiges transfrontaliers.

Ce formulaire peut donc être utilisé tant au niveau national que transfrontalier (pour autant que le litige se situe dans le cadre de l'Union européenne), quelle que soit la valeur en jeu ou le type de litige existant. Les choix offerts doivent permettre de couvrir la plupart des scénarios possibles en matière de litiges de consommation. Ce formulaire est à la disposition de toutes les personnes et organisations intéressées sur Internet dans 11 langues de l'Union européenne.

À défaut d'accord entre le consommateur et le professionnel, ce formulaire pourrait, le cas échéant, être utilisé pour ouvrir une procédure extrajudiciaire.

Cette initiative de la Commission est lancée à titre de projet pilote et devrait faire l'objet d'une évaluation dans un délai de deux ans.

1.2. Recommandation de la Commission concernant les principes applicables aux organes responsables pour la résolution extrajudiciaire des litiges de consommation [28]

40. Les procédures extrajudiciaires visées par la Recommandation sont celles qui se situent hors du cadre traditionnel de la résolution judiciaire des litiges et qui se caractérisent par l'interposition d'une tierce partie qui ne se borne pas à persuader les parties de s'entendre mais qui prend une position concrète sur la résolution du litige. Il va sans dire que ces procédures extrajudiciaires ne pourraient avoir comme objectif de remplacer le système judiciaire et, par conséquent, de priver le consommateur de son droit d'accès aux tribunaux.

Ce volet de l'action communautaire vise à « améliorer et à rendre plus transparentes et plus crédibles les procédures extrajudiciaires pour la résolution des litiges de consommation ». L'idée qui gouverne cette initiative est donc de fixer les principes minimaux devant gouverner les organes œuvrant dans le cadre de la résolution alternative des litiges.

---

28 http://europa.eu.int/comm/dg24/policy/developments/acce_just/acce_just01_fr.html.

Cette initiative est donc destinée à susciter la confiance. D'une part, celle des consommateurs, afin qu'ils soient rassurés quant aux garanties offertes par les procédures extrajudiciaires mises à leur disposition dans leur pays ou dans un autre État membre. D'autre part, celle des organes responsables de la résolution extrajudiciaire des conflits de consommation en cas de litiges transfrontaliers. Il est en effet essentiel que les organes extrajudiciaires puissent œuvrer en toute confiance afin que puisse être envisagée leur mise sur réseau et leur collaboration efficace en vue de la résolution de litiges internationaux.

Afin de parvenir à un niveau de transparence adéquat, la Commission demande aux États membres de lui communiquer le nom des organes responsables pour la résolution extrajudiciaire des litiges de consommation qu'ils considèrent conformes à la Recommandation. Sur la base de ces informations, la Commission est chargée de créer une base de données accessible à toute personne intéressée.

Parmi les principes que les organes extrajudiciaires sont appelés à respecter, on peut citer les suivants : principes d'indépendance, de transparence, du contradictoire, d'efficacité, de légalité, de liberté et de représentation.

Les personnes recourant aux organes repris dans la base de données dont il est question ci-dessus peuvent et doivent donc s'attendre à ce que ces organes respectent les principes fixés par la Recommandation.

1.3. Proposition de directive « commerce électronique »

40. La proposition de Directive « Commerce électronique » aborde, en son article 17, la question du règlement extrajudiciaire des différends. Cette disposition précise que les États membres doivent veiller à ce que « leur législation permette, en cas de conflits entre un prestataire et un destinataire d'un service de la société de l'information, l'utilisation effective de mécanismes de résolution extrajudiciaire, y compris par les voies électroniques appropriées ». Par le biais de cette disposition, la proposition de Directive prévoit donc une obligation pour les États membres de prévoir un recours effectif aux mécanismes de règlement extrajudiciaire des litiges, pour autant toutefois que ces mécanismes respectent les principes exprimés au paragraphe 2 de l'article 17. Ce paragraphe 2 doit être lu à la lumière des principes expliqués dans la Communication de la Commission dont question ci-dessus.

2. La mise en pratique de l'ARL

41. Actuellement, diverses initiatives de règlement en ligne des litiges sont opérationnelles, principalement aux États-Unis et au Canada. C'est le

cas de Virtual Magistrate, CyberTribunal et Online Ombuds Office[29]. L'Organisation Mondiale de la Propriété Intellectuelle (OMPI) propose également un mécanisme alternatif de résolution en ligne des litiges[30].

Ces initiatives sont toutes basées sur l'intervention d'un tiers dans la procédure de résolution, mais à différents degrés. D'une part, le tiers peut tout d'abord limiter son intervention à conseiller les parties sans imposer de solution : c'est le propre de la procédure de *médiation* telle qu'elle est prévue par le CyberTribunal, l'Online Ombuds Office. D'autre part, le tiers peut aussi imposer une décision aux parties dans le cadre de la procédure *d'arbitrage* : c'est le cas du CyberTribunal (qui propose les deux formes de résolution), de Virtual Magistrate et de la procédure mise en place par l'OMPI pour les litiges liés à la propriété intellectuelle et aux noms de domaine de l'OMPI.

2.1. L'intervention d'un tiers en qualité de médiateur

42. Dans le cadre de la médiation, les parties choisissent librement de soumettre leur différend à un tiers neutre, le médiateur. Ce dernier a pour mission d'établir une communication entre les parties et de proposer une solution de compromis. Il ne dispose toutefois pas du pouvoir d'imposer une décision. Comme toute procédure de résolution alternative, les parties ont la possibilité de se retirer à tout moment de la procédure et de soumettre leur litige aux tribunaux.

La médiation se définit comme l'analyse du litige par le médiateur sans que celui-ci n'impose de décision. Les parties se trouvent dans la position de négocier avec l'aide du médiateur afin de parvenir à une solution adaptée à leur litige.

43. Le CyberTribunal - Le projet de CyberTribunal a été développé au Canada en 1996 par l'Université de Montréal. Il s'adresse à tout internaute, qu'il soit professionnel ou consommateur, confronté à un conflit lié au droit des nouvelles technologies, à savoir : le commerce électronique, la concurrence, les droits d'auteur, les marques de commerce, la liberté d'expression, la vie privée, etc. Le CyberTribunal ne tranche toutefois pas les questions d'ordre public. Actuellement, le CyberTribunal propose ses services gratuitement, en français et en anglais, et envisage de les proposer prochainement en espagnol.

Les tiers sélectionnés par le CyberTribunal pour agir en qualité de médiateur sont des spécialistes des nouvelles technologies de l'information

---

29 http://vmag.vcil.org/.
http://www.cybertribunal.org.
http://aaron.sbs.umass.edu/center/ombuds/default.htm.

30 http://www.arbiter.wipo.int/ ; http://internetone.wipo.int/.

et de la communication, ils peuvent être juristes ou non juristes, et sont choisis au Canada comme à l'étranger.

Le choix d'un site marchand — c'est-à-dire d'un site qui offre des produits, services ou licences sur Internet — de participer au mécanisme de résolution des litiges proposé par le CyberTribunal se matérialise par l'apposition d'un sceau[31] qui vise à informer les visiteurs de l'engagement du site à soumettre un différend au CyberTribunal plutôt qu'aux tribunaux. Une clause *ad hoc* est prévue pour informer les visiteurs et les inviter à se rendre sur le site du CyberTribunal.

Préalablement à l'affichage du sceau, le CyberTribunal informe les sites de l'existence d'un code de conduite qui énonce les règles minimales en matière de pratiques commerciales sur Internet. Le code comprend des engagements relatifs aux informations, au spamming, à la protection de la vie privée, aux cookies, à la gestion des liens hypertextes, à la fonction « back », à la sécurité relative aux paiements et au service à la clientèle. Le respect de ce code par le site n'est toutefois pas exigé pour participer à la procédure de médiation, le CyberTribunal ne procède pas à un contrôle *a priori*.

La procédure est déclenchée par une manifestation expresse des deux parties de soumettre le différend au secrétariat du CyberTribunal : cette manifestation peut intervenir avant ou après la naissance du conflit. Le secrétariat[32] reçoit des parties un formulaire de demande, il statue sur la recevabilité de la demande et, le cas échéant, procède à la désignation d'un médiateur. La procédure s'articule autour d'un *site de l'affaire* par lequel les informations sont échangées entre les parties et le médiateur. À ce sujet, une grande liberté est laissée au médiateur pour le déroulement de la procédure afin de favoriser la souplesse de la médiation. Le site de l'affaire est sécurisé par *VeriSign* qui garantit la confidentialité des informations échangées.

Le CyberTribunal intervient pour sanctionner le site et lui retirer le sceau dans le cas où ce dernier refuserait de se soumettre à une procédure de médiation ou arbitrage alors que le secrétariat a déclaré recevable la demande.

L'OnLine Ombuds Office - OnLine Ombuds Office a été créé en juin 1996 par le « Centre for Information Technology and Dispute Resolution » de l'Université du Massachusetts aux États-Unis. OnLine Ombuds Office offre un service de médiation pour les parties qui souhaitent résoudre leurs litiges en ligne, notamment : la participation à des newsgroups, l'attribution des noms de domaine, la concurrence déloyale, le spamming, la propriété

31 L'apposition de ce sceau rejoint la technique de la labellisation telle que décrite dans la partie 2.

32 Le secrétariat désigne le greffe du CyberTribunal : il est composé d'un secrétaire, d'un greffier et d'un greffier adjoint.

intellectuelle, les relations avec le fournisseur d'accès. Les services sont offerts gratuitement.

Outre la procédure de médiation, l'OnLine Ombuds Office propose un service d'information relatif à la résolution en ligne des litiges : ces informations sur les précédents déjà résolus peuvent aider certaines parties à régler elles-mêmes leur litige. Lorsque l'assistance d'un médiateur — appelé ombudsman — est requise par les parties, celui-ci intervient pour favoriser le dialogue entre les parties et assister ces dernières à régler leur différend. Le rôle de l'ombudsman inclut la fourniture et la réception d'informations, la présentation de cas comparables, le recentrage du problème, le développement d'options.

En cas de survenance d'un litige, l'une des parties remplit un formulaire de requête de médiation et l'envoie à l'ombudsman. Ce dernier demandera toutes les informations nécessaires et contactera l'autre partie au litige. Le déroulement de la procédure est conditionné par l'acceptation de cette autre partie qui n'a pas pris l'initiative de contacter l'ombudsman : ce dernier ne peut en effet intervenir que si les deux parties au litige acceptent de soumettre le litige à la procédure de l'OnLine Ombuds Office. Si l'une des parties refuse de coopérer, la médiation ne sera pas possible.

Si la procédure est engagée, les échanges entre les parties et l'ombudsman se feront principalement par courrier électronique. Un logiciel de vidéoconférence est parfois utilisé, tout comme le recours au téléphone et au courrier postal. Le Centre s'attache à garder confidentielles les informations échangées grâce à des logiciels de cryptage.

44. — *Appréciation* **—** L'intervention d'un tiers est ici limitée à l'assistance des parties confrontées à un litige. Malgré l'absence de décision contraignante, le rôle du tiers est décisif puisque, à la demande conjointe des parties, il dialogue avec elles afin de parvenir à une solution qui les satisfasse. Le véritable intérêt de la procédure réside dans le fait que les échanges entre les parties et le médiateur ont lieu en ligne — soit par le biais d'un *site de l'affaire*, comme c'est le cas pour le CyberTribunal, soit par le biais de *courriers électroniques* dans la procédure de l'OnLine Ombuds Office — avec une interactivité qui permet une réponse quasi immédiate aux demandes. Les internautes trouvent un intérêt certain dans cette procédure : en cas de litige, ils ont l'assurance de pouvoir bénéficier – gratuitement de surcroît avec le CyberTribunal et l'OnLine Ombuds Office – des conseils d'un professionnel avisé, sans se déplacer. Une telle procédure est également bénéfique pour les responsables de sites qui, outre l'avantage commercial indéniable lié à l'apposition d'un sceau tel que celui du CyberTribunal, ont intérêt à ce que les litiges éventuels avec leurs clients se résolvent rapidement et dans une certaine confidentialité. Les solutions apportées pour les litiges pourront par ailleurs aider le

responsable du site à améliorer ses pratiques afin de limiter les sources de conflits.

3.2. L'intervention d'un tiers en qualité d'arbitre

45. Une procédure d'arbitrage ne peut avoir lieu qu'à la demande des parties. Toutefois, à la différence de la médiation, elle implique que le tiers qui intervient en qualité d'arbitre impose une solution contraignante aux parties. En acceptant cette procédure, les parties sont certaines de parvenir à une solution qui s'imposera à elles.

46. — *Le Virtual Magistrate* [33]— Le Virtual Magistrate Project (ci-après VMP) vise à instaurer un mode de règlement alternatif des litiges à la fois rapide, peu coûteux et adapté aux nouveaux types de litiges liés à l'utilisation des nouvelles technologies. Le projet a été développé aux États-Unis en 1995 par un groupe de travail composé du *Cyberspace Law Institute*, de *l'American Arbitration Association*, du *Centre for Information Law and Policy* et du *National Centre for Automated Information Research*.

Le VMP offre un arbitrage en ligne pour les plaintes relatives aux infractions au droit d'auteur ou au droit des marques, à l'appropriation illicite de secrets commerciaux, à la diffamation, à la fraude, aux pratiques commerciales déloyales, aux contenus illicites, à la violation de la vie privée, et à tout autre contenu dommageable.

La procédure est ouverte à toute personne, quelle que soit sa situation géographique, à condition que les parties en cause acceptent de participer. La procédure s'ouvre par le dépôt d'une plainte qui peut se faire soit par l'envoi d'un courrier électronique, soit en remplissant un formulaire spécial sur le site du Virtual Magistrate. Si la plainte est déclarée recevable, un arbitre est désigné par *l'American Arbitration Association*. L'arbitre — dans ce cas le *Magistrate* — crée alors un alias qui reproduit les coordonnées électroniques de chaque partie concernée par l'affaire. Un mot de passe est envoyé aux parties afin qu'elles accèdent à l'alias et qu'elles puissent lire les messages envoyés. Les parties ont également la possibilité de communiquer individuellement avec le *Magistrate* par le biais de son adresse personnelle.

Le *Magistrate* dispose des compétences suivantes : il conduit les débats, il peut contacter les parties et leur demander de répondre à des questions, il collecte des informations et prend toute mesure qu'il estime nécessaire. Il conserve une copie de tous les documents qui sont échangés. Pour rendre sa décision, le *Magistrate* dispose d'un délai de 72 heures (trois jours ouvrables) à compter de l'acceptation de chaque partie

33 Le site *Virtual Magistrate* n'est plus actif actuellement. Il est néanmoins décrit à titre illustratif.

concernée de participer à la procédure. La décision est notifiée aux parties par courrier électronique. Les plaintes ainsi que la décision sont rendues publiques sauf en cas d'avis contraire.

47. —*Le CyberTribunal* — Outre la médiation, le CyberTribunal propose également aux parties de résoudre leur conflit par la voie de l'arbitrage. La particularité de la procédure est que la décision rendue est contraignante pour les parties *sans possibilité d'appel*.

Le déclenchement de la procédure est le même que pour la médiation, à la différence que le tiers désigné agit en qualité d'arbitre et non de médiateur. Là aussi, le consentement explicite des parties au conflit est nécessaire pour que la procédure soit engagée. Contrairement à la médiation, l'arbitrage est organisé selon des règles prédéfinies, inspirées notamment des règles de procédure arbitrales de la CNUDCI et de la CCI[34].

48. —*L'OMPI* — Le *Centre d'arbitrage et de médiation* de l'OMPI est chargé de régler les litiges liés aux noms de domaine et à la propriété intellectuelle en général. Le Centre a récemment développé un arbitrage en ligne : un formulaire de plainte est accessible depuis le site du Centre. Les parties communiquent alors avec le Centre et l'arbitre par le biais de messages sécurisés. Même si les règles développées par l'OMPI concernant la médiation et l'arbitrage restent applicables, l'OMPI a développé des règles spécifiques qui tiennent compte du caractère interactif de la procédure, notamment le principe selon lequel l'audition des parties ne doit pas excéder trois jours, et la procédure dans son ensemble doit se clore endéans un délai de trois mois (délai qui est à mettre en comparaison avec le délai de neuf mois dans le cadre de l'arbitrage classique).

49. —*Appréciation* — La particularité de la procédure d'arbitrage se trouve transposée dans l'environnement électronique : dès lors que les parties acceptent de se soumettre à une procédure débouchant sur une décision contraignante, elles ont la certitude que leur litige trouvera une issue dans le cadre d'une procédure rapide et adaptée.

L'intervention du tiers est donc décisive puisqu'elle règle le sort des parties. Elle est également avantageuse en termes de temps puisque, notamment dans le cadre du projet Virtual Magistrate, la décision de l'arbitre doit être rendue dans un délai de trois jours.

Toutefois, l'arbitrage en ligne ne rencontre pas le succès auquel on pourrait légitimement s'attendre. Peu de parties sont en effet enclines à se soumettre à une procédure alternative impliquant une décision contraignante. La pratique du Virtual Magistrate et du CyberTribunal le montre : alors que le premier révèle une faible activité réellement inquiétante, le second n'a traité à l'heure actuelle aucun cas d'arbitrage

34 CNUDCI : Commission des Nations Unies pour le Droit Commercial International ; CCI : Chambre de Commerce Internationale.

(contre une centaine d'affaires traitées dans le cadre de la médiation[35]). Les internautes ne sont sans doute pas encore prêts à soumettre leur litige à un arbitre, en lui déléguant par là même le pouvoir de décision.

3. Recommandations relatives à l'ARL

50. Eu égard à ses caractéristiques, l'intervention d'un tiers dans le cadre d'une procédure d'ARL est de nature à développer un contexte de confiance vis-à-vis des relations qui se nouent sur Internet. L'intervention du tiers médiateur ou arbitre permet de lever l'incertitude liée à la résolution d'un conflit sur le réseau. Il est donc souhaitable que des procédures d'ARL se généralisent afin de conforter les internautes dans l'idée qu'un litige né en ligne peut trouver une solution par le biais d'Internet, moyennant un investissement raisonnable en termes de temps et de coût.

Toutefois, il est nécessaire que cette généralisation des procédures d'ARL se fasse dans le respect de certaines conditions, afin de maximiser leurs chances de succès et leur acceptation par les internautes :

— il apparaît indispensable qu'une *information* complète soit fournie aux internautes sur le but poursuivi par l'ARL, les avantages dont ils peuvent bénéficier et la procédure à suivre. La différence entre les différentes formes de résolution et leurs conséquences doit aussi apparaître clairement : par exemple, les internautes doivent être conscients que la décision du tiers dans une procédure d'arbitrage s'imposera à eux ;

— les procédures d'ARL doivent permettre aux parties de se retirer à tout moment et de se tourner vers les tribunaux ;

— la qualité du tiers qui intervient dans la procédure est fondamentale : celui-ci doit être neutre par rapport aux parties et à l'enjeu du litige et il doit bénéficier d'une compétence particulière dans le domaine en cause ;

— dans le cadre de litiges impliquant des consommateurs, il est important que les règles de protection développées aux niveaux national et européen soient appliquées par le médiateur ou l'arbitre, afin de ne pas cautionner le développement de règles parallèles.

35 Chiffres de juillet 1999.

CONCLUSIONS

51. Le développement des communications sur Internet est de plus en plus conditionné par l'intervention d'un ou plusieurs tiers. Ces derniers peuvent intervenir dans le but soit d'émettre un certificat dans le cadre de l'utilisation de la signature électronique, soit d'effectuer le contrôle d'un site web et de lui délivrer, le cas échéant, un label prouvant que ce site respecte certaines exigences essentielles ou encore de proposer, une fois un litige né, une structure qui aidera les parties à aboutir rapidement à une solution satisfaisante. L'intervention de ces tiers se justifie par le caractère *a priori* non sécurisé de l'Internet. Celui-ci a suscité l'essor de nouveaux métiers, dont l'objectif premier est de mettre fin à l'insécurité propre aux réseaux ouverts en proposant un produit qui crée artificiellement (notamment par des mécanismes de sécurité informatique) un environnement sécurisé pour les transactions qui nécessitent ce contexte de confiance.

Toutefois, les tiers ne peuvent agir dans l'unique but de la recherche de profit. Leurs activités doivent être exercées dans le respect de certaines exigences minimales. Les tiers doivent offrir un produit répondant à l'attente légitime des utilisateurs[36]. En matière de certification électronique et de labellisation, cette attente légitime consiste à pouvoir disposer d'un produit informationnel dans lequel les données sont exactes, complètes et mises à jour, étant donné que ces tiers connaissent les conséquences que pourrait entraîner la publication d'informations inexactes, incomplètes ou obsolètes. Dans ce contexte, les clauses limitatives ou exonératoires de responsabilité doivent être appréciées de façon circonstanciée. Elles ne sont opposables aux personnes qui se fient légitimement aux certificats ou aux labels que si celles-ci en ont pris connaissances ou, à tout le moins, ont pu raisonnablement en prendre connaissance au plus tard au moment de la consultation du certificat ou du label. En toute hypothèse, elles ne pourraient vider l'objet de l'activité des tiers de confiance de son contenu. Seraient considérées comme telles les clauses par lesquelles un tiers de confiance refuserait d'engager sa responsabilité quant à la véracité des informations fournies. En matière d'ARL, l'attente légitime consiste à pouvoir se fonder sur un mécanisme de résolution des litiges à tout le moins respectueux des principes d'indépendance, de transparence et du contradictoire.

La confiance que les tiers peuvent susciter est conditionnée par les engagements qu'ils entendent assumer. Elle apparaît aujourd'hui comme le gage de réussite du commerce électronique.

---

36 À ce sujet, E. MONTERO, *La responsabilité civile du fait des bases de données*, Travaux de la Faculté de Droit de Namur, P.U.N., 1998.