Vers la confiance ou comment assurer le développement du commerce électronique

Antoine, Mireille; Poullet, Yves

Published in:
Authenticité et Informatique

Publication date:
2000

Document Version
le PDF de l'éditeur

« VERS LA CONFIANCE » (1) OU COMMENT ASSURER LE DÉVELOPPEMENT DU COMMERCE ÉLECTRONIQUE

YVES POULLET (*)

PROFESSEUR AU FUNDP ET À L'UL.G.
DIRECTEUR DU CRID-FUNDP

MIREILLE ANTOINE (**)

DIRECTEUR DE RECHERCHES AU CRID-FUNDP (***)

Sommaire

(*) yves.poullet@fundp.ac.be

(**) mireille.antoine@fundp.ac.be

(***) http://www.droit.fundp.ac.be/crid.htm

(1) Nous reprenons ici le titre de l'atelier @gora 98 présidé par l'auteur du rapport à la demande du Ministre des Affaires économiques du précédent gouvernement. Ce rapport a été présenté lors de la conférence de clôture des ateliers consommateurs. Le rapport de l'atelier : Commerce électronique : Vers la confiance! présenté par Y. POULLET et J. ROYEN est disponible sur le site : http://www.agora98.org/fr./conso/fconso.htm. La « confiance » est également le thème de la Communication de la Commission européenne au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions (Assurer la sécurité et la confiance dans la communication électronique : vers un cadre européen pour les signatures numériques et le chiffrement, COM(97)503 final, 1997).

1. – Sans doute, mesure-t-on encore peu aujourd'hui les possibilités du commerce virtuel. L'adoption de standards communs, l'interopérabilité des réseaux à l'échelle de la planète et la digitalisation des sons, écrits et images augurent pour le commerce électronique des lendemains prometteurs tant pour les entreprises, les administrations que les personnes privées.

Cependant la dimension globale de ce dit commerce nécessite comme préalable à son développement un contexte de confiance qu'assuraient, spontanément, jusqu'ici les limites étroites des villages réels. L'entrée dans un monde virtuel et global, pire l'immatérialité et la fugacité des messages qui s'y échangent, accroissent le sentiment d'insécurité pour celui qui veut contracter et représentent un véritable défi pour la technique et le droit.

Ainsi surfant sur Internet, comment être sûr de l'identité de l'interlocuteur qui vous promet mille bonheurs, lorsque pour toute identification, vous ne disposez que d'une adresse e-mail ou du nom de domaine du site Web ? A cette insécurité de l'identité du vis-à-vis, s'ajoutent celles de la qualité du message ou de la promesse qu'il vous adresse et que vous recevez.

Venant de nulle part, ce message qui s'affiche à votre écran constitue-t-il un acte sous seing privé au sens du Code civil ? Emane-t-il bien de celui que très sommairement vous venez d'identifier ? Est-ce une copie fidèle de celui qui a été envoyé ? Quand a-t-il été envoyé ? Et votre interlocuteur de se demander : a-t-il été bien reçu ? Quand a-t-il été reçu ? N'a-t-il point été modifié, chemin faisant ?

Votre angoisse s'accroît encore lorsque vous vous interrogez sur la qualité de votre interlocuteur. Est-il réellement celui qu'il prétend être : agent de change, médecin... ? Est-il capable juridiquement parlant ?

Quant aux règles qui entourent les opérations qu'ils vous proposent, respectent-elles les impératifs légaux ou non de la sécurité, de la confidentialité des messages, de la protection des données voire celle du consommateur ?

2. – Notre propos est d'analyser les réponses que progressivement le droit – au sens le plus large et non entendu au sens strict, c'est à dire comme les seules réglementations étatiques (2) – peut apporter à toutes ces interrogations. Le droit entend d'abord approfondir les concepts traditionnels qui forment les piliers du droit de la preuve des actes juridiques. Nous reviendrons dans le titre I sur la signification qu'il convient désormais de conférer aux notions d'« acte », de « signature » et d'« écrit » dans un environnement désormais digitalisé. Mais au-delà, le droit progressivement – et la technique tantôt l'impose, tantôt y invite – reconnaît l'intervention de nouveaux acteurs afin de renforcer cette confiance. Dans un article récent, Mireille Antoine, Didier Gobert et Anne Salaün (3) parlaient à ce propos des nouveaux « métiers de la confiance ». Si la confiance en effet ne peut naître de la seule activité des interlocuteurs finaux, désespérément trop virtuels, sans douter faudra-t-il s'en remettre à l'intervention de « tiers » indépendants dont l'activité sera précisément de créer, de manière originale, les éléments de la confiance et de la sécurité. Le titre II leur est consacré.

Sans doute, ces tiers, sont-ils multiples. On ne garantit pas l'identité d'un interlocuteur, comme son respect de tel ou tel

(2) L'autorégulation est également source de normativité dans le commerce électronique. Sur cette autorégulation, sa valeur et ses limites, lire Y. POULLET, « Les diverses techniques de réglementation d'Internet : l'autorégulation et le contrôle du droit étatique », *Ubiquité*, n° 5, à paraître en juin 2000.

(3) M. ANTOINE, D. GOBERT, A. SALAÜN, « Le développement du commerce électronique : les nouveaux métiers de la confiance », in *Droit des technologies de l'information, regards prospectifs*, Cahiers du C.R.I.D., n° 16, pp. 3 à 32.

prescrit. On n'atteste pas de l'arrivée d'un message comme de la capacité de son émetteur. Il sera utile, à propos de ces divers « objets » à garantir, d'identifier les réponses déjà données par le Droit et d'en suggérer de futures en ce qui concerne les lacunes contestées. A cet égard, on relèvera que la réponse du Droit reste encore largement lacunaire. On note que le 13 décembre 1999, les instances européennes adoptaient la directive « sur un cadre commun pour les signatures électroniques » (4), et que cette reconnaissance de la signature électronique fait l'objet en Belgique de deux projets de loi : l'un introduit par le précédent gouvernement et non relevé de caducité réformait le Code civil et introduisait une définition de la signature incluant celle électronique (5); l'autre, plus technique, « relatif à l'activité des prestataires de services de certification en vue de l'utilisation de signatures électroniques », a été déposé à la Chambre des Représentants le 16 décembre 1999 (6). De telles initiatives, décrites au point I de ce second titre, à supposer même qu'elles aboutissent en ce qui concerne notre pays, permettront de régler les questions, essentielles certes, de l'identité du contractant et de l'intégrité du message. Mais au-delà, bien des chantiers restent à ouvrir pour sécuriser totalement le commerce électronique. Ce sera l'objet du point II.

(4) Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *J.O.C.E.*, L 13 du 19 janvier 2000, pp. 12 à 20.

(5) Projet de loi visant à modifier certaines dispositions du Code civil relatives à la preuve des obligations, *Doc. Parl.*, Ch. des Repr, sess.ord., 14 avril 1999, n° 2141/1. Le présent article n'a pu tenir compte des modifications de ce projet introduite au delà du 1er mai, ni des discutions parlementaires ou gouvernementales à son sujet.

(6) Projet de loi relatif à l'activité des prestataires de service de certification en vue de l'utilisation de signatures électroniques. Chambre des représentants, DOC, 50 0322/001 du 16 décembre 1999. Le présent article n'a pu tenir compte des modifications de ces projets introduites au delà du 1er mai 2000, ni des discutions parlementaires ou gouvernementales à son sujet.

TITRE 1. – LES CONCEPTS DE BASE DU DROIT DE LA PREUVE À L'ÉPREUVE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

I. – *Où il est question de l'acte en tant que notion première*

3. – Trois concepts dominent le droit de la preuve : les notions d'acte, de signature et d'écrit apparaissent intimement liées même si l'analyse de chacune d'elles révèle qu'elles puissent être parfois dissociées. Sans doute, la notion d'acte est-elle première dans la mesure où sa compréhension se réfère à la fois à un élément intentionnel et à un élément matériel. L'acte, qu'il soit authentique ou seing privé, constitue en effet le concept clé en droit de la preuve. La notion d'acte revêt deux significations intimement liées. Il est avant tout le fruit de la volonté d'une personne de s'engager juridiquement (*negotium*). L'écrit signé constitue également l'« acte », la trace « tangible » de cet engagement spécifique (*instrumentum*). Dressé par un officier public selon certaines formes, l'acte se verra hissé au rang d'« acte authentique » bénéficiant d'une force probatoire spécifique (7).

L'acte, résultant de la combinaison de l'écrit et de la signature, transcende donc ces concepts pour se voir reconnaître une valeur juridique propre.

4. – Le concept d'acte s'articule autour des notions d'imputabilité et de fiabilité. L'imputabilité suppose l'appropriation du contenu de l'écrit et l'identification de la personne « appropriante ». Cette fonction est traditionnellement assurée par la signature. La fiabilité, quant à elle, constitue la qualité intrinsèque que doit revêtir l'écrit. La volonté de la personne « appropriante », pour reprendre le terme employé ci-dessus, s'exprime par rapport à un contenu spécifique. Il faut donc que soit assurée l'inaltérabilité de l'écrit matérialisant le contenu de l'engagement, sa lisibilité et enfin sa stabilité (8).

(7) Le lecteur voudra bien sur ce point se référer au rapport de maître J-L. SNYERS qui aborde le point de vue notarial relatif aux questions que nous traitons ici.

(8) Voir *infra*, n° 14.

Eu égard aux développements techniques récents, il apparaît que l'inaltérabilité est de plus en plus assurée par les nouvelles techniques de signatures. Celles-ci, outre les fonctions d'identification et de manifestation de consentement, sont appelées à assurer une troisième fonction autrefois dévolue au support papier : l'intégrité de l'écrit. Nous reviendrons sur cette question par la suite.

Il existe toutefois des hypothèses où l'imputabilité d'un acte n'est pas correctement assurée à défaut de signature. L'article 1347 du Code civil relatif au commencement de preuve par écrit fait écho à cette problématique en fixant les conditions pour qu'un acte, bien que non signé, puisse toutefois être pris en considération. Constitue un commencement de preuve par écrit « tout acte écrit qui est émané de celui contre qui la demande est formée, ou de celui qu'il représente, et qui rend vraisemblable le fait allégué ». L'article 1347 impose donc une imputabilité « raisonnable » de l'écrit à celui auquel on l'oppose, l'écrit devant par ailleurs rendre vraisemblable le fait allégué, et non pas seulement possible. On ajoute que la notion d'écrit utilisée par cet article a été interprétée de manière très large et désigne tout support y compris audio ou visuel (9) et non les seuls supports texte.

II. – *La signature : un concept à large spectre enfin défini*

§ 1er. – *La signature électronique : description technique*

5. – Il existe une multitude de techniques baptisées « signatures électroniques », dès lors qu'elles permettent, à elles seules ou en combinaison, de réaliser les fonctions dévolues à la signature (10). Cependant, toutes ne présentent pas nécessairement un niveau de sécurité acceptable sur le plan juridique. Parmi toutes ces techniques, seule la technique de la signature digitale, fondée sur la cryptographie asymétrique, constitue la technique de signature qui est la plus répandue et offre pour le moment (11) les meilleures garanties de sécurité. Une explication s'impose (12).

La signature digitale est fondée sur la cryptographie asymétrique, dite « à clé publique ». Dans un système à clé publique, la réalisation de la fonction d'identification suppose qu'une personne dispose de deux clés mathématiques complémentaires : une clé privée, dont le caractère secret doit effectivement être préservé, et une clé publique, qui peut être librement distribuée. La clé publique est une fonction de la clé privée qui est telle qu'il doit être aisé de calculer la clé publique à partir de la clé privée et matériellement impossible de déduire de la clé publique la clé privée correspondante. La clé publique doit dès lors représenter une transformation irréversible de la clé privée. La clé privée permet de « signer » le message. L'opération de décodage s'effectue, quant à elle, selon le principe de la complémentarité des clés : un message encodé avec une clé privée ne peut être décodé qu'avec sa clé publique complémentaire. L'exemple suivant illustre le fonctionnement de la signature digitale (13).

Alice désire envoyer à Bernard un message informatisé signé de façon électronique. Après avoir écrit son message, Alice réalise un condensé de ce message au moyen d'une opération mathématique. Ce condensé est le résultat d'une fonction appelée fonction de hachage irréversible. Cette fonction per-

(9) Pour une analyse approfondie de cette question, voir J. SIMONS, « Photographie, cinéma et télévision : l'avenir de la preuve par l'image », *J.T.*, 1988, pp. 613 à 617.

(10) Pour une analyse approfondie des fonctions de la signature, voir D. GOBERT et E. MONTERO, « La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle », *DA/OR*, avril 2000, n° 53, pp. 17 à 39.

(11) Même si se développent d'autres procédés, ainsi ceux dits de signature biométrique (reconnaissance digitale de l'empreinte vocale ou de l'iris, etc.)

(12) Description de la signature digitale extraite de M. ANTOINE et D. GOBERT, « Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification », *R.G.D.C.*, 1998, n° 4/5, pp. 292 à 295. Voir également : S. PARISIEN et P. TRUDEL, *L'identification et la certification dans le commerce électronique*, Québec, Ed. Yvon Blais Inc., 1996, pp. 93 à 113; J. HUBIN, *La sécurité informatique, entre technique et droit*, Cahiers du C.R.I.D., n° 14, 1998, spéc. pp. 68 à 112.

(13) Voir aussi le processus de création d'une signature digitale dans E.A. CAPRIOLI, « Sécurité et confiance dans le commerce électronique : Signature numérique et autorité de certification », *La Semaine Juridique Edition générale*, avril 1998, n° 14, p. 588.

met de générer de façon concise une chaîne de données qui représente le message en question. Cette représentation est sécuritaire, très précise et permet de détecter tout changement apporté au message. En effet il suffit au destinataire d'appliquer la fonction de hachage au message reçu et de comparer le condensé ainsi obtenu avec celui transmis par l'émetteur. Toute différence entre les condensés signifie que le message a été altéré en cours de transmission.

Ce condensé est par la suite encodé (rendu illisible et inaccessible) à l'aide de la clé privée d'Alice. Ce condensé encodé constitue la signature digitale. Alice envoie alors à Bernard son message (en clair) accompagné de la signature digitale.

Lorsque Bernard reçoit le message et la signature digitale, il décode cette dernière en effectuant une opération mathématique impliquant la clé publique complémentaire d'Alice. S'il parvient à décoder la signature, Bernard est assuré que celle-ci a préalablement été réalisée avec la clé privée complémentaire d'Alice : il sait alors de manière certaine qu'elle est l'auteur du message pour autant qu'une partie tierce (une autorité de certification) certifie que cette clé publique est bien celle d'Alice. Grâce à la fonction de hachage (14), l'intégrité du message d'Alice peut être garantie.

§ 2. – *La directive européenne*

6. – La directive européenne sur un cadre communautaire pour les signatures électroniques (15) vise à la reconnaissance légale des signatures électroniques. Diverses approches étaient possibles pour parvenir à une telle fin. Celle qui a été choisie par la directive se fonde sur une approche fonctionnelle de la

(14) Remarquons toutefois que la réalisation d'un condensé du message à l'aide de la fonction de hachage irréversible n'est pas indispensable. En effet l'émetteur du message pourrait directement encoder le message avec sa clé privée sans nécessairement passer par la production du condensé. Néanmoins, sauf pour garantir la confidentialité du message lui-même, la fonction de hachage irréversible partiel sera souvent utilisée dans un souci de gagner du temps : encoder avec la clé privée un condensé (fichier de petite taille) est plus rapide que l'encodage du message en clair (fichier de plus grosse taille).

(15) Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *op. cit.*

signature, rejoignant sur ce point la loi type sur le commerce électronique adoptée par la CNUDCI (16).

La directive définit la signature électronique comme étant « une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification » (art. 2.1.). Cette définition 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 signé. Cette définition reflète la volonté de la Commission de définir la signature électronique de façon telle à ce que soient prises en considération toutes les techniques particulières de signature électronique, dès lors qu'elles permettent, seules ou combinées entre elles, de réaliser, de manière plus ou moins parfaite selon la technique utilisée, les fonctions dévolues à la signature (17). La définition donnée de la notion de signature s'articule autour du concept d'« authentification ». L'interprétation qu'il convient d'en donner n'est pas claire : l'authentification peut porter tant sur l'origine des données que sur leur intégrité.

La directive opère une distinction entre le terme générique de « signature électronique » et une technique plus spécifique de signature électronique qu'elle qualifie de « signature électronique avancée » (art. 2.2.). Est considérée comme telle, la signature électronique qui satisfait aux exigences suivantes :

(16) La loi type de la CNUDCI sur le commerce électronique propose, en son article 7.1., les conditions générales dans lesquelles des messages de données devraient être considérés comme signés.

« Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données :

a) Si une méthode est utilisée pour identifier la personne en question et pour indiquer qu'elle approuve l'information contenue dans le message de données; et

b) Si la fiabilité de cette méthode est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière.

(17) Ainsi, le code secret à quatre chiffres utilisé pour des transactions bancaires à partir de guichets automatiques peut être qualifié au sens de la directive de signature électronique dans la mesure où le fonctionnement du réseau garantit que de telles données circulent de manière jointe avec les données de la transaction. Il va de soi que cette méthode d'authentification reste cependant faible et que l'intégrité du message joint est faiblement garantie.

a) être liée uniquement au signataire;
b) permettre d'identifier le signataire;
c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif; et
d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

En choisissant le terme « signature électronique avancée », la directive choisit la voie de la neutralité technologique afin, d'une part, d'éviter qu'elle 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 la cryptographie asymétrique (18) répond à la définition de la signature électronique avancée donnée par la directive. Le contenu des annexes ne laisse planer aucun doute à ce sujet.

7. – Si la 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.

La clause d'assimilation (article 5.1.) consiste à assimiler la signature électronique avancée à la signature manuscrite lorsque certaines conditions sont remplies (19), c'est-à-dire à considérer que la signature électronique doit être recevable comme preuve en justice et qu'elle doit bénéficier de la force probante (20) accordée à la signature manuscrite. Cette clause est donc uniquement relative aux signatures électroniques avancées (pour autant que les conditions de l'article 2.2. soient remplies), et non pas à l'ensemble des mécanismes de signature électronique.

(18) Voir *supra*, n° 5.

(19) La signature électronique doit être avancée au sens de l'article 2.2., elle doit reposer sur un certificat qualifié tel que défini à l'article 2.10., et enfin elle doit être créée par un dispositif sécurisé de création de signature tel que décrit à l'annexe 3 de la directive.

(20) Par force probante, en 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.

La clause de non-discrimination (article 5.2.) s'applique lorsque les conditions auxquelles est subordonnée l'application de la clause d'assimilation ne sont pas remplies. Dans ce cas, les Etats membres doivent veiller à ce que l'efficacité juridique (21) et la recevabilité comme preuve en justice d'une signature électronique ne soient pas refusées pour le seul motif que la signature se présente sous forme électronique, ou qu'elle ne repose pas sur un certificat qualifié, ou encore qu'elle ne repose pas sur un certificat délivré par un prestataire de service de certification accrédité au sens de la directive. Le principe énoncé dans cet article doit être entendu comme celui de la recevabilité (22) des signatures électroniques *lato sensu*, ce qui constitue en soi un énorme progrès par rapport aux règles traditionnelles du droit de la preuve (23). Toutefois, à défaut de répondre aux spécifications de l'article 5.1., il appartient à celui qui s'en prévaut de convaincre le juge de la valeur probante du document signé électroniquement (24).

§ 3. – *La loi belge*

8. – En Belgique, la transposition de la directive européenne a fait l'objet de deux projets de loi. Le premier, non relevé de caducité, visait à réformer le Code civil afin d'en ouvrir les concepts aux nouvelles techniques de signature (25). Le second a pour but d'instaurer un régime juridique applicable aux prestataires de service de certification dans le cadre de l'utilisation de signatures électroniques avancées (26).

(21) On peut s'interroger sur la signification concrète de ce concept « d'efficacité juridique »!

(22) Rappelons que la recevabilité est la « prise en considération, par le juge, d'éléments probatoires déclarés admissibles par la loi eu égard à l'objet du litige ». Cela ne signifie donc pas que l'élément dit recevable aura forcément une influence sur la décision du juge; celui-ci peut parfaitement considérer que ledit élément ne prouve rien. Il n'a qu'une seule obligation : étudier l'élément en question.

(23) Comme le montre l'exemple du code secret à quatre chiffres repris ci dessus, note 17.

(24) Sur les conséquences de la distinction recevabilité/valeur probante, D. GOBERT et E. MONTERO, *op. cit.*

(25) Avant-projet de loi modifiant l'article 1322 du Code civil relatif à la preuve des obligations.

(26) Projet de loi relatif à l'activité des prestataires de service de certification en vue de l'utilisation de signatures électroniques, *op. cit.*

Un nouvel avant-projet de loi propose que soit inséré à l'article 1322 du Code civil l'alinéa suivant :

> *« Peut satisfaire à l'exigence d'une signature, pour l'application du présent article, un ensemble de données électroniques pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu du document ».*

Le but poursuivi par cette initiative est d'ouvrir le concept de signature afin que puissent être recevables en justice les actes sous seing privé signés électroniquement. L'interprétation donnée de la signature s'articule autour des concepts d'imputabilité et de maintien d'intégrité. L'imputabilité fait écho aux deux fonctions de la signature, à savoir l'identification du signataire et son adhésion au contenu de l'acte.

9. – La signature électronique dont la valeur juridique vient d'être évoquée peut cumuler, outre les fonctions traditionnelles de la signature traditionnelle, des fonctions nouvelles (27). En effet, la signature électronique basée sur la technique de la cryptographie asymétrique peut, d'une part, assurer l'intégrité du contenu de l'acte (28) et, d'autre part, « conférer à un document le statut de document original », ces fonctions étant autrefois garanties par la signature manuscrite apposée sur support papier. Ainsi, l'original ne se conçoit plus comme le support physique sur lequel est figé le contenu d'un document mais bien comme le résultat de la signature qui fixe logiquement cette fois le document, indépendamment du support (29). Nous verrons toutefois que la fonction d'intégrité reprise dans l'avant-projet de loi prête à discussion.

(27) Sur ces diverses fonctions de la signature, lire D. GOBERT et E. MONTERO, *op. cit.* Voir également, L. CORNELIS, « Contractuele aspekten van e-commerce », in *Le droit des affaires en évolution, Le commerce électronique*, ABJE, 10e Journée des Juristes d'entreprise, 22.X.99, Bruylant-Kluwer, 1999, p. 38.

(28) A ce propos, P. VAN EECKE, « Bewijsrecht en digitale handtekeningen : nieuwe perspectieven », in *Le droit des affaires en évolution, Le commerce électronique*, ABJE, 10e Journée des Juristes d'entreprise, 22.X.99, Bruylant-Kluwer, 1999, p. 234.

(29) Sur ce point, Y. POULLET, « Les transactions commerciales et industrielles par voie électronique », in *Le droit des Affaires en évolution*, 7e Journées des Juristes d'entreprises, 24.X.1996, Bruylant, 1996, p. 57 : « La stabilité du document s'entend non plus d'une garantie de pérennité du contenu et non du support dont la régénération peut être multiple »; E. DAVIO, « Preuve et certification sur Internet », *R.D.C.*, 1997, n° 11, p. 664.

10. – Certains esprits chagrins estimeront que l'acte de signer perd sa valeur symbolique, celle qui lui donne son poids de réflexion (30). C'est sans doute prêter beaucoup d'importance au tracé fait bien souvent à la hâte de quelques ambages au bas de pages parfois laissées en blanc. Rien n'éviterait par ailleurs que pour certains types d'actes, la signature même électronique soit entourée de l'apparition de messages écrans, rappelant les conséquences du simple clic qui la déclenche.

Par ailleurs, la signature électronique perd son attache physique, son lien à la personnalité d'un individu. Ce relâchement du lien nécessaire entre signature et individu explique que dorénavant la signature puisse être l'apanage des personnes tant physiques que morales. Tel est le choix opéré par le législateur belge et suivi par nombre de textes nationaux et internationaux (31). Ce n'est pas le lieu de détailler tous les arguments juridiques et pratiques qui plaident pour ou contre l'octroi de la signature aux personnes morales (32). Notons simplement que lorsque la commande à un site Web commercial est enregistrée et acceptée automatiquement par un logiciel de prise de commande qui émettra le message d'acceptation (33), ce message est signé par l'entreprise opérateur du site Web et non par une personne physique dont au commentateur il importe peu de connaître l'existence. Sans doute, des considérations de lutte contre la fraude pourraient-elles justifier dans certains types d'opérations que l'on puisse retrouver l'émet-

(30) C'est notamment le point de vue du Centre de Droit de la Consommation de l'U.C.L., à ce propos et pour d'autres références, lire V. CAMBIER, *L'authentification du consentement dans les paiements électroniques*, Rapport de recherche, 1998, U.C.L, Louvain-la-Neuve.

(31) C'est le cas de l'ensemble des lois anglo-saxonnes (Etats-Unis et Royaume Uni), la loi italienne va dans le même sens et la directive ne réserve pas aux seules personnes physiques la capacité de signer électroniquement. Pour toutes ces lois, le lecteur consultera les adresses des sites qu'il pourra trouver sur le site du CRID (http://www.droit.fundp.ac.be/crid.htm).

(32) L'exposé des motifs du projet de loi les reprend longuement (pp. 15 et s.)

(33) Ce qui soulève une autre interrogation juridique dans la mesure où le contrat est conclu automatiquement sans intervention humaine. Un tel contrat est-il valable au regard du principe suivant lequel un contrat résulte d'un concours de volontés, dont l'une est absente en l'occurrence ? Sur cette question, Y. POULLET, *How to conclude a contract through electronic means*, Rapport présenté à l'académie allemande de droit comparé, Freiburg, septembre 1999, à paraître.

teur, personne physique, d'un certain message, mais une telle considération d'exception peut être rencontrée par d'autres méthodes sans devoir nier en bloc la validité de la signature des personnes morales.

Quant à l'exigence du maintien de l'intégrité de l'acte, celle-ci ne figurait pas dans le projet initialement déposé devant le parlement (34). On peut craindre, qu'en introduisant une telle exigence, le législateur belge donne une interprétation trop restrictive de la signature qui ne soit pas en accord avec la directive européenne. Celle-ci, en parlant de méthode d'authentification, ne vise pas forcément la garantie de l'intégrité. Si cela avait été le cas, la directive aurait exigé que la signature électronique soit liée et non pas seulement jointe au document. Rappelons à ce propos que la directive (35) prend soin d'affirmer à la suite de la loi modèle de la CNUDCI (36) sur le commerce électronique le principe de non-discrimination. Toute signature électronique même non avancée, ne répondant à aucune des conditions nécessaires à la reconnaissance automatique de l'équivalence doit être recevable en justice même s'il reste au juge d'en apprécier la valeur probante. Eu égard à ces éléments, il convient de considérer que la définition trop stricte de la signature donnée par le législateur belge devrait

(34) *Doc. parl.*, Ch. Repr., sess. ord. 14 avril 1999, n° 2141/1. Celui-ci prévoyait d'introduire, à l'article 1322 du Code civil, la définition suivante : « Est assimilé à une signature manuscrite l'ensemble de données issues de la transformation de l'écrit et dont ressort avec certitude l'identité de l'auteur et son adhésion au contenu de l'écrit ».

(35) « Les Etats membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que :
- la signature se présente sous forme électronique, ou
- qu'elle ne repose pas sur un certificat qualifié, ou
- qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification, ou
- qu'elle n'est pas créée par un dispositif sécurisé de création de signature » (art. 5, 2 de la directive 99/93).

(36) Cf. à ce sujet l'article 9 de la loi modèle de la CNUDCI (loi-type de la CNUDCI sur le commerce électronique et Guide pour son incorporation, 1997 disponible à http://www.un.or.at/uncitral/fr-index.htm) qui traite de l'admissibilité et de la force probante des messages de données : « Aucune règle d'administration de la preuve ne peut être invoquée contre l'admissibilité d'un message de données produit comme preuve... ».

être allégée afin que soit assurée la transposition correcte de la directive.

Rappelons enfin que si la réforme de l'article 1322 du Code civil ne vise que la recevabilité des documents signés électroniquement, il appartient au juge de se prononcer sur la valeur probante des documents qui lui sont soumis. Ce pouvoir d'appréciation devrait s'articuler autour du critère de fiabilité de la technologie de signature utilisée. Celle-ci devrait être appréciée au regard de l'objet du message de données qui a été signé électroniquement, compte tenu de toutes les circonstances (37).

11. – Le projet de réforme de l'article 1322 du Code civil est intimement lié au projet de loi relatif à l'activité des prestataires de service de certification en vue de l'utilisation de signatures électroniques. Celui-ci fait écho, en son article 4 § 4, à la clause d'assimilation prévue par la directive « signature électronique ». Cet article établit un lien entre le projet dont il émane et la réforme proposée du Code civil puisqu'il assimile à une signature au sens de l'article 1322 du Code civil toute signature électronique avancée réalisée sur la base d'un certificat qualifié et créée par un dispositif sécurisé de création de signature. Cette assimilation est motivée par le fait que le dispositif sécuritaire entourant les prestataires de service de certi-

(37) Pour apprécier la fiabilité de la technique de signature utilisée, la CNUDCI propose une série de critères d'évaluation : 1) le degré de perfectionnement du matériel utilisé par chacune des parties; 2) la nature de leur activité commerciale; 3) la fréquence avec laquelle elles effectuent entre elles des opérations commerciales; 4) la nature et l'ampleur de l'opération; 5) le statut et la fonction de la signature dans un régime législatif et réglementaire donné; 6) la capacité des systèmes de communication; 8) la série de procédures d'authentification communiquée par un intermédiaire; 9) l'observation des coutumes et pratiques commerciales; 10) l'existence de mécanismes d'assurance contre les messages non autorisés; 11) l'importance et la valeur de l'information contenue dans le message de données; 12) la disponibilité d'autres méthodes d'identification et le coût de leur mise en œuvre; 13) le degré d'acceptation ou de non-acceptation de la méthode d'identification dans le secteur ou domaine pertinent, tant au moment où la méthode a été convenue qu'à celui où le message de données a été communiqué; et tout autre facteur pertinent (Guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur le commerce électronique (1996), pp. 38 et 39). A ces critères devrait être ajouté celui de l'aptitude du mécanisme de signature de garantir l'intégrité du message.

fication accrédités confère à la signature électronique avancée un niveau de sécurité et de fiabilité au moins équivalent à la signature manuscrite. Il en résulte que la signature avancée revêt la même force probante que la signature manuscrite et qu'elle s'impose donc au juge en cas de litige, sans que celui-ci dispose d'un quelconque pouvoir d'appréciation.

Il découle de cette assimilation que les dispositions des articles 1323 et 1324 du Code civil sont d'application : celui à qui on opposera un acte sous seing privé revêtu d'une signature électronique avancée pourra en désavouer formellement son écriture ou sa signature. Une enquête judiciaire en vérification d'écriture sera ordonnée et exécutée conformément à la procédure prévue aux articles 883 et suivants du Code judiciaire. Sans doute, la procédure en vérification et l'expertise à laquelle elle conduit, seront-elles menées différemment : l'authenticité d'une signature manuscrite exige une vérification par un graphologue; la qualité d'un système technique et organisationnel de production d'une signature électronique relève de l'expertise de sociétés d'audit spécialisées.

§ 4. – *La loi française*

12. – La réforme du droit français de la preuve passe également par une définition de la signature. Le législateur français définit la signature comme suit :

> « *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.*
>
> *Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve du contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat* »
> (article 1316-4 du Code civil).

Le choix de l'article 1316 du Code civil pour introduire une telle définition n'est pas innocent puisque, repris sous le titre de la preuve des obligations et de celle du payement, il précède la première section de ce chapitre consacrée à la preuve littérale. La définition donnée de la signature s'applique donc tant aux actes authentiques qu'aux actes sous seing privé. En procédant à cette réforme, le législateur français a donc franchi un pas important, que n'exigeait pas la directive « signature électronique », puisqu'il offre aux officiers publics la possibilité de dresser les actes authentiques sur support électronique. La passation électronique d'actes authentiques suscite diverses questions qui seront traitées par ailleurs.

13. – L'article 1316-4 fait écho aux deux fonctions de la signature (identification du signataire et volonté de s'approprier le contenu de l'acte). Par ailleurs, la définition de la signature électronique fait référence à l'utilisation d'un procédé fiable d'identification. Ce critère est abandonné à l'appréciation du juge.

La directive établit une équivalence entre la signature manuscrite et la signature électronique lorsque cette dernière est avancée, basée sur un certificat qualifié et créée par un dispositif sécurisé de création de signature. Du fait de cette assimilation, seule la mise en œuvre d'une procédure d'inscription en faux, s'il s'agit d'un acte authentique, ou en désaveu d'écriture ou de signature, s'il s'agit d'un acte sous seing privé, permettra de contester une telle signature électronique (38). La présomption réfragable de fiabilité prévue par la loi française nous semble contraire à toute sécurité juridique (39).

III. – *L'écrit : un concept à définir?*

§ 1er. – *Les trois qualités de l'écrit*

14. – L'exigence d'un écrit en tant que telle, indépendamment de toute signature, n'est pas clairement spécifiée dans la loi. Elle découle de la notion d'« acte », la signature n'ayant de

(38) Il s'agira pour le juge aidé d'un expert de vérifier dans quelle mesure les éléments avancés par la partie qui désavoue son écriture peuvent être suffisamment établis pour remettre en cause l'apparence que crée le système d'information qui a généré la « trace » qui lui est attribuée.

(39) En fait, à la différence de la procédure en désaveu d'écriture, la question devient celle de la fiabilité du système : celui à qui on oppose la signature ne met pas en cause le fait que la trace émane de lui mais bien la capacité du système à générer une trace valable. En d'autres termes, selon la loi française, on peut considérer que, dans le cas d'utilisation d'un système non fiable, l'auteur d'un message pourra remettre en cause sa signature.

raison d'être que par l'écrit auquel elle se rapporte. Avec la dématérialisation des données se pose aujourd'hui la question de la nature de l'« écrit ». Dans le contexte de la recevabilité et de la force probante des actes juridiques, trois qualités devraient le caractériser (40), même si l'article 1347 permet d'accueillir comme écrit de manière plus large des supports ou « traces » de la volonté exprimée.

L'**inaltérabilité** – Dans le contexte papier, celle-ci est assurée par le support lui-même. Le support prévient toute modification ultérieure du contenu du document par les parties ou par des tiers, que ce soit de façon volontaire ou involontaire. Dans le contexte électronique, le support ne garantit plus nécessairement l'inaltérabilité de l'écrit. Puisque le consentement d'une personne à un acte s'inscrit par rapport à un contenu spécifique, il convient de préserver celui-ci adéquatement. Il s'avère dès lors que dans le contexte électronique, l'écrit devient indissociable de méthodes qui en garantissent l'intégrité. Celles-ci seront le plus souvent liées à un processus informatique tel que la signature digitale.

La **lisibilité** – Les informations doivent pouvoir être accessibles à la compréhension humaine grâce à un procédé approprié. Les documents sur papier remplissent directement cette condition par le simple fait qu'ils sont rédigés dans un langage (vocabulaire et grammaire) et dans une symbolique graphique (écriture) accessibles à la compréhension humaine. Concernant les informations contenues sur support informatique, la condition de « lisibilité » implique le recours à une technique adéquate pour restituer les données sous une forme lisible. Cela implique que le logiciel nécessaire à la lisibilité des informations soit préservé ou que les données soient converties de façon telle à les rendre lisibles à l'aide de nouveaux logiciels.

La **stabilité** – Le contenu de l'écrit doit être fixé définitivement au moment de sa rédaction. Dans le contexte papier, la

(40) La CNUDCI fait en partie écho à ces différentes caractéristiques puisqu'elle considère que « lorsque la loi exige qu'une information soit sous forme écrite, un message de données satisfait à cette exigence si l'information qu'il contient est accessible pour être consultée ultérieurement ». Seul n'est pas pris en considération le critère de l'inaltérabilité, jugé trop restrictif (Guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur le commerce électronique, *op. cit.*, p. 35).

stabilité du document est inhérente aux propriétés de son support : il se dégrade peu. En matière électronique, les supports de stockage vieillissent rapidement et nécessitent dès lors une retranscription du contenu. Cela ne revient pourtant pas à dire que les techniques informatiques ne permettent pas de rencontrer l'exigence de stabilité. En réalité, comme déjà affirmé (*supra*, n° 9), la stabilité d'un écrit vise la pérennité de son contenu, indépendamment du support. Peu importe donc que, pour des raisons de pérennité, le contenu d'un écrit ait été transféré d'un support sur un autre, pourvu que son caractère original ait été préservé (41).

§ 2. – *Opportunité d'une réforme de la notion d'écrit*

15. – Si la preuve écrite s'articule en droit autour du concept de signature, l'écrit n'a, quant à lui, pas fait l'objet d'un traitement spécifique. En réalité l'écrit n'a de valeur que par la signature qui l'accompagne.

Une hypothèse doit toutefois être mise en exergue : il s'agit de celle de l'acte authentique ou sous seing privé entaché d'irrégularité suite, notamment, à l'absence de signature. Cette hypothèse est expressément visée par l'article 1347 du Code civil (42) relatif au commencement de preuve par écrit. Puisque l'article 1347, alinéa 2 définit le commencement de preuve par écrit, il ne nous paraît pas opportun d'introduire une (nouvelle) définition de l'écrit dans le Code civil.

(41) A noter que cette qualité se retrouve également dans la définition de la présomption « d'original » proposé par la CNUDCI en son article 8 que ni la directive, ni le projet belge ne reprennent. L'exigence d'original est satisfaite si « ce sont des messages de données qui sont conservés, sous réserve des conditions suivantes :

a) L'information que contient le message de données doit être accessible pour être consultée ultérieurement;

b) Le message de données doit être conservé sous la forme sous laquelle il a été créé, envoyé ou reçu, ou sous une forme dont il peut être démontré qu'elle représente avec précision les informations créées, envoyées ou reçues;

c) Les informations qui permettent de déterminer l'origine et la destination du message de données, ainsi que les indications de date et d'heure de l'envoi ou de la réception, doivent être conservées si elles existent ».

(42) Le commencement de preuve par écrit est défini comme étant « tout acte par écrit qui est émané de celui contre lequel la demande est formée, ou de celui qu'il représente, et qui rend vraisemblable le fait allégué ».

Cela ne veut toutefois pas dire qu'il ne faille pas repenser la notion d'écrit. L'écrit ne doit plus être uniquement envisagé comme un support durable (tel que le papier) mais doit plutôt viser la garantie d'un contenu durable. En effet, dans l'environnement papier, il y a une confusion constante entre le contenu et le support, les deux notions ne faisant qu'une car le contenu est matériellement lié au support et l'intégrité n'est assurée que tant que le contenu se trouve sur le premier support. La fonction d'intégrité (et d'inaltérabilité) est donc partiellement (43) remplie grâce au papier.

16. – Il en va différemment dans le contexte électronique puisque l'intégrité du contenu d'un message peut être garantie alors même que celui-ci change de support (tel est le cas, par exemple, d'un fichier signé digitalement qui se trouve sur une disquette et qui est ensuite transféré sur un disque dur et enfin sur un réseau). Dès lors, on constate que l'intégrité du contenu d'un message n'est plus assurée par le support mais par un mécanisme technique (tel que la signature digitale) qui fige logiquement, et non plus matériellement, le contenu de l'écrit électronique. De telles réflexions nécessitent que soient par ailleurs repensées les notions d'original et de copie (44).

§ 3. – *Loi française*

17. – La réforme de la notion d'écrit est opérée en quatre temps. L'article 1316 du Code civil définit tout d'abord la notion d'écrit de la façon suivante : « La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leurs supports et leurs modalités de transmission ».

L'article 1316-1 détermine les conditions d'admissibilité de l'écrit électronique en justice. Afin qu'un écrit sous forme électronique soit admis en justice au même titre qu'un écrit sur

(43) Elle est, dans une certaine mesure, également remplie par la signature manuscrite dans la mesure où celle-ci est apposée au bas du document ce qui rend difficile les surcharges ou ajouts.

(44) Voir sur cette question les réflexions intéressantes d'E. Davio, *op. cit.*, pp. 664 à 666. Voir également D. Gobert et E. Montero, *DA/OR, op. cit.*, pp. 24 et 25.

support papier, il faut que puisse être « dûment identifiée la personne dont il émane » et qu'il soit « établi et conservé dans des conditions de nature à en garantir l'intégrité ».

L'article 1316-2 règle la question des conflits de preuve littérale : dans cette hypothèse, le juge détermine par tout moyen le titre le plus vraisemblable.

Enfin, l'article 1316-3 prévoit que l'écrit sur support électronique a la même force probante que l'écrit sur support papier.

18. – La réforme française opérée à propos de la notion d'écrit suscite diverses observations. Sans revenir sur la question de l'opportunité d'une définition de la notion d'écrit dans le Code civil, on peut s'interroger sur la définition même donnée de l'écrit. Il est regrettable qu'elle s'attarde à ses formes possibles sans mettre suffisamment en exergue ses qualités intrinsèques.

Cette critique doit toutefois être tempérée dans la mesure où l'article 1316-1 fait explicitement référence à la notion de garantie d'intégrité à propos de la notion d'écrit. On se posera toutefois la question de savoir si le législateur entendait bien définir le concept d'écrit plutôt que celui d'acte. La lecture de l'article 1316-1 à la lumière de l'article 1316-3 traitant de la force probante de l'écrit confirme le doute formulé à ce sujet.

Enfin, le législateur ayant défini le concept d'écrit, l'on peut se poser la question de l'opportunité de réintroduire la notion de support en spécifiant que l'écrit sur support électronique a la même force probante que l'écrit sur support papier (article 1316-3). Une telle précision était inutile à nos yeux pour trois raisons fondamentales : la notion d'écrit doit être, ainsi que nous l'avons vu, détachée du support, une définition de l'écrit supprime toute suprématie et rend donc inutile une telle spécification, enfin la force probante est attachée à la notion d'acte et non d'écrit (45).

(45) « L'écrit ne s'impose en qualité d'acte sous seing privé que pour autant que la signature soit reconnue » ; N. Verheyden-Jeanmart, *Droit de la preuve*, Précis de la Faculté de Droit de l'Université Catholique de Louvain, Bruxelles, Larcier, 1991, p. 271.

TITRE 2. – AU DELÀ DES CONCEPTS : LA MISE EN ŒUVRE DE LA CONFIANCE PAR DES TIERS

I. – *Certifier l'origine, la destination et l'intégrité d'un message : de la signature électronique aux autorités dites de certification*

19. – La signature électronique (46) représente, dans le monde d'Internet, le moyen de certifier l'origine, la destination, voire l'intégrité d'un message. Comme le proposait la définition du défunt projet de loi belge visant à modifier certaines dispositions du Code civil, « une signature peut être un ensemble de données numériques pour autant qu'elle puisse être imputée à une personne déterminée et qu'elle établisse l'intégrité du message ». La directive européenne récemment adoptée la définit comme « une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthodes d'authentification ».

Sans doute, dans la hâte de reconnaître à ce produit de la technique une certaine valeur juridique, a-t-on trop insisté sur les similarités fonctionnelles de la signature électronique et de la signature traditionnelle pour ne pas constater les radicales différences des deux procédés. La signature manuscrite tire sa valeur de sa seule apposition; la signature électronique de la qualité du procédé utilisé et de l'intervention de tierces parties, les prestataires de service de certification.

Comme nous l'avons rappelé *supra*, (n° 6), quatre qualités caractérisent le procédé permettant la « bonne » signature électronique, celle que le projet de loi belge, à la suite de la directive, qualifie d'« avancée » (47) et à laquelle elle réserve des

(46) A propos de la signature dite électronique, les écrits sont nombreux. On se référera en particulier aux écrits, en langue française, de D. GOBERT et E. MONTERO, *op. cit.*, et, en langue néerlandaise, de P. VAN EECKE, *op. cit.*, pp. 214 à 267. Le lecteur y trouvera une bibliographie abondante.

(47) Article 2, 1° du projet de loi relative à l'activité des prestataires de services de certification en vue de l'utilisation de signatures électroniques. Il est à noter que le projet belge ne définit pas à proprement parler la simple signature électronique alors que la directive européenne 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signataires électroniques prend soin de le faire.

avantages légaux : la signature doit « être liée uniquement au signataire », « permettre l'identification du signataire », « être créée par des moyens que le signataire puisse garder sous son contrôle exclusif », enfin, être « liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée ».

20. – L'intervention d'un prestataire délivrant un certificat, c'est-à-dire une « attestation électronique sécurisée par la signature électronique avancée d'un prestataire de service de certification qui confirme notamment le lien entre une personne physique ou morale et les données afférentes à la vérification de la signature de celui-ci », est sans doute l'élément le plus caractéristique de la signature électronique. Alors que l'intervention d'un officier public légalisant la signature manuscrite d'autrui était un procédé rare, il est de l'essence même de la signature électronique d'impliquer le recours à un tiers. La qualité de ce tiers et du certificat qu'il émet est décisive en ce qui concerne la valeur de la signature électronique dite « avancée ». La signature électronique avancée, reposant sur un certificat qualifié, contenant certaines mentions et émis par un prestataire répondant à certaines exigences, et créée par un dispositif sécurisé de création de signature (48) équivaut à une signature manuscrite (49).

Cette équivalence est également reconnue par le droit belge (50) qui ajoute une précision : en cas d'accréditation préalable du prestataire de service de certification (51), la

(48) L'article 2, 6° du projet de loi définit le dispositif sécurisé de création de signature comme suit : « un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature qui satisfait aux exigences de l'article 11 de la présente loi ». Le texte de l'article 11 reprend par ailleurs les exigences définies par l'annexe 3 de la Directive.

(49) Article 5.1. de la Directive « signature électronique ».

(50) L'article 4 § 4 du projet belge estime en effet que « ... une signature électronique avancée réalisée sur base d'un certificat qualifié et créé par un dispositif sécurisé de création de signature est assimilée à une signature au sens de l'article 1322 du Code civil... ». On notera que le projet de loi sur les prestataires de service de certification renvoie implicitement à une modification nécessaire de l'article 1322 du Code civil qui ne pourrait accueillir dans sa version actuelle la signature électronique.

(51) L'accréditation s'opère suite à l'examen par l'Administration du Ministère des Affaires économiques des conditions fixées à l'article 5 § 1.

signature utilisant un certificat émis par ce prestataire bénéficie d'une équivalence automatique. Sans doute, jugera-t-on sensée cette précision belge supplémentaire. En effet, la solution européenne qui n'exige pas l'accréditation du prestataire de service de certification, mais simplement qu'il réponde aux exigences de l'annexe 2 de la directive et qu'il l'indique sur le certificat, fait reposer sur le destinataire d'un message la charge de vérifier le respect, par le prestataire de service de certification, des exigences prévues à l'annexe 2, faute de quoi il risque de voir remise en cause la valeur juridique de la signature ainsi créée. L'équivalence ne pourrait alors dans un tel contexte qu'être présumée (52).

21. – Peut-être regrettera-t-on plus l'ampleur des exigences belges de l'accréditation (53). En particulier, l'accessibilité devant être assurée en permanence par voie électronique à toute personne, accessibilité à une base de données où sont consignés tous les certificats émis, est prévue par l'article 5, § 1, 7° et l'article 10 du projet de loi belge. Une telle exigence est-elle nécessaire lorsqu'il appert que l'objectif de vérification de la signature peut être atteint par d'autres moyens sans nécessiter l'accès de tous à la base de données des certificats (54). Ensuite, la comparution personnelle du demandeur de la signature est requise en Belgique et non point par la directive. Cette exigence, sans doute inutile lorsqu'une autorité de certification belge se borne à garantir un certificat émis à l'étranger par une autorité accréditée dans son pays, permet dans les autres hypothèses d'assurer une plus grande sécurité lors de la procédure de vérification de l'identité et des qualités de la personne, objet de mentions obligatoires dans son certificat. Elles seront le fait vraisemblablement d'autres organismes que les prestataires eux-mêmes.

(52) A propos de l'accréditation des prestataires de service de certification et de l'insécurité juridique résultant de la notion de certificat qualifié donnée par la directive, voir M. ANTOINE, D. GOBERT, « La directive européenne sur la signature électronique. Vers la sécurisation des transactions sur l'Internet », *J.T.D.E.*, n° 68, pp. 74 et 75.

(53) Dont la directive européenne rappelle en son article 3.2. que les critères retenus doivent être « objectifs, transparents, proportionnés et non discriminatoires ». Cette exigence européenne ne semble pas avoir été respectée par l'arrêté royal du 16 octobre 1998 « portant des dispositions diverses relatives à la signature électronique », qui s'applique à la sécurité sociale, en application de l'article 38 de la loi du 26 juillet 1996 portant modernisation de la sécurité sociale et assurant la viabilité des régimes légaux des pensions, *M.B.*, 7 novembre 1998 (prolongé par l'A.R. du 11 avril 1999 (*M.B.*, 2 juillet 1999).

(54) Ainsi, on peut prévoir qu'un message émanant du prestataire et émis à la demande du destinataire confirme l'identité de l'émetteur du message. Il va de soi que la publication de tous les certificats crée des problèmes à la fois de protection des données des personnes reprises dans la base de données et de concurrence déloyale de la part d'autres prestataires.

Ainsi, on peut imaginer que les communes, les notaires, voire certaines entreprises ou associations professionnelles, puissent jouer, vis-à-vis des « Certification Authorities », le rôle de « Registration Authorities », c'est-à-dire d'organes vérifiant l'identité, voire la ou les qualités de la personne. Ni la directive, ni le projet de loi ne mentionnent leur intervention située en amont de celle de l'émission du certificat. Sans doute, faut-il considérer que la responsabilité de leur intervention est entièrement couverte par le prestataire de service de certification qui a sollicité leur intervention, quitte à ce que ce prestataire puisse sur une base contractuelle se retourner par la suite contre eux pour inexécution fautive de leurs obligations (cela pourrait être le cas, par exemple, si la « Registration Authority » orthographie incorrectement l'identité d'une personne ou omet de vérifier le pouvoir de représentation d'une personne physique intervenant pour une personne morale). Enfin, l'avant-projet belge exige l'interopérabilité des prestataires de service de certification sans définir ce que signifie une telle interopérabilité. S'agit-il d'une simple accessibilité croisée des annuaires ou, au-delà, exige-t-on l'adoption de normes communes pour les logiciels de cryptage ?

II. – *Au-delà des autorités de certification*

§ 1er. – *Certifier des éléments de la transaction*

22. – La transaction électronique exige comme toute transaction d'autres garanties que celles déjà évoquées. Au premier rang d'entre elles figure la date. Ainsi, le recommandé postal est-il exigé dans certains cas pour donner à l'envoi et à la réception preuve et date certaine. D'autres procédés existent à ce dernier propos : on pourrait citer l'article 1327 du Code

civil qui subordonne la preuve de la date certaine d'un acte juridique à l'enregistrement de l'acte par l'administration ou encore l'acte authentique, autre mécanisme prévu par ce même Code civil, pour accorder à l'acte passé devant notaire et à sa date de passation pleine foi. Sans doute, importe-t-il que ces procédés puissent trouver leur équivalent électronique fonctionnel! On conçoit aisément qu'au cachet postal du guichetier de la poste, on puisse substituer la trace électronique de la réception d'un message par le certificateur et l'acheminement électronique de ce message en même temps que la trace électronique de sa réception, c'est-à-dire de l'ouverture de la boîte aux lettres électronique. L'enregistrement d'une convention par la conservation des hypothèques suppose simplement qu'une copie fidèle du message électronique signé par les deux parties ou l'échange de messages concordants chacun signé par l'une des parties (55) soit déposé dans la boîte aux lettres électronique de cette administration et que sa réception soit authentifiée par le récepteur du message. Quant à l'acte authentique, les Etats membres, selon la directive relative à certains aspects du commerce électronique (56), peuvent l'exclure du champ d'application de la directive et dès lors interdire qu'il soit conclu par voie électronique. Toutefois, l'acte authentique suppose-t-il nécessairement le face à face des parties et de leur notaire? Ne pourrait-on concevoir que le notaire instrumente certes en l'absence physique des parties, mais bien en leur présence virtuelle? La question est posée aux notaires! Il ne nous appartient pas de la résoudre (57).

(55) Comme le notent avec pertinence MM. GOBERT et MONTERO, *DA/OR*, *op. cit.*, p. 25, « ainsi une doctrine et une jurisprudence unanimes considèrent que la formalité des originaux multiples, imposée en matière d'actes sous seing privé constatant des conventions synallagmatiques, ne leur est pas applicable » (c'est-à-dire dans l'hypothèse de l'échange de données électroniques en vue de conclure un acte sous seing privé).

(56) Cf. à ce propos l'article 9 de la Directive relative à certains aspects juridiques du commerce électronique dans le marché intérieur : « Les Etats membres peuvent prévoir que le paragraphe 1 ne s'applique pas aux contrats suivants :

a) les contrats qui nécessitent l'intervention d'un notaire;

b) .... »

(57) A cet égard, on lira avec attention les réflexions de la Fédération royale des notaires de Belgique lors du forum @gora (site web déjà cité).

23. – Si des équivalents fonctionnels peuvent être trouvés, il s'impose que le législateur réfléchisse à deux points.

– Doit-il, en la matière, confirmer les monopoles existant ou, au regard des possibilités offertes par le marché, libéraliser l'offre de tels services de certification et ouvrir cette offre à des entreprises privées, quitte, comme en matière de signature électronique, à exiger leur agrément? Sur ce point, on regrettera que par un arrêté royal passé inaperçu (58), le précédent gouvernement ait étendu le monopole postal au recommandé électronique du moins dans les applications du recommandé administratif ou judiciaire. En sera-t-il de même demain en matière d'enregistrement?

– Bien des transactions exigeront non seulement le contrôle de l'identité, mais également la qualité de la personne, que ce soit sa capacité juridique en tant que personne physique (est-elle majeure selon sa législation nationale; n'est-elle pas frappée d'interdiction?), ou sa capacité à engager la personne morale, voire l'administration. A ce propos, on peut imaginer qu'à la signature électronique de la personne physique, on ajoute la signature électronique d'un notaire certifiant une telle capacité (59). Au sein de l'administration, des registres officiels certifiant la qualité et la compétence des fonctionnaires, agents publics et mandataires publics devraient également exister (60). Ces signatures permettraient aux tiers lors-

(58) Il s'agit de l'arrêté royal du 9 juin 1999 transposant les obligations découlant de la directive 97/67/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant des règles communes pour le développement du marché intérieur des services postaux de la Communauté et l'amélioration de la qualité du service (*M.B.*, 18.08.99) dont l'article 21 § 2 prescrit : « Pour la protection de l'intérêt général et de l'ordre public, le service des envois recommandés utilisés dans le cadre de procédures judiciaires ou administratives sont également réservés à la poste et ce quel qu'en soit le support »).

(59) La Fédération royale des notaires de Belgique, lors du forum @gora, avait introduit avec beaucoup de pertinence un nouvel article 1334 : « La signature d'un écrit sous seing privé ou assimilé à celle-ci peut être légalisée par un notaire lorsque la signature est apposée en présence du notaire. Le notaire doit s'assurer préalablement de l'identité de la personne qui a apposé sa signature, de la véracité de la signature utilisée par elle et de sa capacité de signer le document... ».

(60) A notre connaissance, en Belgique, seul le Centre régional informatique Bruxellois (C.R.I.B.) a pris une telle initiative. Cf. également l'important projet de recherche AGORA mené en 1997 et 1998 par les S.S.T.C. du Premier Ministre.

qu'ils souhaitent effectuer une opération administrative quelconque avec l'Administration (dépôt d'une demande de permis de bâtir, légalisation d'une signature, envoi d'une déclaration fiscale, paiement d'une taxe,...) de vérifier les compétences et la qualité de l'interlocuteur invité à signer un reçu, une déclaration ou à engager l'Administration.

§ 2. – *Certifier la « copie »*

24. – L'archivage des transactions électroniques rencontre quelques difficultés. Certes, nous l'avons dit (voir n° 9), la signature électronique (61) – et c'est l'essence même de la méthode cryptographique qui la caractérise – permet d'assurer l'intégrité du document dans la durée peu importe les multiples supports qui recueilleront la trace du message. Cependant, l'obsolescence des supports ou plutôt des moyens d'accéder à leur contenu et la nécessité pour des raisons évidentes de régénérer les clés obligent à s'interroger sur la valeur des « copies ». Selon la formule de De Page (62), la copie se distingue en effet de l'original « par la circonstance qu'elle constitue une transaction non signée ». La valeur de copies électroniques générées à partir d'originaux eux-mêmes électroniques (63) devient un sujet crucial dans la mesure où se développe le commerce électronique.

Sans doute, comme l'a néanmoins fait jusqu'ici, et de manière fort critiquable, le législateur belge qui autorise certaines entreprises à prouver par copie pour autant que la confection de cette copie ait été faite sous leur responsabilité (64), ne pourra-t-on demain se contenter de solutions parcellaires, peu fiables et n'offrant pas par des mesures techniques et organisationnelles appropriées la sécurité requise. Sans

(61) Par signature électronique, on vise ici, les signatures basées sur la cryptographie asymétrique.

(62) DE PAGE, *Traité de droit civil*, T. III, p. 7.

(63) Il ne s'agit plus, comme c'était le cas il y a dix ans, de réfléchir sur la manière dont on pouvait microfilmer ou « scanner » des documents papiers.

(64) Pour une critique sévère des multiples textes réglementaires pris pour quelques entreprises de crédit du secteur public, dans un premier temps, pour l'ensemble du secteur bancaire, ensuite, pour le secteur des assurances, enfin, lire J.P. BUYLE, « Nouvelles règles en matière de preuve par copie de documents », *J.T.*, 1993, pp. 197 et s.

doute, s'agira-t-il d'exiger pour ceux qui font profession de commercer et dès lors de générer nombre de transactions d'exiger le suivi de procédures et le respect de certaines normes comme le préconisait, dès 1981, le Conseil de l'Europe (65) afin de garantir la valeur des copies, voire le cas échéant, de prôner l'intervention de tiers agréés qui auditeront les procédures et le respect des normes ou procéderont eux-mêmes à l'archivage (66).

§ 3. – *Certifier le respect par le contractant de certaines exigences réglementaires : la labellisation des sites Web*

25. – La labellisation des sites Web, selon M. Antoine, D. Gobert et A. Salaun (67), s'entend « comme l'initiative de marquer ses propres services d'un niveau de qualité par un engagement à respecter certains critères ». Elle s'inscrit parmi les diverses techniques d'autoréglementation (68). Elle permet de donner aux codes de conduite une certaine effectivité (69) dans

(65) Recommandation du Conseil de l'Europe, n° R (81) 20 relative à l'harmonisation des législations en matière d'exigence d'un écrit et en matière d'admission de reproduction de documents et des enregistrements informatiques. Sur cette recommandation, les commentaires de M. ANTOINE, J-F. BRAKELAND et M. ELOY, *Le droit de la preuve face aux nouvelles technologies de l'information et de la communication*, Cahiers du CRID, n° 7, Story-Scientia, 1991, p. 206.

(66) Sur la nécessité d'une réflexion sur le droit de l'archivage et des premiers éléments de réflexion, lire E. CAPRIOLI, « Variations sur le thème du droit de l'archivage dans le commerce électronique », *Petites Affiches*, 18 août 1999, n° 164, pp. 4 à 11 et 19 août 1999, n° 165, pp. 7 à 12.

(67) D. GOBERT et A. SALAUN, *DA/OR*, *op. cit.*, p. 85. A propos de cette technique, lire Y. POULLET, J. ROYEN, @gora, *op. cit.*

(68) Pour une analyse de ces diverses techniques d'autoréglementation, Y. POULLET, « Les diverses techniques de réglementation d'Internet : l'autorégulation et le rôle du droit étatique », *op. cit.* En réalité, la labellisation s'ajoute à une autre technique d'autoréglementation : le code de conduite. Il s'agit par la technique du label de donner au code de conduite une effectivité plus grande liée aux sanctions propres au label (le retrait du label et la publication d'une black list) et à son mode de publicité.

(69) C'est bien en effet le gros reproche que d'aucuns adressent à l'autoréglementation. Ainsi le code de conduite néerlandais pour le commerce électronique présente comme le « Poldersmodel » et lancé suite à une initiative du Ministère de l'économie (http://www.ecp.nl) ne contient aucune disposition relative à la sanction du code (à propos de ce code, K. STUURMAN, « E-Commerce : What's new ? Enkele recente ontwikkelingen op het terrein van regulerings-initiatieven voor de elektronishe handel », *Computerrecht*, 1999, p. 99).

la mesure où le label affiché sur le site Web indique l'engagement de l'opérateur de celui-ci de respecter le code de conduite. En cas de manquement, certaines sanctions (retrait du label, publication de listes noires) peuvent être appliquées (70). C'est sur ce principe que fonctionnent deux labels récemment introduits, l'un par les consommateurs (Web Trader (71)), l'autre par les sociétés de Marketing direct réunies au sein de la Fedma.

26. – Notre propos n'est pas de définir les différents types de labellisation (72). On sait que la labellisation peut être spécifique (en portant sur le respect d'une réglementation telle que celle relative à la protection de données) ou globale, qu'elle peut être interne ou externe (en impliquant dans ce second cas l'intervention préalable et périodique d'un ou de plusieurs organismes tiers indépendants dans la définition et le contrôle du respect de critères prédéfinis), enfin, que le contrôle des conditions de la labellisation peut être minimal ou maximal (73). *A priori*, on peut songer à divers candidats pour ce type d'activités : à côté des associations sectorielles ou de consommateurs dont les initiatives ont été citées, des sociétés

Cette lacune est à souligner au moment où les défenseurs de l'autoréglementation élaborée par les milieux professionnels eux-mêmes soulignent la plus grande efficacité de celle-ci par rapport aux modes traditionnels d'intervention étatique.

(70) A noter en outre que certains systèmes d'aide à la navigation sont mis au point qui reposent sur la reconnaissance automatique des labels présents sur les sites Web. Ainsi le système P.3.P. élaboré par le W.3.C. permettra à l'internaute de sélectionner les seuls sites Web respectant ses « privacy preferences ».

(71) http://www.budget-net.com/bnet/webtradersite/webtrader_home_be.html

(72) A ce propos, pour une description des « labels » présents sur le marché et les 5 niveaux de labellisation, lire D. GOBERT, A. SALAUN, « La labellisation des sites Web : classification, stratégies et recommandations », *DA/OR*, nov. 1999, n° 51, pp. 83 à 94.

(73) Ainsi, on peut concevoir que le label soit octroyé sur simple déclaration par le site web de son respect des critères et qu'une simple hot mail ou un contrôle aléatoire permette le cas échéant d'examiner le respect des conditions de la labellisation ou, à l'inverse, que la labellisation d'un site ne soit opérée que sur base d'un contrôle *a priori*.

d'assurance (74) ou de révisorat d'entreprises (75) peuvent intervenir en la matière.

27. – La labellisation peut être encouragée par l'Etat : l'article 80 § 3 de la loi belge du 25 mai 1999 (76), qui transpose la directive relative aux contrats à distance (77) octroie au site web labellisé l'avantage de ne plus être soumis à l'interdiction d'exiger un acompte ou paiement quelconque du consommateur et ce avant la fin du délai de renonciation de 7 jours (78). Sans doute, restera-t-il à s'interroger sur la façon dont l'arrêté royal fixera les conditions de la labellisation. A cet égard, le gouvernement s'inspirera peut-être des recommandations de l'atelier @gora.

(74) Le 18 janvier 2000, la société européenne d'assurances « Gerling » annonçait son projet de labellisation de sites : Trusted Shops, lié à l'engagement précis de cette société d'honorer les conséquences des droits de renonciation pour des produits acquis auprès des sites web labellisés par cette société d'assurance.

(75) Ainsi, le projet introduit par l'Institut belge des réviseurs d'entreprises longuement décrit par le rapport de l'atelier @gora déjà cité.

(76) Loi modifiant la loi du 14 juillet 1991 sur les pratiques de commerce et sur l'information et la protection du consommateur, *M.B.*, 23 juin 1999, p. 23670 (à propos de cette loi et de l'article 80 § 3, en particulier, lire les commentaires de A. SALAUN, « Transposition de la Directive Contrats à distance en droit belge : Commentaire de l'article 20 de la loi du 25 mai 1999 », *J.T.*, 2000, pp. 41 et s.).

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

(78) Le Grand Duché de Luxembourg s'oriente également vers une solution parallèle. Un projet soumis lors de la précédente législature (disponible à http://www.droit.fundp.ac.be/textes/EcolU.pdf) permet, en son article 66, à l'opérateur d'un site Web de faire preuve du respect de ses obligations d'informations préalable, de la confirmation écrite des informations lors d'une commande, du respect des délais de rétractation..., en se référant à un « mécanisme de certification de qualité du professionnel ».

Conclusions et autres réflexions à propos de la notion de confiance

28. – *« C'est la liberté qui opprime et la règle qui soulage »... du rôle de l'Etat comme garant de la confiance*

Construire la confiance dans le commerce électronique n'est pas chose aisée. Nous l'avons montré : celle-ci ne peut être créée que par l'intervention de multiples tiers certificateurs.

Quelques réflexions nous paraissent s'imposer à ce propos.

a) La loi, en légiférant à propos de la signature électronique, ne résout que très partiellement le problème de la confiance. Rassurer sur l'identité de l'émetteur ou du destinataire et sur la confidentialité du message est certes essentiel mais ne peut suffire.

b) En ce qui concerne les autres éléments pour lesquels une certification est demandée, on insistera sur le fait que leur intervention n'aura de réel intérêt que si celle-ci entraîne une réelle responsabilité au cas où l'objet de la garantie fait défaut.

c) Traditionnellement, la garantie était assurée par l'intervention d'officiers publics (les notaires) voire de l'Administration. L'obligation de maîtriser la technologie et la tendance encouragée par les dirigeants européens au libre développement du marché aboutissent à abandonner les garanties traditionnelles (79)offertes par le statut public de l'émetteur de la garantie.

d) Une telle évolution conduit-elle l'Etat à laisser au seul marché le soin de créer, y compris par voie d'autoréglementation, la confiance réclamée par le public ? Il semble que non et ce pour deux raisons essentielles : le développement du commerce électronique répond à l'intérêt public tant économique que sociétaire. Toutefois, ce développement ne peut être atteint que par la confiance du public et dans la mesure où il respecte les éléments essentiels de la réglementation, protectrice des intérêts de ce public.

(79) La certification d'identité souvent réclamée pour des opérations à l'étranger était l'apanage des administrations communales ou des notaires.

e) A cet égard, l'intervention de l'Etat proposée par la proposition de loi belge sur la signature électronique est exemplaire. Le principe de la liberté, de la libre création des services de certification est assorti d'une réserve importante. Seule, l'intervention de prestataires « accrédités » dont la responsabilité est alourdie permettra de bénéficier des avantages légaux réservés à l'équivalent de la signature manuscrite. Ce qui est prôné là, peut l'être également, nous l'avons montré, pour d'autres éléments de la certification : l'archivage à propos duquel des normes devraient être établies pour définir les mesures organisationnelles et techniques de la conservation et de la reproduction de documents et où sans doute certaines entreprises pourraient faire l'objet d'accréditation; les techniques de certification d'un ou de plusieurs éléments de la transaction (la date, la qualité des contractants,...) pourraient être normalisées et à nouveau être confiées le cas échéant à des organismes accrédités. Quant à la labellisation, la loi la promeut et nul doute que l'arrêté royal à venir définira, pour l'obtention des avantages légaux prévus, que le système de labellisation réponde à des conditions de transparence, de conformité des critères de labellisation aux prescrits légaux et finalement d'effectivité du contrôle et des sanctions.

f) Au-delà, qu'il soit permis de suggérer que l'Etat joue un rôle précurseur en la matière. Que l'utilisation de signatures électroniques sûres soit encouragée lors de transactions avec l'Administration (80), que le site de l'Administration fasse l'objet d'une labellisation et enfin, que l'Etat mette sur pied des services de certification dans les relations entre administrations, voilà qui encouragera le secteur privé à recopier les modèles étatiques et à les diffuser de ce fait. Le commerce électronique a tout à gagner de cette synergie nouvelle entre Etat et secteur privé.

(80) Dans leur rapport, MM. de Leval, Godin et Mougenot (« Le Code judiciaire à l'épreuve du cyberespace : la nécessaire réforme », in *Le cyberavocat*, Formation permanente CUP, Liège-Namur, février 1999, Vol. XXIX, pp. 395 et s.) insistent sur l'intérêt de l'utilisation de messages électroniques dans les relations entre les avocats et le Palais et plaident pour une révolution du Code judiciaire à cet égard.

29. – *Confiance et attente légitime : là ou les concepts se rejoignent*

Les tiers de confiance tiennent leur pouvoir de la confiance dont ils sont investis. C'est pourquoi ces derniers se doivent d'offrir un produit répondant à l'attente légitime des utilisateurs. Que ce soit en matière de certification électronique ou de labellisation, cette attente légitime consiste à pouvoir disposer d'un produit informationnel (81) dans lequel les données sont exactes, complètes et mises à jour. La confiance, objet des « nouveaux métiers de la confiance » (82), illustre à merveille la tendance actuelle qui consiste à considérer la confiance suscitée chez le créancier comme fondement de la force obligatoire des contrats (83).

En cas de litige, il appartiendra au juge ou au tiers appelé à intervenir dans le cadre d'un « mode alternatif de résolution des litiges », de rechercher la volonté du tiers de confiance à travers les documents de promotion du produit : finalité, domaine couvert, garanties offertes, durée de validité, actualisation,... afin que puisse être déterminée la qualité du label ou du certificat auquel l'utilisateur pouvait légitimement s'attendre.

Notons à ce propos que si l'intervention d'un tiers par le biais d'un mode alternatif de résolution des litiges est elle aussi de nature à renforcer la confiance des internautes, il nous semble impératif que ce tiers soit un organisme indépendant, neutre par rapport aux parties. L'analyse des documents de promotion d'un label ou d'un certificat suppose une indépendance telle qu'un labellisateur ou un certificateur ne pourrait l'assurer (84).

(81) Voir à ce sujet E. MONTERO, *La responsabilité du fait des bases de données*, Travaux de la Faculté de Droit de Namur, P.U.N., 1998.

(82) M. ANTOINE, D. GOBERT, A. SALAÜN, *op. cit.*, pp. 3 à 32.

(83) X. DIEUX, *Le respect dû aux anticipations légitimes d'autrui. Essai sur la genèse d'un principe général de droit*, Bruxelles, Collection de la Faculté de droit de l'Université libre de Bruxelles, Bruxelles, Bruylant, 1995.

30. – *Le prix de la confiance*

Les tiers de confiance ne peuvent agir dans l'unique but de la recherche de leur profit. Leur activité consiste à offrir un produit répondant à l'attente légitime des utilisateurs. Dans ce contexte, les clauses limitatives ou exonératoires de responsabilité doivent être appréciées de façon circonstanciée. Tout d'abord, elles ne peuvent être opposables aux personnes qui se fient légitimement aux certificats et aux labels que si celles-ci en ont pris connaissance ou, à tout le moins, ont pu raisonnablement en prendre connaissance au plus tard au moment de la consultation du certificat (85) ou du label.

Ensuite, ces clauses ne peuvent « détruire l'objet du contrat » (86), en l'occurrence la confiance que les tiers entendent susciter. Serait considérée comme telle la clause par laquelle le tiers de confiance s'exonérerait de sa responsabilité du simple fait que la collecte des informations nécessaires à l'établissement d'un certificat ou à l'attribution d'un label, a été attribuée à un tiers. En effet, on peut considérer qu'en sa qualité de tiers de confiance, une obligation de vérification pèse sur lui.

L'objet de l'activité de ces nouveaux tiers tient donc en ces quelques mots : « susciter la confiance »... que des clauses relatives à la responsabilité ne pourraient anéantir...

(84) Voir à ce propos en matière de labellisation, le label WebTrader (http://www.budget-net.com/bnet/webtradersite/code_be.html) lancé par les associations de consommateurs et dédié à la protection des consommateurs. Le code de conduite prévoit, en son article 10, qu'en cas de litige, l'entreprise « labellisée » s'engage à « accepter l'intervention de l'organisation de consommateur qui a délivré le logo en vue de la résolution amiable et rapide des litiges impliquant des consommateurs ». Même si cet exemple illustre le cas d'un litige qui surviendrait entre un client et une entreprise, il soulève toutefois un malaise dans la mesure où le logo peut avoir été injustement attribué. Le tiers ayant attribué le logo et intervenant par ailleurs dans le cadre de la procédure prévue n'est pas suffisamment neutre par rapport aux parties et à l'enjeu du litige.

(85) Voir à ce propos l'article 6 de la directive du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *op. cit.*

(86) S. STIJNS, D. VAN GERVEN, P. WERY, « Chronique de jurisprudence : les obligations (1985-1995) », *J.T.*, 1996, p. 733.

31. – *Tiers de confiance, notaires du virtuel ?*

Le développement de communications sur Internet est de plus en plus conditionné par l'intervention de tiers, qu'ils soient prestataires de service de certification, labellisateurs,...

La mission qui leur est dévolue les rapproche des notaires. Ne sont-ils pas, tout comme les notaires, appelés à jouer le rôle d'« authentificateurs » ? Il y a là jeu de mots. Alors que les notaires sont appelés à authentifier les documents qui leur sont soumis en leur conférant une forme authentique, les tiers de confiance sont appelés à authentifier personnes et sites, c'est-à-dire à certifier qu'apparence et réalité se rencontrent. Ce jeu de mots à propos de la notion d'authentification ne pourrait toutefois cacher une réalité de moins en moins virtuelle.

Qui seront dès lors, demain, ces tiers de confiance, notaires du virtuel ?