Journal des tribunaux

14 septembre 2002
121e année - N° 6063

Bureau de dépôt : Charleroi X
Hebdomadaire, sauf juillet/août

Editeurs : LARCIER, rue des Minimes, 39 - 1000 BRUXELLES
Edmond Picard (1881-1900) - Léon Hennebicq (1901-1940) - Charles Van Reepinghen (1944-1966) - Jean Dal (1966-1981)

27 ISSN 0021-812X

Extrait du *Journal des tribunaux* n° 6063 du 14 septembre 2002 et reproduit avec l'aimable autorisation des Editions Larcier

LA SIGNATURE ÉLECTRONIQUE APRÈS LES LOIS DU 20 OCTOBRE 2000 ET DU 9 JUILLET 2001

Depuis peu, la signature électronique est devenue une réalité juridique en droit belge. Après avoir fait couler beaucoup d'encre en doctrine et mis à mal les concepts classiques d'écrit, de signature et d'original, la notion de signature électronique a finalement fait l'objet d'une réglementation nationale, sous l'égide du législateur européen. Et c'est par le biais du droit de la preuve que la réforme fut introduite. Néanmoins, de ces certitudes fraîchement acquises naissent de nouvelles interrogations quant à la portée et l'interprétation exacte des lois qui ont fait entrer le Code civil dans l'ère numérique.

I INTRODUCTION

L'avènement de ce qu'il est désormais convenu d'appeler la société de l'information constitue, à de nombreux égards, une révolution sans précédent, que certains n'hésitent pas à comparer à la révolution industrielle du dix-neuvième siècle. Une des manifestations les plus visibles de ce phénomène est l'émergence du commerce électronique. Bien qu'il n'ait pas pris, du moins en Europe, l'essor qu'on lui prédisait il y a à peine un an, il est indéniable que son expansion est considérable.

Cette nouvelle économie ne va cependant pas sans soulever de nombreux problèmes juridiques. Des contrats sont formés via les réseaux, des obligations naissent, et ce souvent entre personnes de nationalités différentes, soumises à des législations distinctes. Il y a rarement un contact physique entre les parties, le contrat étant conclu à distance, sans véritable support tangible. Le lien juridique se crée de manière dématérialisée là où précédemment un écrit « papier » le fixait irrévocablement. C'est donc presque naturellement au niveau de la preuve des obligations que les difficultés d'intégration des nouvelles technologies se sont cristallisées dans la matière du commerce électronique.

Face à ces incertitudes, et soucieuses de ne pas entraver le développement de ce nouveau marché si prometteur, les autorités ne sont pas restées inactives. Ainsi, après avoir rappelé brièvement les principes généraux de droit belge en matière de preuve [1] et présenté les bases tant théoriques [II] que techniques [III] sur lesquelles ont été établis les différents instruments législatifs, une attention particulière sera accordée aux normes européennes [IV] et aux lois belges concernant la signature électronique [V].

Loin d'être un exposé exhaustif sur une matière en permanente évolution et à propos de laquelle surgissent constamment de nouvelles interrogations, il s'agira ici seulement de familiariser le lecteur aux notions de base et d'attirer son attention sur quelques controverses d'actualité. En l'absence quasi totale de jurisprudence (1), nous renvoyons le lecteur à la très importante littérature consacrée à ce sujet (2).

(1) Voy. cependant en droit français la décision de la cour d'appel de Besançon du 20 octobre 2000, R.G., n° 99/0834, disponible sur le site http://www.legalis.net/legalnet.

(2) Pour ne citer que les plus récentes contributions voir E. Montéro, « Définition et effets juridiques de la signature électronique en droit belge : appréciation critique » *in* C.U.P., Formation permanente, *La preuve*, vol. 54, mars 2002, pp. 40 à 82; D. Gobert « Cadre juridique pour les signatures électroniques et les services de certification : analyse de la loi du 9 juillet 2001, *in* C.U.P., Formation permanente, *La preuve*, vol. 54, mars 2002, pp. 83 à 172; P. Lecocq et B. Vanbrabant, « La preuve du contrat par voie électronique : clap 2e », *Act. dr.*, 2002/2, à paraître; M.-E. Storme, « De invoering van de elektronische handtekening in ons bewijsrecht - Een inkadering van een commentaar bij de nieuwe wetsbepaling », *R.W.*, 9 juin 2001, n° 41, pp. 1505-1525; D. Gobert et E. Montéro, « La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle », *D.A.O.R.*, n° 53, pp. 17 à 39; D. Gobert et

SOMMAIRE

- La signature électronique après les lois du 20 octobre 2000 et du 9 juillet 2001, par L. Guinotte 553
- Prescription des créances à charge ou au profit de l'Etat - Prescription quinquennale - Absence d'effet interruptif d'un recours au Conseil d'Etat
  (Cour d'arbitrage, 20 février 2002, note) 562
- Impôt annuel voté par le collège juridictionnel de la Région de Bruxelles-capitale
  (Cass., 1re ch., 4 janvier 2002) 563
- Commerçants - Exécution de bonne foi des conventions - Exécution d'un contrat radicalement déséquilibré - Poursuite du respect de l'accord primitif - Abus de droit
  (Liège, 7e ch., 21 décembre 2001) 564
- Contrat conclu avec la Région de Bruxelles-capitale - Changement d'autorité responsable
  (Bruxelles, 2e ch., 31 mai 2001) 568
- Droit d'auteur - Reproduction publicitaire d'œuvres déjà autorisées
  (Civ. Bruxelles, 4e ch., 10 mai 2002) . 569
- Chronique judiciaire : Lettre ouverte au ministre de la Justice - Billet de la semaine - Colloques - Les deuils judiciaires - Coups de règle - Parallèlement... - Courrier des revues - Dates retenues.

1 EXPOSÉ DU PROBLÈME ET RAPPEL DE QUELQUES PRINCIPES GÉNÉRAUX EN MATIÈRE DE PREUVE DES OBLIGATIONS

Rien n'empêche, à l'heure actuelle, de conclure un contrat sur l'Internet pour autant qu'il s'agisse d'un contrat consensuel. De par la seule rencontre de volonté des parties, le contrat est formé et les obligations qui en découlent sont nées. Il n'en reste pas moins qu'un individu prudent souhaitera vraisemblablement se réserver une preuve efficace de l'existence du contrat et des dispositions qu'il contient, dans l'hypothèse où un litige devrait survenir ultérieurement. Or, l'article 1341 du Code civil impose le recours à l'écrit pour prouver toutes les choses (c'est-à-dire les actes juridiques) dépassant la somme de 375 €. C'est le problème de la recevabilité de la preuve. Par ailleurs, les articles 1319 et 1322 du Code civil déterminent la force probante qu'il convient d'accorder respectivement à l'acte authentique et à l'acte sous seing privé. Relativement au premier, l'article 1319 dispose que « L'acte authentique fait pleine foi de la convention qu'il renferme entre les parties contractantes et leurs héritiers ou ayants cause ». L'article 1322 réserve un statut moins privilégié à l'acte sous seing privé en ce que pour avoir force probante, il doit être reconnu ou légalement tenu pour tel par celui à qui on l'oppose. Le Code civil établit ainsi un système probatoire réglementé.

Si tel est le régime en droit civil, l'article 25, alinéa 1er, du Code de commerce dispose par contre, en matière commerciale, que « Indépendamment des moyens de preuve admis par le droit civil, les engagements commerciaux pourront être constatés par la preuve testimoniale, dans tous les cas où le tribunal croira devoir l'admettre, sauf les exceptions établies pour des cas particuliers ». Ainsi, bien que le régime légal subsiste, il se trouve considérablement assoupli. Non seulement l'admissibilité de la preuve, mais également sa force probante, sont laissées à l'appréciation du juge. Concrètement, il faut apporter au juge le maximum d'éléments susceptibles d'emporter sa conviction (3).

Ainsi, selon la qualité des parties au procès, l'administration de la preuve se fera selon le régime réglementé du Code civil à l'égard du non-commerçant et selon le système de preuve « libre » contre le commerçant. Ici donc, il n'y aurait en principe pas d'obstacles à ce qu'un consommateur puisse prouver par toutes voies de droit qu'un contrat électronique a bien été conclu entre lui-même et un commerçant. Ce dernier sera quant à lui fort démuni pour prouver l'existence du contrat et l'étendue des obligations qu'il contient selon les règles imposées par le Code civil. La problématique est évidemment identique entre deux parties non commerçantes.

En quoi cependant le système de la preuve réglementée et dans une moindre mesure celui de la preuve « libre » sont-elles concrètement un obstacle à la conclusion de contrats électroniques? Cela provient du fait que le Code civil, bien qu'il fasse référence aux concepts de « preuve littérale » (4), « d'acte » (5), « d'écrit » (6) et de « signature » (7) ne les définit pas. Il est cependant généralement admis que l'acte sous seing privé (8) se caractérise par un écrit et une signature. Et la signature a été définie de manière formaliste par la Cour de cassation comme étant « la marque manuscrite par laquelle le testateur révèle habituellement sa personnalité aux tiers » (9). Le terme « manuscrit » impose dès lors qu'il ne peut s'agir que d'une signature apposée sur un document papier.

Ainsi, si la conclusion d'un contrat consensuel sur le réseau est tout à fait réalisable, il pourrait être impossible pour les parties de prouver les droits et obligations qui en découlent, sauf si les parties ont préalablement conclu une convention sur la preuve, les dispositions du Code civil relatives à la preuve n'étant pas d'ordre public (10). Cette technique ne peut cependant être appliquée que dans un nombre limité d'hypothèses et n'est en tout cas pas adaptée au commerce électronique « grand public » où le consommateur occasionnel n'a pas conclu préalablement de convention relative à la manière dont la preuve du contrat pourra être rapportée en cas d'incident.

Face à cet obstacle, différentes solutions ont été proposées. On ne les mentionnera qu'à titre d'information : l'augmentation du seuil fixé par l'article 1341 du Code civil (11), l'adoption généralisée d'un système de preuve libre (12), ou encore l'introduction dans les articles 1347 et 1348 du Code civil de l'écrit électronique par voie d'exception (13). Aucune de ces voies n'a été suivie, probablement parce qu'elles n'apportaient que des solutions partielles à une problématique globale.

2 L'ÉLARGISSEMENT DES CONCEPTS ET LA THÉORIE DES ÉQUIVALENTS FONCTIONNELS

Une autre voie a été proposée, issue d'une réflexion approfondie sur les notions d'écrit et de signature, mais aussi d'original. Ainsi, concernant l'écrit, certains auteurs ont essayé, en se basant sur l'absence de définition légale de celui-ci, de proposer un concept extensif, permettant d'inclure non seulement l'écrit traditionnel mais aussi les documents électroniques. Classiquement, l'écrit est défini comme la représentation lisible du langage ou de la pensée au moyen de graphismes (14). Cette définition interdit de reconnaître la valeur d'écrit à un document électronique. Une conception plus récente se propose d'étendre la notion d'écrit à toute expression de langage par des signes connus ou traduisibles déposés sur un support quelconque (15). Cette définition, beaucoup plus large, assurerait la reconnaissance du document électronique.

Issue de cette réflexion sur les concepts eux-mêmes, c'est finalement la théorie dite des équivalents fonctionnels qui s'est imposée (16). Il s'agit de redéfinir les concepts par rapport aux fonctions essentielles qu'ils sont censés assurer. Selon cette théorie, tout procédé permettant de remplir ces fonctions doit se

E. Montéro, « L'ouverture de la preuve littérale aux écrits sous forme électronique », *J.T.*, 2001, pp. 114 et s.; Th. Verbiest et E. Wéry, avec la collaboration de A. Salaün et D. Gobert, *Le droit de l'internet et de la société de l'information - Droit européen, belge et français*, Collection Création-Information-Communication, Larcier, Bruxelles, 2001; R. Mougenot, *La preuve*, 3e éd. (mise à jour par D. Mougenot), Larcier, no 122, à paraître. Le lecteur trouvera dans ces contributions de très nombreuses références.

(3) C'est la nature de l'acte à prouver, commercial ou non, qui entraîne l'application du régime de la preuve « libre ». En pratique cependant, la qualité des parties est importante dans la mesure où, suivant l'article 2 du Code de commerce, toutes les obligations des commerçants sont présumées commerciales. Elle peuvent donc être prouvées librement, sauf si le commerçant établit que l'obligation en cause n'est pas commerciale. Si une convention est commerciale dans le chef d'une partie et civile dans le chef de l'autre, on parle alors d'acte mixte. Dans cette hypothèse, les deux régimes de preuve s'appliqueront cumulativement, chaque partie devant « combattre avec les armes de l'autre ». Les règles de la preuve civile devront ainsi être respectées par le commerçant, tandis que le non-commerçant pourra, par toutes voies de droit, prouver les obligations du commerçant. Voy O. Caprasse et A. Benoit-Moury, « Validité et force obligatoire des clauses contractuelles relatives à la preuve », *in* C.U.P., Formation permanente, *Droit de la preuve*, vol. XIX, oct. 1997, pp. 118 et 117.

(4) Art. 1316, C. civ.

(5) Art. 1322, 1341, C. civ.

(6) Art. 1344, 1345, C. civ.

(7) 7 Art. 1323, 1324, 1326, C. civ .

(8) Nous n'aborderons pas la notion d'acte authentique électronique dans le cadre de cette étude. Sur cette question, voy. notam. trois études publiées dans *Authenticité et informatique / Authenticiteit en informatica*, congrès de la Fédération royale du notariat belge, Bruxelles, 2000, Kluwer et Bruylant, 2000 : J.-L. Snyers, « De notariële certificatie en de elektronische authentieke akte », pp. 383 à 424; E. Montéro et A. Wallemacq, « La responsabilité du notaire comme auteur, récepteur ou utilisateur du document informatique », pp. 425 à 451; B. Vuylsteke, « *Cybernotary* », pp. 453 à 478;

(9) Cass., 7 janv. 1995, *Pas.*, 1995, I, p. 456; Cass., 2 oct. 1964, *Pas.*, 1965, I, p. 106. Dans un arrêt ultérieur, la Cour de cassation a précisé que : « la signature d'un acte sous seing prive doit, en règle, être tracée directement sur le document lui-même », Cass., 28 juin 1982, *Pas.*, 1982, I, 1286. Pour une analyse détaillée de la signature des actes sous seing privé, voy. M. Van Quickenborne, « Quelques réflexions sur la signature des actes sous seing privé », note sous Cass., 28 juin 1982, *R.C.J.B.*, 1985, pp. 57 et s.

(10) R. Mougenot, « La preuve », *in Rép. not.*, t. IV, liv. II, 1997, no 10.

(11) M. Fontaine considérait que cela constituerait « un ballon d'air frais bien salutaire », voy. M. Fontaine, « La preuve des actes juridiques et les techniques nouvelles », *in La preuve*, colloque U.C.L., 1987, p. 70.

(12) Comme c'est le cas aux Pays-Bas.

(13) Voy. sur ce point D. Mougenot, « Droit de la preuve et technologies nouvelles », *in* C.U.P., Formation permanente, *Droit de la preuve,* vol. XIX, oct. 1997, nos 37 et s.

(14) R. Mougenot, *op. cit.*, p. 127.

(15) M. Fontaine, *in La preuve*, colloque U.C.L., 1987, p. 9.

(16) Voy. sur ce point, notamm., au sujet de la signature électronique D. Gobert et E. Montéro, *D.A.O.R.* 2000, *op. cit.*, pp. 17 à 39, ainsi que les nombreuses références citées à la note 8.

voir reconnaître un statut équivalent. Nous examinerons successivement les notions d'écrit, de signature et d'original, analysées au travers de cette approche.

A. — **L'écrit** (17)

Trois fonctions essentielles de l'écrit ont ainsi pu être dégagées. Il s'agit de l'inaltérabilité, de la lisibilité et de la stabilité.

L'inaltérabilité : c'est la garantie que le document, une fois rédigé, ne sera plus modifié, intentionnellement ou non, que ce soit par une partie ou par un tiers. Dans un environnement papier, c'est le papier lui-même, à savoir le support, qui assure cette inaltérabilité. Au contraire, pour un document électronique, c'est le plus souvent la signature qui fournit cette garantie, la signature étant le résultat d'un traitement du contenu du document. Elle permet dès lors de détecter immédiatement une modification de l'information (18).

La lisibilité : sur un support papier, les informations sont directement lisibles puisqu'elles sont rédigées dans un langage (vocabulaire et grammaire) et dans une symbolique graphique (écriture) accessible à la compréhension humaine. Concernant l'écrit électronique, cette fonction requiert l'utilisation du matériel adéquat permettant de reproduire les informations de manière à ce qu'elles puissent être lues (un ordinateur et un logiciel). Il faut veiller à ce que, soit les informations subissent de fréquentes conversions afin que les nouveaux logiciels puissent les lire, soit les logiciels ayant servi à leur création soient préservés. Dans cette dernière hypothèse, les ordinateurs du futur devront également pouvoir utiliser ces anciens logiciels.

La stabilité : pour un document papier, c'est le support qui assure la stabilité de l'information. En effet le papier, et donc l'information qu'il contient, se détériore peu si des mesures adéquates sont prises pour sa conservation. En revanche, les supports électroniques ont une durée de vie bien inférieure au papier. Néanmoins, ce n'est pas le support en tant que tel qui doit être stable, mais bien l'information qui y est consignée. Cela n'empêche donc pas que l'information soit transférée sur un autre support, si son caractère original est préservé, ce que la signature électronique permet.

Ainsi, lorsque les moyens adéquats sont mis en œuvre pour garantir ces trois fonctions, on peut considérer que l'on se trouve bien en face d'un « écrit » au sens du Code civil (19). Il ne fait aucun doute qu'un document électronique peut remplir ces trois fonctions, parfois même avec un degré de sécurité bien supérieur au support papier.

On regrettera cependant que la notion d'écrit n'ait pas été définie clairement dans la loi, au contraire de la signature électronique (voy. *infra*). Cela a peut-être semblé superflu au législateur de définir cette notion dès lors que si l'on parle de signature électronique, cette dernière se rattache invariablement à un document électronique (20) (21). De nombreuses questions demeurent cependant et il aurait peut-être été opportun de saisir l'occasion de donner à l'écrit, quel qu'il soit, une définition claire (22). La question des fonctions de l'écrit, qu'il soit exigé *ad probationem* ou *ad validitatem* n'est pas encore résolue et ne peut être abordée ici tant la matière est complexe et nécessiterait des développements qui sortent de notre propos. Notons cependant l'article 17, § 2, de l'avant-projet de loi sur certains aspects juridiques des services de la société de l'information (23), qui propose de déclarer satisfaite l'exigence d'un écrit dans le cadre du « processus contractuel » par « une suite de signes intelligibles et accessibles pour être consultés ultérieurement, quels que soient leur support et leurs modalités de transmission ». L'intelligibilité et l'accessibilité pour consultation ultérieure semblent ici être devenus les fonctions déterminantes.

B. — **La signature**

Les fonctions de la signature sont, traditionnellement, doubles. Elle permet d'établir, d'une part, l'identité de l'auteur et, d'autre part, le consentement du signataire relativement au contenu de l'acte ou du message. En outre, une troisième fonction est également attribuée à la signature qui découle de l'usage du papier comme support de la signature : la combinaison de ces deux éléments assure le maintien de l'intégrité des informations que le document contient (24) (25). Tout procédé qui remplit ces fonctions doit en conséquence pouvoir accéder au statut de signature. Dans un document électronique, c'est la signature qui assure, via le maintien de l'intégrité de l'acte, la fonction d'inaltérabilité que l'on assigne à l'écrit.

C. — **L'original**

Nous aborderons brièvement la notion d'original. La différence entre l'original d'un acte sous seing privé et une copie de cet acte réside dans le fait que l'original porte la signature manuscrite. Sur la copie ne se trouve pas cette signature originale, manuscrite, directement apposée à la main, mais seulement la copie de celle-ci (26). Dans un environnement papier, la signature est apposée sur le support, le document papier. Ainsi une nouvelle signature est nécessaire pour tout nouvel original. Dans un contexte électronique au contraire, la signature n'est plus liée au support mais directement au contenu. La signature est en effet indépendante de son support et résulte généralement d'un traitement du contenu de l'acte. Le résultat de ce traitement permet non seulement de vérifier l'identité du signataire, mais également de contrôler si le contenu de l'acte n'a pas été modifié. La « copie » du contenu *et* de la signature du message sur un autre support n'affecte dès lors en rien le caractère original de l'acte.

On peut donc en conclure que la distinction faite par le Code civil entre l'original et la copie connaîtra certainement une application limitée dans l'environnement électronique.

2. LA SIGNATURE ÉLECTRONIQUE : QUELQUES CONSIDÉRATIONS TECHNIQUES

Le terme « signature électronique » recouvre divers mécanismes techniques qui permettent aux destinataires de données transmises par voie électronique de vérifier l'authenticité (27) et l'intégrité de celles-ci. On ne procède-

(17) A propos de cette notion, voy. les travaux préparatoires de la loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, *M.B.*, 22 déc. 2000, p. 42698 et plus particulièrement le rapport fait au nom de la Commission de la justice par M. Bart Somers, *Doc. parl.*, Chambre, 30 juin 2000, session ordinaire, n° 0038/008, pp. 24 à 31. Ci-après cité « rapport de la Commission de la justice ».

(18) Dès lors cette fonction appartient peut-être plus au concept de « signature » qu'à celui « d'écrit ».

(19) Le respect de ces trois fonctions est à mettre en relation avec la problématique de la conservation des documents électroniques. A propos de ce sujet, particulièrement vaste et complexe, voy. notam. le rapport établi par la commission « droit de la preuve » dans le cadre du projet e-justice (M. Antoine, D. Gobert, C. Lazaro et O. Leroux, sous la direction du professeur Y. Poullet, *Rapport final sur le droit de la preuve*, et plus particulièrement le chapitre II, disponible à l'adresse http://www.droit.fundp.ac.be/e-justice/default.htm).

(20) Notons cependant que la signature électronique peut également être utilisée pour garantir le contenu d'un site web ou certifier l'origine d'une information, identifier un ordinateur. Voy. sur ce point la note 31.

(21) Voy E. Montéro, *op. cit.*, n° 4.

(22) Voy. notam., D. Mougenot, « Faut-il insérer une définition de l'écrit dans le Code civil? », *Ubiquité*, 2000/7, pp. 121 à 128.

(23) Approuvé par le conseil des ministres du 29 novembre 2001. Pour un premier aperçu, voy. Th. Verbiest et E. Wéry, « Projet de loi belge sur le commerce électronique : première analyse », actualité du 13 mars 2002, disponible sur le site www.droit-technologie.org, à l'adresse http://www.droit-technologie.org/1_2.asp?actu_id=546

(24) 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.*, juill.-oct. 1998, n°s 4/5, p. 290. Voy. égalem., D. Gobert et E. Montéro, *D.A.O.R.*, *op. cit.*, n° 21.

(25) Cette affirmation est cependant controversée. Pour certains, la signature manuscrite ne remplit pas cette fonction, notamment si un document comporte plusieurs pages et ne comporte de signature que sur la dernière d'entre elles. De même, certaines signatures électroniques ne peuvent remplir cette fonction, comme par exemple la signature biométrique, à moins qu'elle ne comporte une fonction dite de « hachage », c'est-à-dire de transformation du document lui-même. Ainsi, s'il est vrai que le mécanisme de signature numérique fondé sur la cryptographie asymétrique, qui est le plus répandu à l'heure actuelle, assure cette fonction de maintien de l'intégrité, il n'en va pas nécessairement de même de certains autres types de signature électronique. Voy., R. Mougenot, *La preuve*, 3e éd. (mise à jour par D. Mougenot), Larcier, n°s 121-2 et 123 - C, à paraître. Voy. égalem., *infra*, le chapitre consacré aux considérations techniques.

(26) Comme nous l'avons déjà évoqué, la Cour de cassation a précisé que : « la signature d'un acte sous seing privé doit, en règle, être tracée directement sur le document lui-même », Cass., 28 juin 1982, *Pas.*, 1982, I, 1286.

(27) Le terme authenticité est souvent utilisé pour faire référence à la fonction d'identification de la si-

ra pas ici à un exposé détaillé des différents procédés de signature électronique existants, ni de leur mode de fonctionnement précis. Nous renvoyons le lecteur intéressé à l'importante doctrine consacrée à ce sujet (28). Seuls seront ici examinés sommairement les principes de base de la signature digitale à cryptographie asymétrique, qui est actuellement considérée comme un des systèmes les plus sûrs et surtout le plus répandu pour signer électroniquement.

Cette technique met en œuvre une relation triangulaire entre le signataire, le destinataire du message et une autorité de certification. Concrètement, celui qui souhaite signer électroniquement demande à l'autorité de certification de lui délivrer une clé privée (pour faire bref, il s'agit d'une formule mathématique), qui doit rester secrète et sous le contrôle exclusif du signataire. Dans le même temps, l'autorité de certification crée une clé publique complémentaire de la clé privée (29). Cette clé publique est, comme son nom l'indique, accessible à tout un chacun par l'organisation d'un système de publicité tel un annuaire. Elle est contenue dans un certificat qui établit explicitement le lien entre une personne déterminée et sa clé publique. Une fois ces démarches préalables effectuées, le signataire, s'il désire envoyer un message signé au destinataire, appliquera la clé privée au message. Il résultera de cette opération que le message sera crypté selon la formule mathématique que constitue la clé privée. Lors de la réception du message, le destinataire tentera de décrypter le message à l'aide de la clé publique de l'émetteur supposé du message. Si les deux clés correspondent, le message pourra être décrypté et le destinataire aura alors la certitude que le message a bien été signé par la clé privée de l'émetteur. Il aura dès lors l'assurance raisonnable que c'est bien l'auteur de l'acte lui-même qui a signé. La fonction d'identification de l'auteur du message est ainsi remplie. Si le décryptage échoue, cela signifie que le message n'a pas été signé avec la clé privée de l'auteur présumé.

La deuxième fonction, celle de l'adhésion de l'auteur au contenu de l'acte, intimement liée à la première, peut être présumée remplie dès l'instant où la vérification mentionnée ci-dessus est effectuée avec succès et que la clé privée de chiffrement a été appliquée volontairement par son propriétaire, à l'exclusion de tout procédé automatique de signature (30).

Enfin, la fonction du maintien de l'intégrité du contenu du document est quant à elle assurée par le cryptage à l'aide de la clé privée d'un condensé du message (obtenu à l'aide d'une fonction dite de « hachage irréversible » transmis avec le message en clair lui-même. En effet, ce que l'on appelle la signature électronique sera en fait le petit fichier contenant ce condensé du message crypté à l'aide la clé privée et transmis avec le message lui-même. Ce dernier ne sera généralement pas crypté, pour une évidente raison de rapidité : il est plus facile et plus rapide de crypter une petit fichier qu'un gros. Si après le décryptage de ce condensé à l'aide de la clé publique, et sa « décompression » à l'aide de la même fonction de « hachage », on constate une différence entre le document transmis en clair et le message décrypté et décompressé, c'est qu'il y a eu altération du message entre-temps. Si au contraire les versions sont identiques, on est assuré que l'intégrité du contenu du message a été préservée (31).

Par ailleurs, la signature digitale, qui est basée sur la technologie de la cryptographie, permet également d'envoyer des messages confidentiels. La démarche est ici inverse à celle suivie pour signer un message : l'auteur du message signe celui-ci à l'aide de la clé publique du destinataire, qu'il se sera procurée au préalable sur le registre contenant le certificat du destinataire. Lorsque ce dernier recevra le message, il devra faire usage de sa clé privée pour décrypter le message. En effet, tout message crypté avec une des deux clés ne peut être décrypté qu'avec l'autre. Le message ne pourra donc être lu que par le destinataire et personne d'autre. Rien n'empêche de surcroît l'auteur de l'acte de doubler l'opération de cryptage par l'utilisation du système de signature digitale. Il appliquera donc sa clé privée au message préalablement crypté à l'aide de la clé publique du destinataire. Ainsi, comme on le voit, la signature électronique permet également de garantir la confidentialité des communications électroniques. C'était la fonction première de la cryptographie (32).

Le rôle des autorités de certification apparaît donc fondamental. Ce sont elles qui en définitive seront les garantes de la bonne marche du système mis en place. Une de leurs tâches essentielles sera donc d'établir et de garantir le lien entre la clé publique contenue dans le certificat, qu'elles devront publier dans des registres, et la clé privée qui y correspond. Outre la clé publique, le certificat contiendra différentes informations relatives à l'identité de la personne qui en est titulaire, telles que son nom, son adresse, et toute autre information que le titulaire souhaitera voir figurer sur le certificat. Compte tenu de l'importance de leur mission, il était impératif que des mesures adéquates soient prises pour entourer leurs activités des garanties nécessaires à la fiabilité et à l'efficacité des opérations. C'est précisément l'objet de la directive européenne sur les signatures électroniques (33) et de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (34). Compte tenu de la complexité de cette matière (35), nous nous limiterons à l'examen des dispositions de ces textes relatives à la valeur juridique des signatures électroniques, en ce compris le nouvel alinéa 2 de l'article 1322 du Code civil, introduit par la loi du 20 octobre 2000 (36).

4 LES DIRECTIVES EUROPÉENNES SUR LES SIGNATURES ÉLECTRONIQUES ET LE COMMERCE ÉLECTRONIQUE

Le Conseil et le Parlement européen ont adopté le 13 décembre 1999 une directive relative à un cadre communautaire pour les signatures électroniques.

La plus grande partie de la directive est consacrée à régler le statut et les obligations des

gnature. Le choix de ce terme peut paraître inopportun en ce qu'il risque de créer une certaine confusion avec la notion d'authenticité au sens d'acte authentique, tel que prévu à l'article 1317 du Code civil.

(28) Pour un éventail des procédés existants et une analyse plus approfondie du fonctionnement de la signature digitale, voy. notamm. : P. Lecocq et B. Vanbrabant, *op. cit.*, n^os^ 30 à 43; D. Gobert, « La sécurisation des échanges par la reconnaissance de la signature électronique : conditions d'existence des réseaux d'avocats », *in* C.U.P., Formation permanente, *Multimédia, le cyberavocat*, vol. XXIX, févr. 1999, pp. 180 et 181; S. Parisien et P. Trudel, « L'identification et la certification dans le commerce électronique », Québec, Ed. Yvon Blais Inc., 1996, pp. 117 et s.; E. Davio, « Certification, signature et cryptographie », *in* E. Montéro (éd.), « Internet face au droit », *Cahiers du C.R.I.D.*, n° 12, E. Story-Scientia, 1997, pp. 80 et s., et du même auteur, « Preuve et certification sur internet », *R.D.C.*, 1997 n° 11, pp. 660 à 670; M. Antoine et D. Gobert, *R.G.D.C.*, *op. cit.*, n° 4/5, pp. 285-310; D. Gobert et E. Montéro, *D.A.O.R.*, *op. cit.*, n^os^ 10 à 26.

(29) Notons qu'il est impossible de déduire la clé privée du signataire à partir de la clé publique correspondante.

(30) Voy., R. Mougenot, *La preuve*, 3^e^ éd. (mise à jour par D. Mougenot), Larcier, n° 121-3, à paraître. Il faut également que la signature soit liée de manière logique au document, à défaut d'un lien (quasi) physique entre les deux, comme c'est le cas des écrits signés manuscritement. Cette exigence conduit la doctrine à considérer que la signature électronique suppose nécessairement une transformation de l'écrit (comme ici le cryptage du message). Voy. D. Gobert et E. Montéro, *D.A.O.R.*, *op. cit.*, n° 20; E. Montéro, *op. cit.*, n^os^ 34 à 36.

(31) Notons que les fonctions de la signature digitale décrites ci-dessus ne sont qu'une partie des applications que l'on peut en faire. Plus largement, la signature digitale permet de contrôler l'origine et l'intégrité de données électroniques, quelles qu'elles soient. Il peut donc s'agir de contrôler l'origine et l'intégrité d'un javascript, de vérifier l'authenticité d'une page web ou d'un site internet (voy. sur ce point J. Dumortier et P. Van Eecke, « De Europese ontwerprichtlijn over de digitale handtekening : waarom is het misgelopen? », *Computerrecht*, 1999/1, pp. 3 à 5).

(32) La méthode utilisée était alors la cryptographie dite symétrique, c'est-à-dire que la même clé servait à crypter et à décrypter les messages. Cependant, outre la lourdeur technique de ce procédé, seule la technique de la cryptographie asymétrique peut être utilisée à des fins de signature, en permettant d'identifier le signataire et de garantir le maintien de l'intégrité de l'acte.

(33) Directive européenne 1999/93/C.E. du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques, 13 déc. 1999 (*J.O.C.E.*, n° L 013, 19 janv. 2000, pp. 0012 à 0020).

(34) *M.B.*, 29 sept. 2001.

(35) Pour un examen de la directive et de la loi, voy. notam. M. Antoine et D. Gobert, « La directive européenne sur la signature électronique : vers la sécurisation des transactions sur l'Internet? », *J.T.D.E.*, 2000, n° 68, pp. 73 à 78; E. Caprioli, « La loi française sur la preuve et la signature électronique dans la perspective européenne », *J.C.P.*, 3 mai 2000, pp. 787 à 795. Sur la loi du 9 juillet 2001, voy. D. Gobert, C.U.P., *op. cit.* pp. 83 à 172.

(36) Loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, *M.B.*, 22 déc. 2000.

autorités de certification, qui seront chargées de délivrer des certificats de signatures électroniques. Comme nous venons de le voir, ces certificats permettront de garantir que la signature électronique apposée sur un document émane bien de la personne qui l'a apposée.

C'est à l'article 5 que l'on trouve les principes gouvernant les effets juridiques des signatures électroniques. Il faut ici distinguer deux régimes distincts.

Premièrement, l'article 5.1, qui ne concerne que les signatures électroniques qui répondent à certaines conditions (37), prévoit purement et simplement qu'elles auront la même valeur que les signatures manuscrites. Ce qui veut dire qu'elles doivent être admissibles comme preuve en justice et qu'elles doivent bénéficier de la force probante accordée aux signatures manuscrites. C'est ce qu'il est convenu d'appeler la *clause d'assimilation*. Cette reconnaissance pleine et entière de la signature électronique s'explique par les moyens techniques mis en œuvre pour sa création, qui assurent un haut degré de fiabilité.

Deuxièmement, l'article 5.2 traite des effets juridiques des signatures électroniques qui ne répondent pas à toutes les conditions fixées à l'article 5. 1. Pour ces signatures, il est prévu une *clause de non-discrimination*. Dans cette hypothèse, les Etats membres doivent veiller à ce que l'efficacité juridique *et* la recevabilité comme preuve en justice d'une signature électronique ne soient pas contestées 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 délivré par un prestataire de service accrédité, ou encore qu'elle n'est pas créée par un dispositif sécurisé de création de signature. Cet article consacre donc la recevabilité des signatures électroniques *lato sensu*. Pour faire bref, un juge ne pourra pas refuser un document dont l'une des partie prétend qu'il est signé électroniquement. Toutefois, à défaut de répondre aux spécifications de l'article 5. 1, il appartiendra à celui qui s'en prévaut de convaincre le juge qu'il s'agit bien d'une signature.

Cette directive envisage principalement, mais pas uniquement, la validité *ad probationem* de la signature électronique. Les effets de la signature électronique sur le plan probatoire sont réglés par la directive. Cela ressort de l'article 1er de la directive qui énonce que : « Elle (la directive) ne couvre pas les aspects liés à la conclusion et à la validité des contrats ou d'autres obligations légales lorsque des exigences d'ordre formel sont prescrites par la législation nationale ou communautaire; (...) ». Néanmoins, l'article 5.2, relatif à la clause de non-discrimination parle également de « l'efficacité juridique des signatures », de sorte que l'on ne peut parler d'une limitation du champ d'application au droit de la preuve. Ainsi, il est permis de penser que la validité de la signature *ad validitatem* est également visée (38). Cette interprétation de la directive peut en outre se fonder sur la formulation de l'article 1er de la directive qui prévoit que celle-ci ne couvre pas les aspects liés à la conclusion et à la validité des contrats lorsque des exigences d'ordre formel sont prescrites par la législation nationale ou communautaire. En effet, dès lors que la directive règle précisément le régime juridique applicable aux signatures électroniques, on peut en déduire que les exigences d'ordre formel dont question dans cet article visent d'autres conditions de forme que la signature.

L'article 9 de la directive européenne sur le commerce électronique (39), dispose quant à lui que : « Les Etats membres veillent à ce que leur système juridique rende possible la conclusion de contrats par voie électronique. Les Etats membres veillent notamment à ce que leur régime juridique applicable au processus contractuel ne fasse pas obstacle à l'utilisation des contrats électroniques ni ne conduise à priver d'effet et de validité juridique de tels contrats pour le motif qu'ils sont passés par voie électronique ». Suit alors une énumération de domaines pour lesquels il est permis aux Etats membres de conserver le régime actuel et d'écarter ces domaines de la réforme (art. 9.2) (40). Cet article semble pouvoir être interprété comme imposant de supprimer les obstacles à la conclusion électronique des contrats autres que ceux relatifs à la signature (41), puisque la directive sur les signatures électroniques règle déjà cette question, lorsqu'il fait référence à « l'efficacité juridique » des signatures électroniques. Signalons que la transposition de cette directive en droit belge est en cours (42).

5 LE DROIT BELGE

Le législateur belge a choisi de transposer la directive européenne sur les signatures électroniques au moyen de deux lois, soit la loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, qui ajoute, notamment, un alinéa 2 à l'article 1322 du Code civil et la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (que nous désignerons ci-après par loi P.S.C. pour loi relative aux prestataires de services de certification).

Nous n'aborderons pas les dispositions de la loi P.S.C. qui réglementent l'activité de ces derniers (43). Nous examinerons seulement les paragraphes 4 et 5 de l'article 4 [B] de cette loi ainsi que le nouvel article 1322 du Code civil [A], en examinant les rapports qu'entretiennent ces deux dispositions [C]. Signalons néanmoins que la loi affirme en son article 4, § 1er, le principe selon lequel nul ne peut être contraint de signer électroniquement. Il ne saurait en être autrement dès lors que l'utilisation de la signature électronique suppose un équipement technique dont tout le monde ne dispose pas.

A. — L'article 1322, alinéa 2, du Code civil

La loi du 20 octobre 2000 a introduit, entre autre, un alinéa 2 à l'article 1322 du Code civil. Il s'agissait pour le législateur de transposer la clause de non-discrimination contenue à l'article 5.2 de la directive européenne sur les signatures électroniques.

Celui-ci dispose que : « Peut satisfaire à l'exigence d'une signature [1], pour l'application du présent article [2], un ensemble de données électroniques [4] pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte [3] ».

1. — « *Peut satisfaire à l'exigence d'une signature* : le début de cet alinéa semble pouvoir être lu comme « satisfait à l'exigence d'une signature électronique... ». La formulation retenue est due au parcours législatif et aux amendements successifs dont a fait l'objet cet article (44). La problématique liée à

(37) Il s'agit, selon l'article 5 de la directive des « signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature ». Une *signature électronique avancée* est une signature qui satisfait aux exigences suivantes : *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; *d*) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable. Un *certificat qualifié* est un certificat qui satisfait aux exigences visées à l'annexe I de la directive et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II de la directive. Un *dispositif sécurisé de création de signature* est un dispositif de création de signature qui répond aux exigences prévues à l'annexe III de la directive.

(38) Pour l'utilisation des signatures dans le secteur public, voy le considérant n° 19 de la directive sur les signatures électroniques qui précise : « Les signatures électroniques seront utilisées dans le secteur public au sein des administrations nationales et communautaires et dans les communications entre lesdites administrations ainsi qu'avec les citoyens et les opérateurs économiques, par exemple dans le cadre des marchés publics, de la fiscalité, de la sécurité sociale, de la santé et du système judiciaire ».

(39) Directive 2000/31/C.E. du Parlement européen et du Conseil relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, du 8 juin 2000 (*J.O.C.E.*, n° L178, 17 juill. 2000, pp. 1 à 16).

(40) L'article 9.2 précise que certains contrats ne sont pas soumis à la réforme. Il s'agit 1) des contrats qui créent ou transfèrent des droits sur les biens immobiliers, à l'exception des droits de location; 2) les contrats pour lesquels la loi requiert l'intervention des tribunaux, des autorités publiques ou de professions exerçant une autorité publique; 3) les contrats de sûretés et de garanties fournis par des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale; 4) les contrats relevant du droit de la famille ou du droit des successions. Il ne s'agit bien évidemment que d'une possibilité accordée aux Etats membres, la liberté leur étant laissée d'aller au-delà de que ce que prévoit la directive.

(41) Tels que ceux liés au formalisme particulier de certains contrats où à l'opposabilité du contrat aux tiers.

(42) La directive devait être transposée dans le droit des Etats membres pour le 17 janvier 2002. Un avant-projet a été rédigé doit être déposé à la Chambre prochainement.

(43) Voy. sur cet aspect la récente étude de D. Gobert, C.U.P., *op. cit.*, pp. 83 à 172.

(44) Voy., en ce sens, P. Lecocq et B. Vanbrabant, *op. cit.*, n° 99 et la note 219 et E. Montéro, *op. cit.*,

cette interprétation sera développée au point B.

2. — *Pour l'application du présent article* : c'est-à-dire tant que d'autres formes ne sont pas prescrites par une législation spécifique. Cela ressort clairement du commentaire de l'article (45). Il s'agit de l'application du principe *lex specialis derogat lex generalis*. Cette législation spécifique peut provenir du Code civil lui-même (46) ou d'une réglementation spécifique (47). Ces quelques mots insérés dans le nouvel article 1322 du Code civil mettent en lumière le fait que le législateur belge n'envisageait ici que l'aspect probatoire de la signature électronique.

3. — *Pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte* : il s'agit ici de déterminer quelles sont les conditions que doit remplir la signature électronique pour être reconnue. En fait, il faut prouver que la signature électronique en est bien une. Il faudra non seulement démontrer l'imputabilité de la signature à une personne déterminée mais également que l'intégrité du contenu de l'acte a été sauvegardée. Sous le terme « imputabilité » sont comprises les fonctions d'identification et d'adhésion au contenu de l'acte (48). En bref, il faudra rapporter la preuve que le procédé de signature électronique identifie la personne dont il émane, manifeste son consentement au contenu de l'acte et qu'il garantit que l'acte n'a pas été modifié ou altéré lors du transfert de l'information. La définition fonctionnelle de la signature transparaît au travers de cet article.

4. — *Un ensemble de données électroniques* : les termes utilisés sont larges et ce dans un souci d'embrasser tout type de signature électronique. Par rapport au projet initial, on peut remarquer que l'on n'exige plus que cet ensemble de données électroniques doive résulter d'une transformation de l'écrit. Cela semble signifier que la signature ne doit plus être liée logiquement au message. Néanmoins, les définitions données dans la loi P.S.C. de la signature électronique et de la signature électronique avancée reprennent toutes deux cette exigence de lien logique entre le message et la signature (voy. art. 2, al. 2, 1° et 2°, L. P.S.C.) de sorte que cet « oubli » dans l'article 1322, alinéa 2, n'aura vraisemblablement pas de conséquences (49).

On remarquera que le principe de neutralité technologique apparaît *a priori* respecté dans la mesure où le texte est rédigé de manière fort large et ne fait explicitement référence à aucune technique particulière de signature électronique (50).

B. — **Les paragraphes 4 et 5 de l'article 4 de la loi du 9 juillet 2001**

1. — *L'article 4, § 4, énonce que* : « sans préjudice des articles 1323 et suivants du Code civil, une signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, est assimilée à une signature manuscrite, qu'elle soit réalisée par une personne physique ou morale ».

Cet article assure la transposition de la clause d'assimilation prévue à l'article 5.1 de la directive sur les signatures électroniques. Concrètement, les signatures électroniques qui répondront à ces conditions seront automatiquement considérées comme signatures.

La loi définit les notions de signature électronique avancée (art. 2, al. 2, 2°), de certificat qualifié (art. 2, al. 2, 4°), et de dispositif sécurisé de création de signature électronique (art. 2, al. 2, 7°), en renvoyant pour l'essentiel aux annexes I, II et III de la loi. Par commodité, ce type de signature sera désigné par le terme de « signature parfaite », emprunté à P. Lecocq et B. Vanbrabant (51).

On notera au passage que le paragraphe 4 prévoit explicitement la possibilité d'attribuer une signature à une personne morale, ce qui constitue une innovation, et ce même si les amendements qui ont été apportés au projet en cours d'adoption ont quelque peu diminué l'impact de cette modification (52).

Par ailleurs la loi prévoit un système d'accréditation libre pour les autorités de certification, conformément à la directive. En prenant un raccourci extrême, le principe de l'accréditation est le suivant : une autorité de certification ne peut être accréditée que si, après enquête, il a été démontré qu'elle est en mesure de proposer des signatures parfaites (53). Cette accréditation, une fois accordée, permet à l'autorité de certification de délivrer des signatures électroniques qui bénéficieront alors d'une « présomption » de perfection. Des contrôles ultérieurs sont possibles par l'autorité accréditante (en Belgique, le ministère des Affaires économiques). Il s'agit en quelque sorte d'un label de qualité délivré par l'administration. Ce régime d'accréditation est cependant libre, de sorte qu'il n'est pas obligatoire pour une autorité de certification d'être accréditée pour pouvoir délivrer des signatures parfaites. Néanmoins, les signatures délivrées par une autorité de certification accréditée bénéficieront *de facto* d'un avantage sur les autres dans la mesure où la seule preuve de l'accréditation de l'autorité de certification qui aura délivré la signature devrait suffire pour que le principe de l'assimilation s'applique. Pour les signatures délivrées par des autorités de certification non accréditées, la preuve du respect des exigences posées par les trois annexes de la loi devrait en principe être rapportée, même si en pratique, il est envisageable de limiter les éléments à vérifier (54).

Notons au passage que la personne à qui l'on impute une signature électronique, même parfaite, conserve la possibilité de ne pas reconnaître cette signature, conformément aux articles 1323 et suivants du Code civil. Indépendamment de l'adéquation peu évidente de l'article 4, § 4, de la loi P.S.C. avec les textes relatifs à la dénégation d'écriture et à son corollaire, la procédure en vérification d'écriture (art. 883 et s., C. jud.), on peut se poser la question de savoir s'il était opportun de laisser cette faculté au signataire présumé d'un document électronique. En effet, le degré de fiabilité offert par une telle signature est bien plus élevé que celui d'une signature manuscrite, aisée à contrefaire. En outre, la charge de la preuve appartiendrait alors à la personne qui tente d'imputer la signature à son auteur présumé, tâche ardue et malaisée dans le meilleur des cas. Signalons cependant que cette question n'est pas tranchée et que les

n° 23. Cette interprétation n'est cependant pas unanime. Voy égalem. les travaux préparatoires de la loi du 9 juillet 2001 (*Doc parl.*, Chambre, 50, 322/007, p. 4).

(45) Rapport de la Commission de la justice, p. 29.

(46) Ainsi l'article 970 du Code civil relatif au testament olographe prescrit que le testament doit être « écrit en entier, daté et signé de la main du testateur », ou encore l'article 1326 du même Code qui prévoit que dans le cas d'une convention unilatérale, l'acte sous seing privé doit être écrit de la main et celui qui s'engage ou que sa signature soit précédée de la mention manuscrite « bon pour » ou « approuvé ». On peut remarquer que relativement à ce dernier article, la loi française sur la signature électronique a remplacé les termes « de sa main » par « par lui-même » (art. 5), permettant dès lors l'usage de la signature électronique dans cette hypothèse. On relèvera également l'article 17, § 2, de l'avant-projet de loi belge sur le commerce électronique qui prévoit notamment que l'exigence d'une mention écrite de la main de celui qui s'oblige peut être satisfaite par tout procédé garantissant que la mention émane de ce dernier ».

(47) La Convention de Genève du 7 juin 1930 qui fixe les règles d'établissement d'un chèque, d'un billet à ordre ou d'une lettre de change, demeure inchangée. Il est donc actuellement impossible d'établir un chèque par voie électronique. De même, l'article 17 de la loi sur le crédit à la consommation, même s'il ne précise pas que la signature doit être manuscrite, prévoit néanmoins en son alinéa 2 que : « Le consommateur doit faire précéder sa signature de la mention manuscrite et en toutes lettres : " lu et approuvé pour ... francs à crédit. ". Il doit y apporter également la mention manuscrite de la date et de l'adresse précise de la signature du contrat. »

(48) Rapport de la Commission de la justice p. 30 et justification de l'amendement n° 12 à ladite proposition de loi (*Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 38/006).

(49) Voy sur ce point les réflexions émises par E. Montéro, *op. cit.*, n° 35.

(50) Même s'il ne fait aucun doute sur le fait que ce soit la technique de la cryptographie asymétrique qui ait été prise comme modèle technologique pour la rédaction du texte.

(51) P. Lecocq et B. Vanbrabant, *op. cit.*, n° 80, et la note 185. M.-E. Storme désigne quant à lui ce type de signature par les termes « gekwalificeerde elektronische handtekening », M.-E. Storme, *op. cit.*, n° 37, tandis qu'E. Montéro adopte la dénomination de « signature électronique qualifiée », E. Montéro, *op. cit.*, n° 6, note 11.

(52) Sur la signature électronique des personnes morales, voy. B. Vanbrabant, « La signature électronique des personnes morales », *in* C.U.P., Formation permanente, *La preuve*, vol. 54, mars 2002, pp. 173 à 228.

(53) L'accréditation suppose en effet que le prestataire de services de certification ait satisfait aux exigences de l'annexe II, que ses certificats soient conformes à l'annexe I et que les dispositifs de création de signature utilisés répondent à l'annexe III (art. 17, § 1er, de la loi). Bien que parmi ces exigences ne figure pas celle que la signature électronique soit avancée, on conviendra avec P. Lecocq et B. Vanbrabant que si les exigences des annexes I, II et III sont rencontrées, la signature qui sera créée sera nécessairement avancée (P. Lecocq et B. Vanbrabant, *op. cit.*, n° 106 et la note 236.)

(54) P. Lecocq et B. Vanbrabant, *op. cit.*, n° 107.

auteurs divergent quant à « qui » devra prouver ou à ce qu'il faudra prouver (55). Une partie de la doctrine (56) précise cependant que dans l'hypothèse où le signataire contesterait avec succès sa signature, celui-ci n'en resterait pas moins tenu d'indemniser l'autre partie sur la base de la responsabilité aquilienne. Les paragraphes 1er et 2 de l'article 19 de la loi P.S.C. précisent en effet en substance que le titulaire d'une signature électronique est responsable de la confidentialité de la clé privée (§ 1er) (57). Si un doute naît quant à cette confidentialité, il appartient donc au titulaire de faire révoquer le certificat (§ 2) (58). A défaut pour lui de le faire, il engagerait sa responsabilité extracontractuelle à l'égard de la partie qui se prévaut de la signature, puisqu'il n'a pas pris les mesures nécessaires pour « bloquer » sa signature électronique en sachant que celle-ci n'était plus sous son seul contrôle. Le dommage serait alors pour l'autre partie la non-conclusion du contrat (59). La seule possibilité pour le signataire d'éviter une quelconque part de responsabilité serait de démontrer que sa signature électronique a été « piratée » et utilisée à son insu, situation qui risque de se présenter rarement en pratique et dont la preuve risque d'être impossible à rapporter (60). Cette question est d'importance puisqu'un régime trop strict pourrait constituer un frein important au développement de la confiance tant recherchée, que la réglementation sur la signature électronique devait promouvoir.

2. — *Le paragraphe 5 de l'article 4 dispose quant à lui* : « Une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice 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 ».

Il s'agit de la transcription littérale de l'article 5.2 de la directive européenne sur les signatures électroniques, relatif à la clause de non-discrimination. Ce paragraphe a été ajouté au projet de loi à la fin de son parcours législatif, afin d'assurer la transposition la plus complète possible de la directive. Le législateur souhaitait en effet réaliser « l'équivalence absolue entre la signature électronique et la signature manuscrite, tant pour les procédures judiciaires qu'extrajudiciaires » (61). Cet ajout ainsi que sa place dans cette loi, peuvent sembler surprenants dès lors que la clause de non-discrimination faisait en principe déjà l'objet d'une transposition via l'article 1322, alinéa 2 nouveau, du Code civil. Cela tient probablement au fait que le législateur considérait que l'assimilation de la signature électronique à la signature manuscrite telle que prévue par l'article 1322, alinéa 2, n'était que facultative (62). Nous avons cependant précisé que si la formulation de cet article laisse supposer une simple faculté de reconnaissance d'une signature électronique, l'analyse de la gestation législative du texte ouvre la porte à une interprétation selon laquelle la reconnaissance doit être acquise pour autant que les conditions énumérées dans cet article soient remplies (voy. pt A 1.). Quoi qu'il en soit, l'ajout de ce paragraphe 5 n'est pas sans conséquence, comme nous le verrons par la suite.

De manière claire, comme déjà évoqué ci-dessus lors de l'analyse de l'article 5.2 de la directive, la loi interdit donc *notamment* de déclarer irrecevable comme preuve en justice un document dont une partie prétend qu'il est signé électroniquement pour le seul motif que la signature est électronique. Notons cependant qu'il est toujours possible de considérer comme irrecevable une signature électronique (ou plutôt le document que l'on souhaite produire à titre de preuve sur laquelle elle est apposée) pour d'autres motifs que ceux énoncés dans cet article, par exemple le fait que la signature ne serait pas avancée. Cet article vise donc toutes les signatures qui ne sont pas parfaites, c'est-à-dire les signatures « simples », « avancées » et « avancées avec certificat qualifié ». Si les deux dernières doivent être déclarées recevables (la première pouvant l'être), il appartient cependant à celui qui s'en prévaut de démontrer qu'il s'agit bien d'une signature électronique.

Certains auteurs (63) ont précisé que dans les hypothèses visées par l'article 5.2 de la directive (et donc de l'article 4, § 5, de la loi), une fois la signature électronique déclarée recevable, le juge était libre de lui accorder force probante ou non en fonction des éléments qui lui étaient soumis, au contraire du système prévu par l'article 5.1 de la directive (ou 4, § 4, de la loi), où le juge *devait* accorder force probante à la signature parfaite, conséquence logique de son assimilation à la signature manuscrite. Cette interprétation se base notamment sur les travaux préparatoires de la loi P.S.C. (64) et sur la formulation actuelle de l'article 1322, alinéa 2 (65). On remarquera cependant que la distinction entre recevabilité et force probante de la signature électronique dans le cadre de la clause de non-discrimination peut paraître quelque peu artificielle. En effet, en vertu de l'article 1322, alinéa 2 nouveau, du Code civil, dès lors qu'un mécanisme technique que l'on prétend être une signature électronique assure les fonctions d'imputabilité et d'intégrité prévues par ce texte, il faut considérer que l'on est bien en face d'une signature, et partant d'un acte sous seing privé (en partant du principe que les mots « peut satisfaire » se lisent comme « satisfait »). Le rôle du juge se limiterait en conséquence à vérifier « simplement » si ces deux fonctions sont remplies. Soit elles ne le sont pas et le juge doit déclarer le document électronique irrecevable, soit elles le sont et le juge doit déclarer le document recevable et, partant, lui accorder force probante, puisqu'il s'agit d'un écrit signé (sous réserve de la dénégation d'écriture). Il s'agit, pour reprendre l'expression de P. Lecocq et B. Vanbrabant, d'une règle du tout ou rien (66). Du reste, en décider

(55) Voy. sur cette question P. Lecocq et B. Vanbrabant, *op. cit.*, nos 109 à 112; D. Gobert et E. Montéro, *J.T.*, *op. cit.*, pp. 114 et s., estiment quant à eux qu'une signature parfaite bénéficie d'une présomption réfragable selon laquelle les fonctions d'imputabilité et d'intégrité sont remplies. Selon ces auteurs : « un signataire peut toujours, comme pour la signature manuscrite, contester sa signature puisque la présomption est réfragable, avec néanmoins la différence fondamentale qu'il ne lui suffit plus de désavouer sa signature mais qu'il doit renverser la présomption »; R. de Corte, « Elektronische handtekening en de identificatie in de virtuele wereld », 11 juill. 2001, non publié; de manière plus nuancée, voy E. Montéro, *op. cit.*, p. 46.

(56) E. Montéro, *op. cit.*, nos 43 à 45; R. Mougenot, *La preuve*, 3e éd. (mise à jour par D. Mougenot), Larcier, no 158, à paraître; D. Gobert, C.U.P., *op. cit.*, pp. 153 à 158.

(57) Le paragraphe 1er énonce : « Dès le moment de la création des données afférentes à la création de signature, le titulaire du certificat est seul responsable de la confidentialité de ces données ».

(58) Le paragraphe 2 énonce quant à lui : « En cas de doute quant au maintien de la confidentialité des données afférentes à la création de signature ou de perte de conformité à la réalité des informations contenues dans le certificat, le titulaire est tenu de faire révoquer le certificat ».

(59) Qui ne s'identifie cependant pas nécessairement au dommage qui aurait été considéré contractuel si le désaveu de signature n'avait pas abouti avec succès.

(60) Comp., D. Gobert, *op. cit.*, p. 155.

(61) Voy. les travaux préparatoires de la loi du 9 juillet 2001, *Doc. parl.*, Chambre, 50, 322/7, p. 4.

(62) Voy. les travaux préparatoires de la loi du 9 juillet 2001, *Doc. parl.*, Chambre, 50, 322/7, p. 4, ainsi que *Doc. parl.*, Sén. 2-662/3, sess. ord. 00/01.

(63) D. Gobert et E. Montéro, « La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle », *op. cit.* no 55; D. Gobert et E. Montéro, « L'ouverture de la preuve littérale aux écrits sous forme électronique », *op. cit.*, pp. 119 et 120; D. Gobert, « Belgique : projet de loi " signature électronique " déposé à la Chambre », actualité du 11 février 2000, disponible sur http://www.droit-technologie.org; Th. Verbiest et E. Wéry, avec la collaboration de A. Salaün et D. Gobert, *Le droit de l'internet et de la société de l'information, droit européen, belge et français*, Collection Création-Information-Communication, Larcier, Bruxelles, 2001, nos 667 et 668.

(64) Voy *Doc. parl.*, Ch., 50 322/001, sess. ord. 99/00, p. 13 : « Pour résumer le lien entre les deux projets de loi, on peut dire que le projet relatif aux autorités de certification accorde force probante aux signatures électroniques avancées créées par un dispositif sécurisé de création de signature et combinées à un certificat qualifié. Ces signatures bénéficient des mêmes effets juridiques que ceux qui sont reconnus aux signatures manuscrites (...) Par contre, le projet relatif au droit de la preuve se limite à créer le principe de la recevabilité de tout type de signature, même électronique, le juge étant alors libre d'apprécier la valeur probante à accorder à celle-ci (il pourrait très bien accorder une valeur probante équivalente à celle de la signature manuscrite s'il estime que les différentes fonctions de la signature sont réalisées avec une certitude raisonnable) ».

(65) Cette interprétation est en effet confortée par le choix par le législateur des termes « peut satisfaire à l'exigence d'une signature... » de l'article 1322, alinéa 2, du Code civil. Nous avons néanmoins signalé au point A que cette formulation pouvait se lire comme « satisfait », de sorte que le pouvoir d'appréciation qui semble être laissé au juge sur ce point est inexistant.

(66) P. Lecocq et B. Vanbrabant, « La preuve du contrat par voie électronique », *in Le commerce électronique : un nouveau mode de contracter*, actes du colloque organisé par la Faculté de droit de Liège (Unité de droit privé) et la Conférence libre du Jeune barreau de Liège le 19 avril 2001, a.s.b.l. Editions du Jeune barreau de Liège, 2001, *op. cit.*, nos 96 et 99

autrement reviendrait à créer une distorsion juridique sérieuse et non justifiée entre le régime de la signature manuscrite et celui de la signature électronique, puisque dans l'environnement « papier » le juge ne peut pas déclarer un acte sous seing privé recevable et lui dénier ensuite toute force probante (67). Cependant, la controverse existante en doctrine sur cette question n'est peut-être qu'une querelle de mots, dans la mesure où les thèses en présence reconnaissent toutes deux au juge un pouvoir d'appréciation, mais à des stades distincts. Fondamentalement, il s'agira toujours de démontrer à celui-ci que le procédé technique utilisé est bien une signature et qu'il doit se voir attribuer les mêmes effets. Il n'est donc pas impossible que l'impact de la controverse soit limité dans la pratique quotidienne de la matière.

Une autre conséquence non négligeable provient du libellé de l'article 4, § 5 et de la suppression dans l'article 4, § 4, de la référence à l'article 1322 (référence qui existait jusqu'à l'amendement du texte par le Sénat). D'une part, l'article 4, § 5, parle de la recevabilité de la signature électronique en justice et de l'efficacité juridique des signatures électroniques et, d'autre part, l'article 4, § 4, s'est affranchi de son lien avec l'article 1322 du Code civil, qui semblait le cantonner au domaine de la preuve (68). Ceci tend à démontrer que tant la clause d'assimilation que la clause de non-discrimination, transposées en droit belge, ne concernent pas uniquement le droit de la preuve mais doivent être appliquées à chaque fois que le terme « signature » apparaît dans une norme juridique. Ces deux clauses ont donc une portée générale en droit belge, ce qui a pour conséquence qu'il ne sera théoriquement pas nécessaire de modifier tous les textes où le mot « signature » apparaît, en y mentionnant que la signature électronique est aussi acceptée. A titre d'exemple, l'article 1034*ter*, 6°, du Code judiciaire, qui prévoit que la requête doit être signée par le requérant ou son avocat à peine de nullité, ne devra en principe pas être modifié pour permettre aux avocats de signer électroniquement une requête. Cette interprétation large (69) n'est pas retenue par une partie de la doctrine (70), mais ressort clairement du considérant 19 de la directive sur les signatures électroniques et d'une partie de l'exposé des motifs de la loi P.S.C. (71). Elle est également confirmée par la formulation actuelle des paragraphes 4 et 5 de l'article 4 de la loi. Enfin, et la précision est d'importance, l'article 17 de l'avant-projet de loi sur certains aspects juridiques des services de la société de l'information confirme selon nous de manière non équivoque cette solution. Cet article précise en effet que :

« § 1er. Toute exigence légale ou réglementaire de forme relative au processus contractuel est réputée satisfaite à l'égard d'un contrat par voie électronique lorsque les qualités fonctionnelles de cette exigence sont préservées.

» § 2. Pour l'application du paragraphe 1er, il y a lieu de considérer :

» . . . . . .

» que l'exigence, expresse ou tacite, d'une siqnature est satisfaite dans les conditions revues soit à l'article 1322, alinéa 2, du Code civil, soit à l'article 4, § 4, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ».

Il est donc ici fait expressément référence aux articles 1322, alinéa 2, du Code civil et 4, § 4, de la loi P.S.C. pour définir ce qu'il faut ou non considérer comme une signature, en dehors du strict domaine de la preuve. Bien qu'il ne s'agisse que d'un avant-projet, et que celui-ci ne vise que « le processus contractuel », il peut s'en déduire que ces articles constituent le socle juridique sur lequel s'appuie la notion juridique de signature électronique, quel que soit le rôle ou le domaine dans lequel celle-ci est envisagée. Du reste, pourquoi faudrait-il aller chercher ailleurs une définition déjà complète de la signature (surtout au regard des annexes de la loi P.S.C.)? Une multiplication des définitions ne ferait qu'accroître les difficultés d'application d'une législation déjà fort complexe.

C. — L'articulation des articles 1322 du Code civil et 4, §§ 4 et 5, de la loi du 9 juillet 2001

La question ne se pose pas vraiment pour les « signatures parfaites », dont le statut est réglé par l'article 4, § 4, de la loi, soit la clause d'assimilation pure et simple, qui ne laisse subsister aucun doute quant aux conditions à remplir pour ce type de signature et quant aux effets à leur accorder, que l'on envisage ou non la signature sous l'aspect probatoire.

Au contraire, pour les signatures « non parfaites », il semble *a priori* que deux dispositions concurrentes soient applicables : l'article 1322, alinéa 2, du Code civil et l'article 4, § 5, de la loi du 9 juillet 2001. Nous avons déjà précisé que la clause de non-discrimination devait initialement être transposée par l'article 1322, alinéa 2, du Code civil. Celui-ci va cependant plus loin qu'une simple expression d'un principe de non-discrimination des signatures électroniques. Il traduit dans un texte législatif la définition fonctionnelle de la signature et énonce des règles plus strictes que l'article 5.2. de la directive, soit les fonctions que doit remplir la signature, conditions que ne contient pas l'article 5.2. de la directive. Il s'agit probablement de la raison principale pour laquelle un paragraphe 5 a été ajouté à l'article 4 de la loi du 9 juillet 2001, reprenant fidèlement le texte même de la directive (72). Néanmoins, cet ajout est venu perturber l'attribution des rôles respectifs que l'on reconnaissait traditionnellement à l'article 1322, alinéa 2, du Code civil (clause de non-discrimination) et l'article 4, § 4, de la loi du 9 juillet 2001 (clause d'assimilation).

L'agencement de ces deux dispositions peut selon nous être résumé comme suit : si l'article 4, § 5, contient de manière certaine les principes de la recevabilité et de l'efficacité des signatures électroniques, il ne détermine pas les conditions ni les critères qui doivent être rencontrés pour qu'un procédé technique déterminé puisse accéder au rang de signature. Il faut pour cela s'en référer au contenu de l'article 1322, alinéa 2, du Code civil, et au besoin, au contenu des annexes de la loi P.S.C. Il peut donc s'en déduire qu'une signature non parfaite sera considérée comme une signature par une application combinée des articles 4, § 5, de la loi P.S.C. et 1322, alinéa 2, du Code civil. Dans le domaine probatoire *sensu stricto* cependant, l'article 1322, alinéa 2, se suffit à lui même (73). Il n'est en effet pas nécessaire de faire le détour par l'article 4, § 5, de la loi P.S.C. pour trouver l'expression du principe de la recevabilité des signatures électroniques comme preuve en justice, puisque l'article 1322 le contient déjà. Cet article était en effet déjà en vigueur avant l'adoption de l'article 4, § 5, de la loi P.S.C., sans qu'il ait été contesté que le principe de recevabilité était bien concrétisé par cette disposition (74). Du reste, il nous semble plus

(voy. égalem. les mêmes auteurs, *op. cit.*, nos 96 et 99); En ce sens égalem. E. Montéro, *op. cit.*, no 23.

(67) Toujours sous réserve de la dénégation d'écriture.

(68) Signalons cependant que l'article 4, § 4, fait toujours référence aux articles 1323 et suivants, de sorte que la « filiation » de la matière avec le droit de la preuve subsiste.

(69) Voy. en ce sens E. Montéro, *op. cit.*, nos 17 et 18. Voy. égalem. P. Lecocq et B. Vanbrabant, *op. cit.*, nos 81, 88 et 116 à 119 s'appuyant sur le principe d'interprétation conforme du droit national par rapport au doit communautaire.

(70) Voy. notam., M. Antoine et D. Gobert, *J.T.D.E.*, 2000, *op. cit.*, pp. 73 et s., no 14; D. Gobert et E. Montéro, *J.T.*, 2001, *op. cit.*, p. 116; comp. l'opinion de D. Mougenot dans R. Mougenot, *La preuve*, 3e éd. (mise à jour par D. Mougenot), Larcier, no 122-3, *in fine*, à paraître.

(71) *Doc. parl.*, Ch. repr. Doc. 50, no 322/007, pp. 3 et 4.

(72) Sur ce point, voy. E. Montéro, *op. cit.*, nos 19 et 20 et les différentes notes citées par l'auteur sous ces numéros.

(73) En ce sens, P. Lecocq et B. Vanbrabant, *op. cit.*, no 117; comp. R. De Corte, *op. cit.*, nos 102 et 103;

(74) Comp. Y. Poullet et M. Antoine, « Vers la confiance ou comment assurer le développement du commerce électronique », *in Authenticité et infor-*