La sécurisation des échanges par la reconnaissance de la signature électronique

Gobert, Didier

Published in:
Multimédia : Le cyberavocat

Publication date:
1999

Document Version
le PDF de l'éditeur

LA SECURISATION DES ECHANGES PAR LA RECONNAISSANCE DE LA SIGNATURE ELECTRONIQUE : CONDITION D'EXISTENCE DES RESEAUX D'AVOCATS

Didier Gobert

(publié dans *Multimédia : Le cyberavocat*, Formation permanente CUP, Volume XXIX, Liège-Namur, février 1999, pp. 163-191.)

INTRODUCTION

Dans le monde et notamment dans notre pays, de plus en plus d'actes juridiques sont accomplis par voie électronique. Les technologies de l'informatique et des télécommunications créent, tant dans le secteur privé que dans le secteur public, des possibilités permettant de travailler plus vite et plus efficacement. Des contrats peuvent être établis au moyen d'un ordinateur et ensuite être transmis pour approbation au contractant par le biais de réseaux, après quoi ils pourront être stockés sous une forme électronique. Ils occuperont ainsi un espace d'archivage moins important et pourront être consultés plus rapidement.

Il est vrai que le monde des affaires a déjà intégré depuis un certain temps des systèmes télématiques permettant d'effectuer automatiquement certaines transactions juridiques, appelés EDI (Electronic Data Interchange). Le monde bancaire a également mis en place un réseau interbancaire, Isabel, qui permet notamment aux clients d'effectuer des transactions bancaires par voie électronique et de communiquer avec d'autres utilisateurs du réseau Isabel. Mais il s'agit ici de réseaux fermés, fortement sécurisés, dont les utilisateurs sont préalablement et physiquement identifiés et surtout dans lesquels les parties ont l'occasion de se rencontrer auparavant pour signer un contrat papier en vue notamment de fixer le régime juridique qui s'appliquera aux transactions futures. Avec les nouvelles applications, cette rencontre préalable est de moins en moins possible. En effet, elle s'envisage difficilement lorsque l'on ne passe une transaction avec un commerçant que de manière sporadique. Elle s'envisage encore moins lorsque la transaction s'effectue par le biais d'un réseau ouvert, tel Internet, dont l'intérêt est justement de pouvoir communiquer rapidement et à distance, sans rencontre physique préalable. Or, ces transactions sont de plus en plus fréquentes : il est possible de réserver des voyages, de commander des livres, des vêtements, des logiciels, voire des voitures et des actions par le biais d'Internet. D'une manière plus prospective, de nombreuses consultances pourraient également s'opérer par le réseau. Sur le plan administratif, un particulier ou une entreprise peuvent être intéressés par l'envoi de leur déclaration au bureau des contributions par un moyen électronique. Il en est de même pour les déclarations à envoyer à l'ONSS[1], et d'une manière générale, pour tout type de relation avec

[1] Dès à présent, les entreprises des secteurs de la construction et du transport doivent, sauf dérogation, effectuer leurs déclarations immédiates d'emploi par voie électronique (AR du 22 février 1998 « instaurant une déclaration immédiate de l'emploi, 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.*, 18 mars 1998). Pour ce faire, l'Arrêté Royal du 16 octobre 1998 (« portant des dispositions 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) met en place un système provisoire de signature électronique pour la sécurité sociale, et

l'administration (introduction du permis d'urbanisme, demande d'autorisations diverses, …). Plus particulièrement, l'avocat ne rechignera pas à pouvoir envoyer ses conclusions à la partie adverse et au greffe par un moyen électronique qui est techniquement et juridiquement fiable. De même, il comprendra vite les avantages notables que procure la possibilité d'introduire un recours par voie électronique, surtout quand il y a urgence. Enfin, on peut s'attendre dans un avenir proche à ce que des contrats soient négociés voire conclus par un système de vidéoconférence et donc par voie électronique.

Ces différentes transactions restent cependant limitées voire empêchées en raison de certains obstacles juridiques. De nombreux Etats ont pris conscience que la législation s'appliquant par défaut, c'est-à-dire en l'absence de convention contraire, constitue parfois un frein au développement de transactions électroniques. Il est par exemple encore difficile, voire impossible, de prouver un grand nombre d'actes juridiques passés par voie électronique car la plupart des juges exigent toujours un écrit papier signé manuscritement. Le 12 juin 1998, le Conseil des ministres adoptait en première lecture deux avant-projets de loi[2] en vue de mettre fin à l'incertitude juridique néfaste au développement des communications électroniques : l'un visant à « modifier certaines dispositions du Code civil relatives à la preuve des obligations », l'autre relatif à « l'activité d'autorités de certification agréées en vue de l'utilisation de signatures digitales ». Notons que cette intervention législative n'est pas propre à la Belgique. L'Allemagne[3] et l'Italie[4] ont déjà adopté une loi dans ce domaine. Des projets de loi comparables sont en préparation dans d'autres Etats Membres (Pays-Bas, Autriche, Luxembourg, Danemark, France)[5]. La question est également prise très au sérieux aux niveaux européen et international. En effet, la Commission européenne a présenté le 16 juin 1998 une proposition de directive sur un cadre commun pour les signatures électroniques[6] et la Commission des Nations Unies pour le Droit Commercial International (CNUDCI) travaille sur l'élaboration de règles uniformes pour les signatures électroniques[7].

Dans une première partie, nous traiterons du problème de la reconnaissance juridique de la signature électronique ainsi que des solutions possibles et présenterons les deux avant-projets de loi belges en préparation, sans négliger les aspects de droit comparé. Dans une deuxième partie, nous envisagerons la question de la signature électronique dans une perspective européenne et internationale et présenterons brièvement la proposition de directive européenne en ce domaine ainsi que les travaux qui sont réalisés au sein de la CNUDCI.

---

notamment pour les déclarations immédiates d'emploi. La présentation de cet exemple n'implique pas une opinion favorable de l'auteur quant à ces textes.

[2] Ces deux avant-projets de loi ne sont pas encore publiés.

[3] Loi allemande sur le multimédia du 13 juin 1997, article 3 (sur la signature digitale), Journal officiel allemand du 22 juillet 1997 (BGBl, IS, 1870), entrée en vigueur le 1er août 1997, http://www.iid.de/iukdg/iukdge.html

[4] Décret présidentiel italien du 10 novembre 1997, n° 513 on « Regulations establishing criteria and means for implementing Section 15 (2) of Law N° 59 of 15 March 1997 concerning the creation, storage and transmission of documents by means of computer-based or telematic systems », publiée in Gazzetta Ufficiale, 13 mars 1998, n° 60, http://www.aipa.it/english/law[2/pdecree51397.asp

[5] OCDE, Groupe d'experts sur la sécurité de l'information et la vie privée, « Inventaire des approches en matière d'authentification et de certification dans une société de réseaux mondialisée », octobre 1998, DSTI/ICCP/REG(98)3/REV3.

[6] Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, COM (98)297 final, 13 juin 1998, *J.O.C.E.*, C 325/5-11 du 23 octobre 1998 ou http://www.ispo.cec.be/eif/policy/com98297fr.doc

[7] Voir par exemple Commission des Nations Unies pour le Droit Commercial International, Rapport du groupe de travail sur le commerce électronique sur les travaux de sa trente et unième session (New York, 18-28 février 1997), A/CN.9/437, 12 mars 1997 ; Commission des Nations Unies pour le Droit Commercial International, Rapport du groupe de travail sur le commerce électronique sur les travaux de sa trente troisième session (New York, 29 juin-10 juillet 1998), A/CN.9/454, 21août 1998. Voir aussi http://www.un.or.at/uncitral/fr-index.htm

1ière partie. En Belgique : une avancée significative…

En Belgique, des initiatives ont été prises afin d'assurer une reconnaissance juridique de la signature électronique. En effet, le 12 juin 1998, le Conseil des ministres a adopté, en première lecture, deux avant-projets de loi allant dans ce sens. Le premier vise à modifier certaines dispositions du Code civil relatives à la preuve des obligations (ci-après « projet preuve »). Le second vise à mettre en place un régime juridique applicable aux activités des autorités de certification agréées (ci-après « projet autorités de certification »), et cela dans le cadre de l'utilisation de signatures digitales.

En sus de la demande d'avis de la section de législation du Conseil d'Etat, ces deux textes ont été discuté au sein d'Agora 98[8] initié par le ministre Di Rupo, forum de discussion officiel à propos de la société de l'information en Belgique[9]. Ces discussions ont débouché sur un rapport[10] de grande qualité et sur des recommandations remises au Ministre des Affaires économiques.

Par simplicité, et sans toutefois nier le lien évident qui existe entre ces deux avant-projets, nous traiterons ces textes dans un titre distinct.

Titre 1. Le projet preuve

Le projet preuve poursuit principalement l'objectif de modifier les règles de preuve du Code civil afin qu'un document signé électroniquement puisse, moyennant le respect de certaines conditions, faire preuve au même titre qu'un écrit papier signé manuscritement.

Commençons par rappeler les principes actuels qui gouvernent le droit de la preuve ainsi que leurs faiblesses pour ensuite présenter des solutions envisageables et enfin exposer la solution adoptée par l'avant-projet de loi.

Chapitre 1er. Rappel des principes.

L'article 1341 du Code civil consacre le principe de la prééminence de l'écrit[11]. Il dispose que « Il doit être passé acte devant notaire ou sous signature privée, de toutes choses excédant une somme ou valeur de 15.000 francs ». En d'autres mots, la partie qui veut faire la preuve d'un acte juridique en matière civile[12], dont la somme dépasse 15.000 francs, doit apporter la preuve par un écrit signé[13].

[8] http://www.agora98.org/

[9] Plus exactement, ces textes ont été discutés dans l'atelier 1 de la branche « Consommateurs », relatif à la signature électronique et à la certification des sites, présidé par le Professeur Yves Poullet. Cet atelier regroupait des experts et personnes intéressées par le sujet issus du secteur tant privé que public, du barreau, du notariat, du monde universitaire, etc.

[10] Ce rapport (Position Paper) est disponible à l'adresse suivante : http://www.agora98.org/fr/conso/fconso.html

[11] Pour une étude approfondie des principes, voy. R. MOUGENOT, *Droit des obligations : La preuve*, Larcier, 1997, 2ième édition, pp. 98 et s. ; N. VERHEYDEN-JEANMART, *Droit de la preuve*, Précis de la Faculté de Droit de l'Université Catholique de Louvain, Bruxelles, Larcier, 1991, pp. 234 et s.

[12] En matière commerciale, la preuve est libre.

[13] Ce qui exclut la preuve par témoignages et présomptions, sauf si la partie peut se prévaloir des exceptions à l'article 1341, soient l'article 1347 (commencement de preuve par écrit) ou l'article 1348 (impossibilité de se procurer un écrit).

Une question fondamentale réside dans celle de savoir ce qu'on entend par « écrit signé ». Le Code civil ne donne de définition ni de la notion d'écrit ni du concept de signature. La position selon laquelle la loi n'exclut pas la signature électronique est donc défendable[14].

Toutefois, la jurisprudence constante de notre Cour suprême[15] et une partie de la doctrine[16] ont pallié cette carence en envisageant l'écrit comme un écrit sur support papier et en définissant la signature comme devant être un signe, accompagné d'un certain graphisme, qui est apposé de manière manuscrite.

On comprend que dans ce contexte les utilisateurs de nouvelles technologies soient réticents à supprimer la voie papier lorsqu'ils doivent se ménager des moyens de preuve.

Chapitre 2. Les solutions possibles

§1. Une jurisprudence et une doctrine minoritaire

Avec l'utilisation sans cesse croissante des nouvelles technologies et le développement de la société de l'information, certains auteurs[17] ont proposé d'abandonner la définition formelle de la signature et ont plaidé pour une approche fonctionnelle de celle-ci. Selon eux, peu importe la forme que peut prendre la signature. Ce qui compte en effet, c'est que la signature puisse remplir les fonctions traditionnellement assignées à celle-ci, à savoir identifier le signataire et permettre à celui-ci de manifester son consentement au contenu de l'acte auquel la signature se réfère. Dans une certaine mesure, on doit pouvoir admettre que la signature remplit une troisième fonction, celle de maintien de l'intégrité du contenu de l'acte. En effet, dans l'environnement papier, on constate que la fonction d'intégrité est remplie par le support papier mais aussi par la signature manuscrite qui, apposée au bas du document, permet

---

[14] Cette interprétation est défendue par un arrêt du tribunal civil de Namur du 25 juin 1990, *R.R.D.*, 1992, pp. 60 et s. X. Thunis en conclut même que la « notion d'écrit signé peut s'interpréter assez largement étant donné l'imprécision ou l'ouverture providentielle des concepts fondamentaux, écrit et signature », X. THUNIS, *Responsabilité du banquier et automatisation des paiements*, Travaux de la Faculté de droit de Namur, P.U.N., 1996, p. 228 et les références citées aux notes 67 et 68.

[15] Cass., 24 févr. et 3 nov. 1910, *Pas.*, 1910, I, pp.241 et 475 ; Cass., 1er mars 1917, *Pas.*, 1917, I, p.118 ; Cass., 7 janv. 1955, *Pas.*, 1955, I, p.456 ; Cass., 2 oct. 1964, *Pas.*, 1965, I, p.106 ; Cass., 28 juin 1982, *R.C.J.B.*, 1985, p. 69, note M. VAN QUICKENBORNE.

[16] Voir par exemple E. Dubuisson qui considère que la signature numérique ne constitue pas l'équivalent de la signature manuscrite, E. DUBUISSON, « La personne virtuelle : proposition pour définir l'être juridique de l'individu dans un échange télématique », *D.I.T.*, 1995/3, p.8 ; M. VAN QUICKENBORNE, "Quelques réflexions sur la signature des actes sous seing privé", note sous Cass. 28 juin 1982, *R.C.J.B.*, 1985, p. 69.

[17] M. ANTOINE, J.-F. BRAKELAND et M. ELOY, *Le droit de la preuve face aux nouvelles technologies de l'information et de la communication*, Cahier du C.R.I.D., n° 7, Bruxelles, Story Scientia,1991, pp. 38 et s. ; 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.*, juillet-octobre 1998, n° 4/5, pp.285-310 ; E. DAVIO, « Preuve et certification sur Internet », *R.D.C.*, 1997, n°11, pp.660 à 670 ; M. FONTAINE, "La preuve des actes juridiques et les techniques nouvelles", in *La preuve*, Colloque U.C.L., 1987 ; J. LARRIEU, « Les nouveaux moyens de preuve : pour ou contre l'identification des documents informatiques à des écrits sous seing privé », *Cahiers Lamy Droit de l'informatique*, 1988, H/88, p.8 et I/88, p.26 ; D. MOUGENOT, « Droit de la preuve et technologies nouvelles : synthèse et perspectives », *Droit de la preuve-Formation permanente CUP*, Volume XIX, octobre 1997, pp.45-105 ; Y. POULLET, « Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve », in *Le droit des affaires en évolutions, Le juriste face à l'invasion informatique*, Colloque ABJE, 24 oct. 1996, Bruxelles, Bruylant, Anvers, Kluwer, 1996, pp.39 à 67; D. SYX, « Vers de nouvelles formes de signature ? », *Droit de l'inf.*, 1986/3, pp.133 et s.

d'éviter toute ajoute non autorisée au texte[18]. Dans le monde électronique, la question est d'autant plus pertinente que la fonction d'intégrité sera souvent remplie uniquement par le mécanisme de signature électronique, qui fige logiquement et non plus matériellement le contenu de l'écrit électronique, indépendamment de tout support.

Certaines décisions, malheureusement isolées, osent franchir le pas et interprètent d'une manière évolutive les concepts d'écrit et de signature. A cet égard, deux arrêts méritent d'être mentionnés : un arrêt du tribunal civil de Namur du 25 juin 1990[19] et un arrêt de la chambre commerciale de la Cour de cassation française du 2 décembre 1997[20].

Le 25 juin 1990, le tribunal civil de Namur statue en degré d'appel sur un litige relatif au renouvellement d'un bail commercial. Le juge de paix, au premier degré, avait estimé nulle la demande de renouvellement de bail au seul motif que le formalisme de la loi n'avait pas été respecté, et en l'espèce, que la lettre de renouvellement n'avait pas été signée par les preneurs. Ceux-ci s'étaient limités à écrire manuscritement la lettre ainsi que leurs noms et prénoms au bas de la lettre. En appel, le tribunal civil réforme cette décision en précisant que d'une part, il convient « de relever que la forme ou le graphisme d'une signature ne sont point l'objet de prescriptions légales précises », que d'autre part, on se doit de « souligner que le rôle *authentificateur* des engagements conférés à la signature tend à s'estomper à mesure que se répandent de nouvelles techniques d'authentification, faisant par exemple appel à des codes secrets ou à des pistes magnétiques personnalisées accompagnant les modes de paiements électroniques susceptibles d'être utilisés sans aucun recours à la signature traditionnelle », et termine en indiquant que la question fondamentale est « de savoir si, par le seul effet de la mention des noms et prénoms des preneurs, la demande de renouvellement doit ou non être tenue pour émanant effectivement d'eux et si elle a pu être tenue pour telle par le bailleur ». Le tribunal s'attache donc plus à la réalisation des fonctions (identification, approbation et maintien de l'intégrité) qu'au respect d'un simple formalisme.

L'arrêt de la Cour de cassation française du 2 décembre 1997 est encore plus progressiste. Il s'agit d'une affaire de cession de créance. La question était de savoir si l'acceptation de la cession peut être valablement donnée par le débiteur, sous la forme d'une télécopie. En l'espèce, la Cour répond favorablement en jouant non pas sur le concept de copie fidèle et durable ou sur celui de commencement de preuve par écrit mais tout simplement sur le concept d'écrit (acte sous seing privé). Pour la Cour, le concept d'écrit peut être interprété largement pour autant qu'il réponde à certaines fonctions. L'écrit « peut être établi et conservé sur tout support, y compris par télécopie, dès lors que son intégrité et l'imputabilité de son contenu à l'auteur désigné, ont été vérifiées ou ne sont pas contestées ». Ce qui compte en effet, ce n'est ni le formalisme, ni le support physique, ni le mode de communication des volontés ; c'est la certitude que l'écrit émane bien de celui auquel il pourrait être opposé, en d'autres termes, que ni son origine, ni son contenu n'ont été falsifiés (la Cour parle d'imputabilité et d'intégrité).

Les utilisateurs de nouvelles technologies considéreront ces arrêts comme réjouissants mais manifestement pas suffisants pour opérer un renversement de la jurisprudence. Il en résulte qu'une certaine insécurité juridique subsiste. C'est une des raisons pour laquelle le Conseil

[18] M. ANTOINE et D. GOBERT, *o.c.*, p.290.
[19] Civ. Namur, 25 juin 1990, *R.R.D.*, 1992, pp. 60 et s.
[20] Cass. fr. (com.), 2 déc. 1997, *Dalloz*, 1998, p. 192.

des ministres du 30 mai 1997[21] a décidé de préparer un projet de loi adaptant les règles de preuve du Code civil aux nouveaux mécanismes de signatures.

[21] Pour un extrait de la note soumise au Conseil des ministres, voy. J. DUMORTIER et P. VAN EECKE, « Naar een juridische regeling van de digitale handtekening in België », *Computerrecht*, 1997/4, pp. 154-159.

§2. La nécessité d'une intervention législative

Partant du constat que la jurisprudence restait très conservatrice quant à l'interprétation des règles de preuve, le législateur a ressenti le besoin d'intervenir afin de faire évoluer celle-ci. Différentes alternatives s'offrent au législateur pour admettre la preuve électronique.

1. Instaurer un système libre de preuve

L'idée consiste à supprimer le régime de la preuve réglementée. Ainsi, la loi n'exigerait plus qu'un acte juridique dont la somme dépasse 15.000 francs soit nécessairement prouvé par un écrit signé. Un document électronique deviendrait recevable au titre de présomption par exemple.

Ce principe a été introduit dans le Code civil des Pays-Bas en 1988[22]. L'adoption d'un système libre de preuve a également été préconisé par une Recommandation du Conseil de l'europe de 1981[23]. En effet, cette recommandation invitait les Etats membres à supprimer l'exigence par laquelle il fallait prouver par écrit les actes juridiques supérieurs à un certain montant.

2. Elever le seuil en deçà duquel la preuve est libre

Rehausser la limite fixée à l'article 1341 du Code civil permettrait d'augmenter le nombre d'actes juridiques qui peuvent être prouvés librement. En deçà du montant fixé par la loi, un document signé électroniquement serait recevable par le juge.

Cette solution est également encouragée par la recommandation de 1981 dans le cas où un Etat membre ne supprimerait pas l'exigence d'un écrit. La France et le Grand-Duché du Luxembourg s'étaient engagés dans cette voie. La loi française du 12 juillet 1980 prévoit que le montant visé à l'article 1341 du Code civil n'est plus fixé par la loi mais par décret[24]. Le Grand-Duché du Luxembourg a fait de même par la loi du 22 décembre 1986.

3. Légitimer la preuve électronique par le biais d'exceptions

Cette solution consisterait à étendre le champ d'application des exceptions à l'article 1341 Cc. Dans le cadre de l'article 1347, on pourrait considérer qu'un écrit électronique constitue sans nul doute un commencement de preuve par écrit ou que lorsqu'on agit par voie électronique, on se trouve dans l'impossibilité de se procurer une preuve écrite au sens de l'article 1348.

Cette voie a également été suivie par la France et le Grand-Duché du Luxembourg, ceux-ci ayant précisé à l'article 1348 que l'impossibilité de se procurer un écrit peut être matérielle ou morale.

---

[22] I. de LAMBERTERIE, « La valeur probatoire des documents informatiques dans les pays de la C.E.E. », *Rev. int. dr. comp.*, 1992, n°3, pp. 641-685.

[23] Recommandation R(81) 20 « relative à l'harmonisation des législations en matière d'exigence d'un écrit et en matière d'admissibilité des reproductions de documents et des enregistrements informatiques ».

[24] Ce qui permet un révision plus rapide et plus fréquente.

4. Adopter une approche ouverte et fonctionnelle de la signature

Ces trois premières solutions ont été exploitées par certains pays[25] comme évoqué ci-dessus. Elles ont cependant montré leurs limites liées aux inconvénients qu'elles présentent[26]. C'est la raison pour laquelle une quatrième solution semble s'imposer peu à peu.

L'idée, déjà défendue par de nombreux auteurs[27], consiste à adopter, à coté de la conception formelle de la signature traditionnelle, une approche fonctionnelle du concept de signature. Ainsi, en introduisant une définition fonctionnelle de la signature dans le Code civil, on considèrerait que constitue une signature, non seulement la signature manuscrite, mais également tout mécanisme qui permet de remplir de manière fiable les fonctions traditionnellement assignées à celle-ci (identification, adhésion ainsi que le maintien de l'intégrité).

Depuis quelques années, cette approche semble s'imposer à tous niveaux.

Dans sa loi type sur le commerce électronique de 1996[28], la CNUDCI invite les Etats à adopter une définition fonctionnelle de la signature. Il suffit pour s'en convaincre de citer l'article 7 relatif à la signature qui dispose que « 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 ; … ».

La proposition de directive européenne[29] pour un cadre commun sur les signatures électroniques suggère dans son article 5 que, pour autant que certaines conditions soient remplies, la signature électronique soit admissible comme preuve en justice de la même manière que la signature manuscrite.

En Italie, une loi du 15 mars 1997[30] stipule en termes généraux dans son article 15 que « la création d'actes ou de documents informatiques ainsi que leur transmission et leur conservation par voie télématique sont légalement valides ». Cette loi a été précisée par un décret présidentiel du 10 novembre 1997[31] qui dispose dans son article 4 que les documents informatiques qui respectent les prescriptions du décret doivent être considérés comme rencontrant les exigences légales en matière d'écrit. L'article 5 prévoit le même type d'assimilation pour le concept de signature. En France, un rapport du Conseil d'Etat du 2 juillet 1998[32] propose de modifier le Code civil et de traiter un document assorti d'une signature électronique fiable de la même manière qu'un écrit papier signé manuscritement. Au Grand-Duché du Luxembourg, un avant-projet de loi sur le commerce électronique est en préparation. Celui-ci prévoit d'introduire dans le Code civil luxembourgeois une définition fonctionnelle de la signature.

---

[25] I. de LAMBERTERIE, *o.c.*

[26] Pour une analyse de ces inconvénients, voy. M. ANTOINE et D. GOBERT, *o.c.*, pp.289 et 290.

[27] cfr *infra*, note 17.

[28] Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation, 1996, Nations Unies, New York, 1997 disponible à l'adresse suivante : http://www.un.or.at/uncitral/fr-index.htm

[29] Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, *o.c.*, note 6.

[30] Law N° 59 of 15 March 1997 « concerning the creation, storage and transmission of documents by means of computer-based or telematic systems », http://www.aipa.it/english/law[2/law5997.asp

[31] Décret présidentiel italien du 10 novembre 1997, *o.c.*, note 4.

[32] http://www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm, pp. 74-92.

Chapitre 3. La solution belge : l'approche fonctionnelle

L'initiative belge ne se démarque pas de l'approche évoquée ci-dessus. En effet, l'avant-projet de loi visant à « modifier certaines dispositions du Code civil relatives à la preuve des obligations », adopté par le Conseil des ministres du 12 juin 1998, prévoit dans son article 3 d'introduire une définition fonctionnelle de la signature à l'article 1322 du Code civil. Il se libelle comme suit : « 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 ».

Cette définition soulève quelques commentaires.

D'une part, on perçoit que la définition reprend les deux fonctions traditionnellement assignées à la signature classique. Elle doit identifier l'auteur de l'acte et permettre à ce dernier de manifester son consentement sur le contenu de celui-ci. La fonction d'intégrité n'est pas reprise expressément dans la définition. Cependant, on doit la considérer comme sous-entendue : on n'imagine pas qu'on puisse adhérer à un acte qui pourrait être modifié par la suite sans que l'on s'en aperçoive. Notons que l'avant-projet de loi luxembourgeois reprend expressément cette troisième fonction dans la définition de la signature.

D'autre part, la définition conserve une distinction entre la signature manuscrite et d'autres formes de signatures. L'intérêt de cette distinction est probablement d'affirmer que peut désormais exister et être admis d'autres formes de signatures que la signature manuscrite, sans toutefois balayer l'interprétation jurisprudentielle et doctrinale qui a été faite de cette dernière.

Enfin, une signature électronique suppose une transformation de l'écrit. En effet, dans l'environnement électronique, il est primordial que la signature soit liée logiquement à l'écrit, sans quoi on ne peut être sûr que c'est cet écrit qui émane du prétendu signataire.

A côté de cette modification fondamentale, l'avant-projet de loi apporte deux nouveautés supplémentaires.

Premièrement, un alinéa supplémentaire est ajouté à l'article 1322 du Code civil. Celui-ci stipule que « En cas d'application de l'alinéa précédent, est assimilé à un acte sous seing privé original l'écrit signé dont le maintien de l'intégrité du contenu est établi avec certitude ». Cette disposition vise la notion d'original et n'est pas sans incidence sur l'archivage de documents signés électroniquement. Elle part du constat que des reproductions sont effectuées continuellement dans l'environnement électronique. En d'autres termes, un document change régulièrement de support. Toutefois, et contrairement à l'environnement papier, on ne peut pas dire qu'un document électronique perd automatiquement la valeur d'original dès la première reproduction, dès qu'il ne se trouve plus sur le premier support. En effet, il gardera la valeur d'original si l'intégrité du contenu du document est établie avec certitude. Or on constate que dans le monde électronique, c'est n'est généralement plus le support qui assure le maintien de l'intégrité mais un mécanisme informatique qui fige logiquement le contenu de l'écrit électronique, indépendamment du support sur lequel il se trouve[33].

Deuxièmement, l'article 1315 du Code civil relatif à la charge de la preuve a été modifié. En effet, l'article 2 de l'avant-projet de loi en fait désormais une disposition impérative. L'article

[33] Voir sur cette question les réflexions intéressantes d'Etienne DAVIO, *o.c.*, pp.664 à 666.

2 ajoute un alinéa à l'article 1315 qui stipule que « Les conventions qui dérogent aux dispositions de cet article, sont réputées nulles à l'exception de celles conclues après le commencement d'un procès judiciaire ». Cette modification est surprenante. Même si l'objectif est louable, à savoir protéger la partie faible à une convention contre les clauses qui prévoient une répartition inéquitable de la charge de la preuve, la manière de l'atteindre est discutable. Plutôt que d'agir par le biais du Code civil qui s'applique également aux conventions conclues entre commerçants, n'aurait-il pas été plus approprié d'agir par les lois particulières qui assurent déjà une protection de la partie faible à une convention (la loi sur les pratiques du commerce, plus particulièrement l'article 32, 18°, la loi sur les contrats de travail,etc). De plus, cette modification va à l'encontre du caractère supplétif des règles de preuve du Code civil admis unanimement par la jurisprudence[34].

Passons désormais à une analyse succincte du deuxième avant-projet, intimement lié au projet preuve, intitulé « projet de loi relative à l'activité d'autorités de certification agréées en vue de l'utilisation de signatures digitales » que l'on appellera par soucis de simplification « projet autorités de certification ».

Titre 2. Le projet « autorités de certification »

Le projet « autorités de certification » est technique et orienté du point de vue de la technologie. En effet, il se limite au mécanisme de la signature digitale, aussi appelée signature numérique.

Il convient de ne pas confondre signature électronique et signature digitale. Le concept de signature électronique se présente comme un terme générique englobant un ensemble de mécanismes techniques (code secret, techniques basées sur la cryptographie symétrique ou asymétrique, signature biométrique, etc) qui méritent l'appellation de signature électronique dans la mesure où ils permettent la réalisation par voie électronique des fonctions de la signature classique, à savoir, l'identification du signataire et l'expression de sa volonté d'adhérer au message signé. La signature digitale[35], par contre, ne constitue qu'un mécanisme particulier de signature électronique. Elle est basée sur une technique particulière de cryptographie, à savoir la cryptographie asymétrique.

Le projet de loi se limite à la technique de la signature digitale. Et cela, pour deux raisons : d'une part, cette technologie est devenue un standard *de facto* en matière de commerce électronique car elle constitue la technique la plus mûre et qui présente le plus haut degré de sécurité pour les échanges de données en réseau ouvert[36] et, d'autre part, l'intervention d'autorités de certification ne s'effectue actuellement que dans le cadre de l'utilisation de la signature digitale or le projet vise essentiellement à réglementer les activités des autorités de certification agréées.

[34] La Cour de cassation a décidé que les dispositions légales relatives à la preuve n'étaient ni d'ordre public (Cass., 30 janv. 1947, *Pas.*, 1947, I, p.29 ; Cass., 30 sept. 1948, *Pas.*, 1948, I, p.520 ; Cass., 20 juin 1957, *Pas.*, 1957, I, p.1256) ni impérative (Cass., 16 oct. 1962, *Pas.*, 1963, I, p.229 ; Cass., 22 mars 1973, *Pas.*, 1973, I, p.695 ; Cass., 24 juin 1994, *Pas.*, 1994, I, p.651).

[35] La littérature utilise également le terme signature numérique, 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.587 ; P. TRUDEL et S. PARISIEN, *L'identification et la certification dans le commerce électronique*, Québec, Les éditions Yvon Blais Inc., 1996, p. 96.

[36] P. TRUDEL et S. PARISIEN, *o.c.*, p. 96.

Chapitre 1er. Fonctionnement de la signature digitale et rôle de l'autorité de certification[37]

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. Ces deux clés sont générées sur base d'une fonction telle qu'il est impossible de déduire de la clé publique la clé privée correspondante. La clé publique doit dès lors représenter une fonction 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[38].

Alice désire envoyer à Bernard un message informatisé signé digitalement. 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 permet 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[39], l'intégrité du message d'Alice peut être vérifiée.

L'utilisation de la signature digitale ne peut être envisagée sans l'intervention au départ d'autorités de certification (ci-après nommées AC). Celles-ci sont appelées à jouer un rôle fondamental dans le cadre de l'identification des différents utilisateurs de réseaux ouverts.

---

[37] Ce chapitre s'inspire entièrement de l'article de M. ANTOINE et D. GOBERT, *o.c.*, pp.292 et 294. Voy. aussi J. CHONG, « A primer on digitale signatures and Malaysia's digitale signatures act 1997 », *Computer Law & Security Report*, 1998, Vol.14, n°5, pp.322-333.

[38] Voir aussi le processus de création d'une signature digitale dans E.A. CAPRIOLI, *o.c.*, p.588, n°27.

[39] 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 la fonction de hachage irréversible 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).

La principale fonction d'une autorité de certification est d'assurer un lien formel entre une personne et sa clé publique[40]. Ce lien sera confirmé dans un certificat digital émis par l'AC. Ce certificat contient ainsi différentes informations relatives notamment à l'identité du titulaire du certificat (celui qui veut signer et s'identifier comme tel), sa clé publique et relatives à l'identité de l'AC. Le certificat est réalisé et signé par l'AC à l'aide de sa propre clé privée et est, de ce fait, protégé contre les altérations.

L'exemple suivant illustre l'utilisation possible de certificats. Alice transmet à Bernard un message ainsi que sa signature digitale réalisée à l'aide de sa clé privée. Après avoir reçu ces documents, Bernard commence par vérifier le certificat (qu'il aura soit reçu d'Alice soit été chercher dans un répertoire électronique de certificats) à l'aide de la clé publique de l'AC. Si la vérification s'avère concluante, il est assuré de l'intégrité des informations contenues dans le certificat, soient l'identité d'Alice, de sa clé publique ainsi que de l'identité de l'AC. Il peut ensuite utiliser la clé publique d'Alice pour vérifier la signature du message transmis par celle-ci.

L'AC peut remplir d'autres fonctions qui sont subsidiaires à la certification : l'archivage des informations qui sont relatives aux certificats (surtout pour des questions de preuve) ; le cas échéant, la génération de la paire de clés, sans toutefois conserver copie de la clé privée ; la tenue d'un registre électronique de certificats accessible au public ; l'horodatation de messages signés digitalement ; la vérification de signatures digitales et la confirmation de leur validité[41].

Ainsi qu'on le voit, le rôle de l'AC n'est pas minime. Elle doit mettre en place une infrastructure qui permette de collecter des informations et d'assurer leur intégrité en toute sécurité. L'efficacité du processus d'identification représente un élément déterminant de la responsabilité de l'AC.

Pour ces raisons et dans la droite ligne de la note adoptée par le Conseil des ministres le 30 mai 1997, ce dernier a adopté le 12 juin 1998 un avant-projet de loi visant à réglementer les activités des autorités de certification agréées.

Pour résumer, la signature digitale qui est basée sur la technique de cryptographie asymétrique et est combinée à l'utilisation d'un certificat permet de remplir trois fonctions importantes[42] : d'une part, elle garantit l'identité de l'auteur d'un document signé digitalement, d'autre part elle garantit l'intégrité de ce même document, enfin, elle atteste la volonté du signataire de s'approprier le contenu de l'acte signé digitalement[43].

---

[40] Cette clé publique ainsi que la clé privée complémentaire peuvent être générées soit par le titulaire soit par l'AC. Dans ce dernier cas, l'AC ne peut ni enregistrer ni conserver la clé privée générée.

[41] P. TRUDEL et S. PARISIEN, *o.c.*, pp. 128 à 130 ; E.A. CAPRIOLI, *o.c.*, p.589.

[42] Outre son utilisation aux fins de signature, la cryptographie peut également être utilisée afin d'assurer la confidentialité des messages. En vertu de l'article 79 de la loi du 19 décembre 1997, l'usage de la cryptographie est libre en Belgique (loi du 19 décembre 1997 modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques afin d'adapter le cadre réglementaire aux obligations en matière de libre concurrence et d'harmonisation sur le marché des télécommunications découlant des décisions de l'Union européenne, *M.B.*, 30 décembre 1997, p. 34986).

[43] Dans ce sens, E.A. CAPRIOLI, *o.c.*, p.588, note 66.

Chapitre 2. Les grandes orientations du projet autorités de certification

Quatre principes majeurs se dégagent du projet « autorités de certification » : adoption d'un système libre d'agréation ainsi que d'agréations variables, introduction d'une clause d'assimilation à la signature manuscrite et délivrance de certificats tant à des personnes physiques que morales.

§1er. Adoption d'un système libre d'agréation

Dans un système libre d'agréation[44], une AC n'a pas l'obligation de demander une agréation pour exercer ses activités de création, de délivrance et de gestion des certificats. Toutefois, si une AC désire obtenir une agréation, elle doit introduire sa demande auprès d'une administration déclarée compétente à cet effet. L'agréation n'est accordée et maintenue que si l'AC répond aux conditions d'agréation stipulées par ou en vertu de la loi, et appréciées par l'administration ou une entité désignée par elle (offrir des garanties d'indépendance, de fiabilité et de sécurité, d'informations, d'interopérabilité, etc). Ces conditions ont pour objectif de garantir un ensemble d'impératifs de nature à accroître la confiance dans les AC qui répondent à celles-ci (AC agréées).

L'obtention et le maintien de l'agréation a pour conséquence de soumettre à l'application de la loi d'une part, l'AC agréée et d'autre part, les titulaires de certificats émis par l'AC agréée ainsi que les destinataires de messages signés digitalement émanant de ces derniers.

La loi ne s'applique pas aux AC qui ne demandent pas ou n'obtiennent pas une agréation. Ces AC ne peuvent donc pas se prévaloir du statut d'AC agréée. En contrepartie, elles ne sont pas tenues par les dispositions de la loi qui sont notamment relatives au contenu du certificat, au registre électronique, à la suspension et à la révocation des certificats, etc.

La loi ne s'applique pas non plus aux titulaires de certificats émis par une AC non agréée ainsi qu'aux destinataires de messages signés digitalement émanant de ces derniers. Ils ne peuvent, notamment, se prévaloir des droits reconnus par cette loi, tels que, par exemple ceux qui consistent à obtenir un certificat avec un contenu minimum, à obtenir une suspension ou révocation immédiate du certificat, à bénéficier d'un niveau de sécurité adéquat, etc. Toutefois, si la loi ne s'applique pas, le juge pourrait toujours, en cas de litige, s'inspirer des principes fondamentaux de celle-ci (niveau de sécurité adéquat, régime de responsabilité, etc) sans qu'il ne soit cependant tenu de les appliquer.

Notons que l'adoption d'un système libre était encouragée par la Commission européenne qui indique dans sa communication du 8 octobre 1997[45] que « en tout état de cause, il faut assurer la coexistence de systèmes de signatures numériques réglementées et non réglementées ». Elle ajoute « un cadre réglementaire (communautaire) devrait permettre la coexistence d'AC licenciées et non-licenciées ». Plus récemment, ce système libre est préconisé par l'article 3 de la proposition de directive sur un cadre commun pour les signatures électroniques[46].

---

[44] Pour une analyse favorable à ce système, voy. M. ANTOINE et D. GOBERT, *o.c.*, pp.302 et 303.

[45] COM(97)503 : Vers un Cadre Européen pour les Signatures Numériques et le Chiffrement : Assurer la sécurité et la confiance dans la communication électronique, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions, 8 octobre 1997, disponible à l'adresse suivante : http://www.ispo.cec.be/eif/policy/97503toc.html

[46] Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, *o.c.*, note 6.

§2. Adoption d'un système d'agréations variables

En vue de garantir un maximum de souplesse au système, la loi donne la possibilité pour une AC de demander une agréation plus ou moins étendue en fonction des personnes auxquelles elle souhaite délivrer des certificats. L'agréation peut donc avoir un contenu variable qui dépendra au départ de la demande effectuée par l'AC. En effet, la loi permet qu'une AC puisse demander une agréation large qui couvre la délivrance de certificats à la fois à des personnes physiques ou morales (de droit privé ou public). Inversement, l'AC peut restreindre l'étendue de son agréation à la délivrance de certificats à l'une ou l'autre de ces personnes. Elle peut même limiter son agréation à la délivrance de certificats à des personnes physiques ayant un attribut particulier. Par exemple, une AC peut se spécialiser dans la certification de la profession d'avocat ou de médecin : l'AC sera donc agréée pour certifier une personne physique ayant l'attribut avocat ou médecin mais ne pourra pas se prévaloir de son statut d'AC agréée pour les autres catégories de personnes physiques (notaire, architecte,…) ni pour les personnes morales. Toutefois, son agréation couvrira la certification de toute personne physique n'ayant aucun attribut à certifier (l'AC se limite à certifier l'identité d'un citoyen).

Ces distinctions ont une grande importance car elles conditionnent le plan de sécurité et les pratiques d'authentifications mises en place par l'AC qui demande l'agréation. Il en résulte que l'audit effectué sera bien entendu différent en fonction du type d'agréation demandée. En effet l'AC sera tenue d'exposer clairement les pratiques et procédures suivies pour identifier voire authentifier la personne qui demande un certificat ainsi que vérifier l'éventuel attribut dont cette personne demande la certification. Or ces pratiques et procédures différeront suivant le type de personne et d'attribut. Par exemple l'identification d'une personne physique ne se fait pas de la même manière et sur la base des mêmes documents que l'identification d'une personne morale. Dans le même sens, la vérification de l'attribut d'avocat se fera d'une manière différente de celle de l'attribut de médecin ou de réviseur d'entreprise. Dans le premier cas, elle établira des procédures fiables de récolte d'informations auprès de l'ordre national des avocats par exemple et dans le second auprès de l'ordre des médecins ou de l'Institut des Réviseurs d'Entreprises, chacun ayant leurs spécificités propres.

Cette variabilité des agréations peut se justifier par le fait qu'il eût été lourd d'exiger qu'une AC doive obtenir une agréation large alors qu'elle désire se spécialiser dans la certification d'un attribut précis. Une telle exigence aurait pour conséquences d'obliger l'AC :

- à mettre en place un système capable de délivrer des certificats à tout type de personne et tout type d'attribut et donc à mettre en place un processus contraignant mais superflu de vérifications des informations ;
- à engager des coûts non négligeables pour obtenir une agréation qu'elle n'aurait exploitée qu'en petite partie ;
- à faire l'objet d'un audit plus astreignant que ce qui est nécessaire;
- à se soumettre à l'application de la loi pour la délivrance de certificats à tout type et catégorie de personne.

Afin d'éviter ces inconvénients, la loi met en place un système qui offre un maximum de souplesse et de liberté aux AC. Ce système permet la coexistence sur le marché d'une part, d'AC non agréées, d'autre part, d'AC agréées n'effectuant de certification qu'en leur qualité d'A.C. agréée et enfin, d'AC effectuant de la certification de telle ou telle catégorie de personne en tant qu'AC agréée et de la certification d'autres catégories de personne en tant qu'AC non agréée. Pour éviter les ambiguïtés et les risques d'usurpation de la qualité d'AC

agréée, la loi oblige toute AC à inscrire dans le certificat l'étendue de l'agréation de celle-ci en vue d'indiquer à l'utilisateur du certificat qu'elle certifie en qualité d'AC agréée ou non.

§3. La clause d'assimilation à la signature manuscrite

Le régime sécuritaire qui entoure l'infrastructure de certification agréée est tel qu'il confèrera à la signature digitale un niveau de sécurité équivalent, voire supérieur à la signature manuscrite. Dès lors, les conséquences juridiques liées à l'utilisation de la signature digitale doivent être les mêmes que celles qui sont actuellement attachées à l'usage de la signature manuscrite[47]. Le message signé électroniquement à l'aide d'une signature digitale combinée à un certificat émis par une autorité de certification agréée doit constituer une signature au sens de la définition fonctionnelle de la signature qui est insérée dans le Code civil.

Cette clause d'assimilation consiste à créer une présomption (réfragable) selon laquelle l'identité de l'auteur, son adhésion au contenu de l'acte ainsi que le maintien de l'intégrité de celui-ci ressortent avec certitude dès que la signature prend la forme d'une signature digitale combinée à un certificat émis par une autorité de certification agréée. Si le certificat est émis par une AC non agréée ou s'il ne s'agit pas d'un mécanisme de signature digitale, il appartiendra à celui qui se prévaut d'une signature électronique de prouver que le mécanisme utilisé permet de garantir l'identité, le maintien de l'intégrité et l'adhésion au contenu avec certitude.

§4. Délivrance de certificats aux personnes physiques et morales

Contrairement à la loi allemande, l'avant-projet permet à une AC de délivrer des certificats non seulement à des personnes physiques mais également à des personnes morales (de droit privé ou de droit public). On peut s'en réjouir car il est vrai que sur les réseaux, bon nombre d'entreprises s'identifient sous leur dénomination sociale ou leur nom commercial. Par exemple, le site web d'une société prend généralement pour « domain name » le nom de celle-ci[48], sans référence à une personne physique. Ces certificats délivrés à des personnes morales seront également très utiles pour les sociétés qui recourent à la labellisation de leur site, c'est-à-dire qu'une espèce de « sceau de qualité » délivré par un tiers certifie que leur site n'est pas un site fantôme et qu'il respecte par exemple la loi sur les pratiques du commerce ou le respect de la vie privée.

La première version de l'avant-projet permettait uniquement à toutes personnes ayant la personnalité juridique de demander et d'obtenir un certificat. Il en résulte qu'un citoyen, une société commerciale, une ASBL, un GIE, l'Etat, un parastatal, une EPA,… pouvaient devenir titulaire d'un certificat. A l'inverse, les entités qui n'avaient pas la personnalité juridique ne pouvaient pas obtenir de certificat d'une AC agréée. La raison de ce choix résidait dans la difficulté pour une AC de vérifier et de confirmer l'identité d'une entité qui n'existe pas juridiquement alors que cette tâche s'avère plus aisée pour les personnes ayant une personnalité juridique (une personne physique peut être identifiée au moyen d'un document officiel, les données d'identification d'une personne morale sont publiées au Moniteur Belge et un Registre national des personnes morales existe). De plus, il est difficile de reconnaître à

[47] Selon E.A. Caprioli « Avec l'usage d'une signature numérique, le consentement à l'acte ne semble faire aucun doute, …, l'adjonction de l'abrégé du message chiffré avec la clé privée au message correspond en quelque sorte à la signature au bas d'un acte. Ainsi, la signature numérique est intimement liée au contenu de l'acte établi sous la forme d'un message », *o.c.*, p.588 et la note 66.

[48] www.tractebel.be ; www.belgacom.be ; www.fundp.ac.be ; etc.

une entité qu'elle puisse être titulaire d'une clé privée et d'un certificat, susceptible a priori de l'engager, si cette entité n'a pas la personnalité juridique. Malheureusement, la dernière version du texte étend la délivrance de certificats à des associations de fait, ce qui sera de nature à créer une certaine insécurité juridique.

Si l'avant-projet permet la délivrance de certificats à des personnes morales, il n'a toutefois pas poussé son raisonnement jusqu'au bout en admettant la signature des personnes morales. En effet, la clause d'assimilation prévue dans l'avant-projet stipule qu'elle ne s'applique que pour les personnes physiques. On peut se demander s'il était raisonnable d'indiquer une telle précision dans un texte de loi, d'autant que le Code civil n'indique nul part que la signature est réservée aux personnes physiques. Une telle précision empêchera toute éventuelle interprétation jurisprudentielle favorable à la reconnaissance de la signature des personnes morales[49].

2ième partie.Au niveau international : une volonté d'harmonisation

Au niveau international, on peut mettre en exergue deux initiatives fondamentales : les travaux de la Commission des Nations Unies pour le Droit Commercial International (CNUDCI) qui, au sein de son groupe de travail sur le commerce électronique, planche sur l'élaboration de règles uniformes pour les signatures électroniques ainsi que la proposition de directive européenne sur un cadre commun pour les signatures électroniques.

Titre 1. Les travaux de la CNUDCI

La CNUDCI a adopté en 1996 une loi type sur le commerce électronique et un guide pour son incorporation[50].

Elle part du constat que le recours à des moyens modernes de communication tels que le courrier électronique et l'échange de données informatisées pour la conduite des opérations commerciales internationales se répand rapidement et devrait continuer de se développer à mesure que l'accès aux supports techniques tels que les autoroutes de l'information et l'Internet s'élargit. Toutefois, la communication d'informations ayant une valeur juridique sous forme de messages sans support papier peut être entravée par des obstacles juridiques à l'utilisation de tels messages ou par l'incertitude quant à leur effet ou leur validité juridique. La Loi type a pour objectif d'offrir aux législateurs nationaux un ensemble de règles internationalement acceptables sur la manière de surmonter un certain nombre de ces obstacles et de créer un environnement juridique plus sûr pour ce que l'on appelle aujourd'hui le "commerce électronique". Les principes énoncés dans la Loi type se veulent également utiles pour les particuliers qui pratiquent le commerce électronique pour la formulation de certaines des solutions contractuelles pouvant être nécessaires pour surmonter les obstacles juridiques au développement de ce type de commerce.

[49] La question de la reconnaissance de la signature aux personnes morales a fait l'objet d'un débat animé dans le cadre des discussions menées au sein d'Agora 98. Pour un aperçu de ces discussions, on consultera utilement le rapport de l'atelier présidé par le Professeur Yves Poullet à l'adresse suivante : http://www.agora98.org/fr/conso/fconso.html

[50] Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation, 1996, Nations Unies, New York, 1997 disponible à l'adresse suivante : http://www.un.or.at/uncitral/fr-index.htm

Dans ce document, la CNDCI adopte une approche ouverte et fonctionnelle des concepts d'écrit, de signature et d'original. De plus, elle traite du problème de l'archivage électronique, du moment et du lieu de formation d'un contrat électronique, de l'accusé de réception électronique, etc.

D'une manière plus spécifique, le groupe de travail sur le commerce électronique de la CNUDCI planche actuellement sur l'élaboration d'un projet de règles uniformes sur les signatures électroniques et les autorités de certification[51]. Par celui-ci, elle définit les notions de signature électronique, signature numérique, certificat et autorité de certification. Elle détermine les effets juridiques de ces signatures. Elle fixe le contenu minimal du certificat et le régime de responsabilité des autorités de certification ainsi que des utilisateurs de certificats. Elle propose des règles en matière de reconnaissance mutuelle des certificats.

Ces différents textes adoptés par la CNUDCI ne sont pas contraignants. Il ne s'agit pas de conventions internationales destinées à être ratifiées par les Etats. Il s'agit simplement d'une bonne source d'inspiration mise à la disposition des législateurs nationaux. Ces textes méritent une attention particulière dans la mesure où ils constituent un ensemble de règles internationalement acceptables, qui permettent une certaine harmonisation et qui jouent une influence évidente sur les autorités européennes.

Titre 2. La proposition de directive européenne

Le 16 juin 1998, la Commission européenne a présenté une proposition de directive sur une cadre commun pour les signatures électroniques[52].

Cette proposition de directive[53] résulte du constat que les initiatives législatives se multiplient dans plusieurs Etats membres et qu'il devient urgent d'avoir un cadre juridique harmonisé au niveau européen afin d'éviter que le fonctionnement du marché intérieur ne soit gravement entravé.

Cette proposition est le fruit d'une réflexion amorcée à la suite de la Communication au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions: « Une initiative européenne dans le domaine du commerce électronique »[54]. Par après la Commission a présenté une Communication 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

[51] Voir par exemple Commission des Nations Unies pour le Droit Commercial International, Rapport du groupe de travail sur le commerce électronique sur les travaux de sa trente et unième session (New York, 18-28 février 1997), A/CN.9/437, 12 mars 1997 ; Commission des Nations Unies pour le Droit Commercial International, Rapport du groupe de travail sur le commerce électronique sur les travaux de sa trente troisième session (New York, 29 juin-10 juillet 1998), A/CN.9/454, 21août 1998. Voir aussi http://www.un.or.at/uncitral/fr-index.htm

[52] Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, COM (98)297 final, 13 juin 1998, *J.O.C.E.*, C 325/5-11 du 23 octobre 1998 ou http://www.ispo.cec.be/eif/policy/com98297fr.doc

[53] Pour un commentaire approfondi de cette proposition de directive, voy. Rosa JULIA-BARCELO et Thomas C. VINJE, « Electronic signatures - another step towards a european framework for electronic signatures : the Commission's Directive proposal. », *Computer Law & Security Report*, octobre 1998, n° 14/5, pp. 303-313.

[54] COM(97)157 : Vers une initiative européenne en matière de commerce électronique, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions, 15 avril 1997, §36, disponible à l'adresse suivante : http://www.cordis.lu/esprit/src/ecomcom.htm

chiffrement »[55]. Le 1er décembre 1997, le Conseil a accueilli favorablement cette communication et a invité la Commission à soumettre dès que possible une proposition de directive au Parlement européen et au Conseil sur les signatures numériques.

La proposition de directive poursuit essentiellement deux objectifs. Premièrement, elle vise à promouvoir la reconnaissance légale de la signature électronique, et à définir les critères pour ce faire. C'est l'objet de l'article 5 qui contient une clause d'assimilation ainsi qu'une clause de non discrimination. La clause d'assimilation consiste à assimiler la signature électronique à la signature manuscrite lorsque certaines conditions sont remplies c'est-à-dire à considérer qu'elle doit avoir la valeur juridique d'une signature manuscrite et qu'elle doit être admissible comme preuve en justice de la même manière que celle-ci. Par contre, la clause de non discrimination s'applique lorsque les conditions ne sont pas remplies pour bénéficier de la clause d'assimilation. Dans ce cas, Les Etats membres doivent veiller à ce que l'effet ou la validité juridique d'une signature électronique ne soit pas contestée au seul motif que la signature se présente sous forme électronique, ou qu'elle ne repose pas sur un certificat agréé, ou encore qu'elle ne repose pas sur un certificat délivré par un prestataire de service de certification accrédité au sens de la proposition de directive. Deuxièmement, la proposition détermine les règles communes qui s'appliquent aux prestataires de services de certification (au niveau de la responsabilité, du contenu du certificat, de la reconnaissance internationale des certificats, de la vie privée, des conditions d'agrément, etc).

Les grandes orientations adoptées par la proposition sont les suivantes :

cadre neutre du point de vue technologique: étant donné le rythme de l'innovation technologique, cette proposition prévoit la reconnaissance juridique des signatures électroniques, indépendamment de la technologie utilisée (par exemple les signatures numériques reposant sur la cryptographie asymétrique ou la biométrie) tout en reconnaissant que la signature numérique, fondée sur la cryptographie asymétrique, est actuellement considérée comme de première importance.

champ d'application: cette proposition concerne la fourniture au public de certificats visant à identifier l'expéditeur d'un message électronique, mais elle ne s'applique pas aux groupes fermés d'utilisateurs tels que les intranets ou les systèmes bancaires, dans lesquels une relation de confiance existe déjà, et où, par conséquent, il n'existe pas de besoin manifeste de réglementation. Dans ces systèmes, la liberté contractuelle doit continuer à prévaloir.

système volontaire d'agrément : les prestataires de service de certification doivent pouvoir offrir leurs services sans être obligés d'obtenir une autorisation préalable. Toutefois, les prestataires de services souhaiteront peut-être bénéficier de la validité juridique que confèrent aux signatures électroniques des régimes volontaires d'accréditation liés à des exigences communes. L'accréditation doit être considérée comme un service public offert aux prestataires de service de certification désireux de fournir des services de haut niveau. Ceci ne doit en aucun cas impliquer qu'un prestataire de services non accrédité est automatiquement moins sûre.

Notons qu'une version plus récente, non publiée, de la proposition de directive a été soumise au Conseil des ministres européens du 27 novembre 1998 en vue d'aboutir à une position commune. Malheureusement, cette tentative a échoué. Le point principal de désaccord porte sur l'introduction d'une annexe III relative aux exigences pour les dispositifs de création de

[55] COM(97)503 final, 1997. http://www.ispo.cec.be/eif/policy/Welcome.html#digital

signatures électroniques. Dès lors, il est peu probable que la directive soit adoptée dans les tous prochains mois.

CONCLUSION ET REFLEXIONS PROSPECTIVES

Que ce soit au niveau international ou national, une effervescence législative particulière s'est fait ressentir ces deux dernières années dans le domaine de la signature électronique. Après avoir adopté une loi type sur le commerce électronique, la CNUDCI s'attache désormais à la rédaction de règles uniformes sur les signatures électroniques. Même si la procédure d'adoption du texte vient d'essuyer un échec le 27 novembre 1998, il n'empêche qu'une proposition de directive existe bel et bien en cette matière et que l'on peut espérer qu'elle sera rapidement adoptée. Pour leur part, les différents Etats membres ont soit déjà adopté une loi, soit sont en train de préparer une projet de loi dans ce secteur. Ces différents textes poursuivent généralement les mêmes objectifs, même s'ils ne le font pas toujours d'un manière identique : assurer une reconnaissance légale de la signature électronique et déterminer le régime juridique qui s'applique aux autorités de certification.

On voit donc que le phénomène n'est pas isolé et qu'il dépasse un simple effet de mode. Il répond manifestement à des besoins liés au développement du commerce électronique, qui prend un envol non négligeable avec l'explosion récente d'Internet. Ces initiatives législatives sont encourageantes et de nature à promouvoir la passation de communications électroniques dans un cadre juridique sûr. Elles devraient satisfaire l'avocat qui, dans un soucis évident d'organisation, de rationalisation des procédures et de recherche d'efficacité, fera de plus en plus usage des moyens de communication modernes.

Toutefois, il serait vain de se limiter à ce stade. La reconnaissance légale de la signature électronique ne sera pas de grande utilité si on n'effectue pas en parallèle une consécration juridique du recommandé électronique ainsi qu'une réflexion approfondie sur le problème de l'archivage électronique, ou plus exactement de la validité dans le temps et de la lisibilité technique des documents signés digitalement. Enfin, il conviendra d'opérer un recensement systématique et de modifier toutes les lois particulières que exigent encore un écrit papier ou une signature manuscrite.

Didier Gobert
Assistant à la Faculté de droit de Namur
Chercheur au CRID