

UNIVERSITE DE DROIT, D'ECONOMIE ET DE SCIENCE SOCIALES
PARIS II PANTHEON-ASSAS



LA SIGNATURE ELECTRONIQUE

*Mémoire de DESS de droit du Multimédia et de l'Informatique.
Sous la direction de Monsieur le professeur Jérôme HUET*

Année universitaire 2002-2003

Julien ESNAULT

A Monsieur le Professeur Jérôme HUET,

Pour m'avoir offert la chance de suivre cette formation,

A Maître Eric CAPRIOLI et Monsieur François COUPEZ,

Pour leurs précieux conseils,

A mon ami Monsieur Rouzbeh ZIAEI,

Pour son soutien et ses connaissances en droit civil.

L'université n'entend donner aucune approbation ou improbation aux opinions émises dans les mémoires et thèses. Ces opinions doivent être considérées comme propres à leur auteur.

INTRODUCTION

« Parturiunt montes ;

nascetur ridiculus mus »

Horace, *Art poétique*, 139.

Depuis sa création, l'informatique a eu pour vocation de favoriser les échanges. De l'interconnexion généralisée des postes informatiques est né l'Internet, aussi appelé réseau des réseaux.

Aujourd'hui, l'Internet est devenu un nouveau mode de distribution. Les avantages offerts aux utilisateurs sont, en effet, nombreux : comparaison des produits on-line¹ et en temps réel, paiement en ligne, prix des produits souvent plus bas dû au modèle économique², livraison à domicile. L'essor significatif du commerce en ligne³ – qui est amené à s'amplifier- nécessite alors que la confiance puisse être assurée.

Cette confiance pourra être notamment acquise par l'établissement d'un écrit, c'est-à-dire par la reconnaissance d'une valeur juridique à un « document » électronique.

Or la notion d'écrit se rattachait traditionnellement au support papier, de sorte que la signature - nécessaire à la perfection d'un acte juridique – n'était pas adaptée au monde dématérialisé.

En effet, la preuve « littérale » désignait « *une écriture apposée en signes lisibles sur un support tangible*⁴ ».

Cependant, avec l'essor du numérique, la jurisprudence a démontré, en la matière, une faculté d'adaptation appréciable. En effet, la Cour de cassation a reconnu dès 1989 la validité de la convention de preuve introduite dans le contrat porteur des cartes bancaires⁵, ce qui a permis au paiement électronique de se développer. De même, la photocopie, à qui la Cour de

¹ « En ligne » - Il existe à cet effet de nombreux sites de comparaison des prix tels que « *kelkoo.com* ».

² La boutique traditionnelle est remplacée sur la toile par un site, sorte de boutique virtuelle qui serait ouverte 24h/24h, tout au long de l'année, permettant en outre une meilleure gestion des commandes dans la mesure où celles-ci sont saisies directement par le client.

³ Avec 19% d'acheteurs en 2002, la France entre dans le top 10 des pays comptant la plus forte proportion d'acheteurs en ligne parmi les internautes. Cependant la sécurité du paiement demeure le frein principal à l'acte d'achat on-line. Voir en ce sens l'étude TNS-Sofres sur le e-commerce en 2002 (http://www.tns-sofres.com/etudes/interactive/180702_ecommerce.htm).

⁴ P. Catala, « *Ecriture électronique et actes juridiques* », Mélanges Cabrillac, Dalloz et Litec, 2000, p.95.

⁵ C. Cass. 1^{ère} civ., 8 Nov. 1989 (2 arrêts): Bull. Civ. I, n°342; JCP G 1990, II, note G. Virassamy ; RTDC com. 1990, p.78, obs. M. Cabrillac et B. Teyssié, D. 1990 somm., p.327, obs. J. HUET.

cassation avait dénié toute portée juridique⁶, a finalement été reconnue comme valant commencement de preuve par écrit⁷. La recevabilité de l'écrit, et par extension de la signature, tend alors à se définir indépendamment de son support, et selon des critères précis que sont l'*identification* de son auteur et l'*intégrité*, qui seront les deux conditions essentielles posées par la loi du 13 Mars 2000. Les données informatiques étant par nature modifiables à volonté, immatérielles et volatiles, il était nécessaire d'adapter le droit national à ces nouvelles exigences.

D'aucuns ont évoqués une révolution du numérique⁸, ou un dédoublement de la preuve⁹, mais on peut également envisager la consécration de la signature électronique dans le Code civil comme le fruit d'une évolution annoncée par la jurisprudence. Ainsi, la signature électronique ne s'opposerait pas à la signature « traditionnelle » : elle serait un mode alternatif d'expression de sa volonté.

Parce que le statut incertain des actes et documents dématérialisés se devait d'être clarifié, la Commission de nations unies pour le droit commercial international (CNUDCI) a adopté en 1996 une loi-type sur le commerce électronique¹⁰ qui encourage la reconnaissance juridique des outils du commerce électronique. En juillet 1998, le Conseil d'Etat rend un rapport « *Internet et les réseaux numériques* ». Il y propose de reconnaître une valeur juridique aux outils de transaction électronique.

La directive européenne du 13 Décembre 1999¹¹ va alors marquer une avancée significative dans la mesure où elle va reconnaître en son article 5¹² l'admissibilité de la signature électronique. Le but de cette directive était de promouvoir la sécurisation des transactions sur les réseaux numériques. Pour ce faire, elle attribue un minimum d'effets juridiques aux signatures électroniques dans le marché intérieur, et assure la libre circulation des produits et

⁶ C. Cass. com., 15 déc. 1992 : Bull. civ. IV, n°419.

⁷ C. Cass. 1^{ère} civ., 14 fév. 1995 : JCP G 1995, II 22402, note Y. Chartier.

⁸ Selon M. Christian Paul, rapporteur à la commission des lois.

⁹ P. Y. Gautier, « *Révolution Internet: le dédoublement de l'écrit juridique* », D. 2000, n° 12, p. V.

¹⁰ A l'origine, loi type sur l'échange de donnée informatisée (EDI). Le groupe de travail des paiements internationaux, renommé *Groupe de travail sur l'échange des données informatisées* a été finalement baptisé *Groupe de travail sur le commerce électronique*.

¹¹ Voir en ce sens E. Caprioli, « *La directive européenne n°1999/93/CE : sur un cadre communautaire pour les signatures électroniques* », Gaz. Pal. 29/31 Oct. 2000, p.1842.

¹² « *Les Etats membres veillent à ce que les signatures électroniques avancées [...] répondent aux exigences légales d'une signature à l'égard de données électronique de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier* », Directive n°1999/93/CE du Parlement et du Conseil du 13 Décembre 1999 sur un cadre communautaire pour les signatures électroniques (JOCE 19 Janv. 2000, n° L13, p.12)

services attachées à celle-ci, notamment en prévoyant la liberté d'établissement des prestataires.

Les définitions données par la directive sont plutôt d'ordre technique et non fonctionnel. Certaines notions clés sont définies à l'article 2 : On entend par signature électronique « *une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification* ». De même, la signature électronique avancée est une signature électronique qui satisfait en outre à d'autres exigences : « *être liée au signataire, permettre son identification, être créée sous des moyens que le signataire puisse garder sous son contrôle exclusif être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure soit détectable* »

De plus, la directive va introduire la notion de « certificats de signature » et de « prestataire de services de certification ». Ainsi, même si aucune référence n'est explicitement faite à l'infrastructure *PKI* ou à *clé publique*, neutralité technologique oblige, celle-ci paraît la seule en mesure de satisfaire aux exigences de la directive.

La loi du 13 Mars 2000 est venue modifier le droit français relatif à la preuve. Désormais, le droit reconnaît l'équivalence du support papier et du support numérique dès lors qu'un certain nombre de conditions sont respectées. Le code civil dispose en son article 1316-4 que « *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.*

Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat. »

Le législateur ne fait aucune référence à la technique employée pour satisfaire aux critères de fiabilité. Il laisse le soin au pouvoir réglementaire de déterminer les critères techniques garantissant la fiabilité. C'est un choix à approuver car cela permet une plus grande évolutivité face à l'avancement de la technique¹³.

¹³ Selon E. Joly-Passant, « *L'analyse de la loi du 13 Mars 2000 montre que le législateur est resté technologiquement neutre vis-à-vis des procédés de mise en œuvre de la signature électronique en déléguant au pouvoir réglementaire le soin de définir les conditions de sécurisation de la signature électronique. Toutefois, compte tenu de la fugacité de l'état de la technique, on ne peut qu'approuver une telle sagesse.* » in « *le décret du 31 Mars 2001 pris pour application de l'article 1316-4 du Code civil et relatif à la signature électronique* » : Lamy droit de l'informatique et des réseaux, n°137, juin 2001.

Le décret du 30 Mars 2001 va transposer la directive sur la signature électronique. Il distingue la signature électronique simple de la signature électronique « sécurisée¹⁴ », qui doit satisfaire à certains critères techniques afin de bénéficier de la présomption de fiabilité. En outre, on pourra y trouver à l'article 1^{er} une définition du signataire : « *toute personne physique agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en œuvre un dispositif de création de signature électronique* ».

Le décret du 18 avril 2002 est relatif à l'évaluation et à la certification des produits offerts par les PSCE¹⁵, prestataires de services de certification électronique.

Ainsi, il conviendra d'étudier dans un premier temps le mécanisme de création de la signature électronique, notamment la nécessité pour la signature électronique de garantir l'identification du signataire et l'intégrité du document (Titre I), puis, dans un second temps, d'envisager la mise en œuvre de la signature sous un angle juridique, c'est-à-dire en s'attachant à la force probante de la signature électronique et à la mise oeuvre de la responsabilité des prestataires de services de certification (Titre II).

¹⁴ La directive employait le terme de signature avancée.

¹⁵ Qui sera étudiée plus loin.

TITRE I

La création de la signature électronique

La notion de signature n'avait jamais été définie par le droit. Cependant, avec la nécessité d'adapter le droit de la preuve à l'ère du numérique, le législateur a dû donner une définition de la signature. La signature manuscrite peut se définir comme une émanation de la personne. Cette émanation est porteuse d'un double sens : d'une part, elle permet d'identifier la personne (Chapitre I), puisque la signature est propre à chaque individu et, en théorie, unique. D'autre part, le fait d'apposer sa signature sur un acte juridique manifeste l'adhésion du signataire avec le contenu de l'acte. De plus, il est nécessaire pour une signature électronique que soit assurée l'intégrité (Chapitre II) du document. En effet, il suffirait de modifier l'acte après apposition de la signature pour modifier la teneur de l'engagement contractuel.

Chapitre I - Nécessité de garantir l'identification du signataire.

Pour que la validité de la signature électronique puisse être assurée, l'auteur doit pouvoir être identifiable. Il ne s'agit donc pas ici de fournir des informations de type état civil, l'usage d'un pseudonyme pouvant être reconnu. Toutefois, l'utilisation d'un pseudonyme doit être limitée dans certains cas. En effet, il faut que le signataire puisse être formellement identifié pour certains actes, les plus graves, c'est pourquoi il paraît important que le prestataire délivrant le certificat possède ici toutes les informations nominatives concernant celui-ci, nécessaires à sa parfaite identification. Faute de quoi, l'exigence légale d'identification ne serait pas respectée et donc la signature privée de sa force probante.

Section 1 - Un moyen sous le contrôle direct du signataire.

Le décret du 30 Mars 2001 exige dans son article 1^{er}, alinéa 2, que la signature électronique avancée soit *créée par des moyens que le signataire puisse garder sous son contrôle exclusif*.

De même, l'alinéa 4 de l'article 1316 du Code civil pose la condition que *l'identité du signataire* [soit] *assurée*.

La signature électronique utilise, pour satisfaire aux exigences légales, une *Infrastructure de gestion de Clé Publique (ICP ou PKI : Public Key Infrastructure)*¹⁶. C'est un système fondé sur la cryptologie asymétrique¹⁷. On peut, ainsi, employer également le terme de signature numérique. Le dispositif de création de la signature va émettre deux clés ; une clé privée (car connue du seul signataire) et une clé publique (car accessible à tous). Ces deux clés sont une séquence de chiffres, générées en même temps par un algorithme mathématique, et liées entre elles. En effet, ce qu'une clé fait, seule l'autre peut le défaire¹⁸.

En pratique, la clé privée est un identifiant numérique qui peut être intégré dans divers supports, tels qu'un logiciel, une carte à puce ou un « *dongle*¹⁹ ». A terme celle-ci pourra être remplacée par l'usage de la biométrie, qui permet l'identification de l'être humain par ses données organiques²⁰. La clé publique est, quant à elle, apposée sur/dans le certificat de signature électronique, sorte de carte d'identité virtuelle dont nous verrons plus loin la signification et la composition.

La clé privée permet de signer le document électronique, c'est donc l'équivalent du stylo auquel il faut ajouter le savoir-faire du signataire, car la clé privée peut permettre de produire une vraie signature, à la différence du faussaire qui ne pourra pas mieux imiter votre signature en se servant de votre stylo²¹. Il est donc impératif que celle-ci ne soit pas divulguée et reste en la possession de son propriétaire²². De plus, le recours à un code d'accès complémentaire pourrait être une garantie supplémentaire. Ainsi, la mise en œuvre du procédé de signature ne

¹⁶ La société *Magicaxess* offre une solution alternative car elle permet un procédé de signature électronique par les « *tokens* », qui permettent une gestion dynamique des mots de passe. L'identification est ici a priori effectuée par le téléphone mobile du signataire.

¹⁷ Par opposition à la cryptographie symétrique, qui n'utilise qu'une seule clé. Ce procédé n'est pas utilisé pour la signature électronique car il eût été trop risqué, la clé unique pouvant être interceptée.

¹⁸ Il ne faut, cependant, pas assimiler ICP et signature électronique : en effet, le chiffrement d'un message à l'aide de la clé publique assurera une fonction de confidentialité puisque seul le porteur de la clé privée pourra en prendre connaissance. Au contraire, le chiffrement à l'aide d'une clé privée assurera la fonction de signature électronique puisque l'auteur pourra être identifié. Toutefois, le bi-clé ne saurait servir à la fois à assurer les fonctions de confidentialité et de signature : « *il a été démontré que, dans certaines conditions, des attaques peuvent réussir si une bi-clé est utilisée à la fois pour chiffrer et pour signer* », T. Autret L. Bellefin, M.-L. Oble-Laffaire, « *Sécuriser ses échanges électroniques avec une PKI* », Ed. 2002, p.32.

¹⁹ Aussi appelé « *clé électronique* » ; dispositif matériel permettant l'accès au logiciel.

²⁰ A ce sujet, voir l'affaire des cantines ayant recouru à la biométrie par numérisation de la paume de la main. De même, le film d'anticipation « *Minority Report* » de S. Spielberg offre une vision des risques liés un recours déraisonné aux procédés de biométrie.

²¹ Les puissants utilisaient autrefois un sceau pour signer, celui-ci pouvant être volé pour usurper leur identité.

²² Pour ce faire, il est important de veiller également à la sécurisation lors de la remise de la clé privée, pour éviter toute interception, voire envisager une remise en main propre.

pourrait être validé qu'une fois un code ou un « identifiant » saisi²³, ce qui permettrait l'accès à la clé privée.

L'arrêt de la cour d'appel de Besançon du 20 Octobre 2000²⁴, *Sarl Chalets Boisson c/ Bernard G.* est apparu pour certains²⁵ comme étant la première jurisprudence sur la signature électronique. En effet, la signature « informatique » était ici un simple fichier informatique qui reproduisait visuellement une signature manuscrite (c'est-à-dire une signature numérisée).

...En conséquence, les dispositions de ce texte sont inapplicables en l'espèce d'autant plus que le décret destiné à préciser les conditions de la fiabilité d'identification de la personne qui appose la signature n'est pas encore paru à la date des débats devant la cour.

Partant, la cour n'est pas en mesure d'apprécier le degré de fiabilité du processus décrit par l'appelante au regard d'un texte dont la parution est attendue.

La fiabilité du procédé utilisé en l'espèce par l'avocat est au demeurant toute relative dans la mesure où le code permettant d'accéder à la signature peut être détenu par une autre personne du cabinet.

L'identification de la personne ayant recours à la signature informatique est dès lors très incertaine.

En l'espèce, il est évident que la simple image de la signature ne pouvait pas avoir la valeur d'une signature électronique puisqu'elle ne permettait d'assurer *ni le lien avec l'acte auquel elle s'attache, ni l'intégrité du message*²⁶. La cour s'est toutefois interrogée sur l'éventuelle validité de ce procédé de signature, et en a conclu que qu'un simple code de protection ne pouvait valablement justifier de l'identité du signataire.

De même, une très récente décision de la deuxième chambre civile de la Cour de cassation en date du 30 Avril 2003²⁷, apporte une solution finale à l'affaire « *Chalets Boisson* ». Elle refuse la validité d'une signature créée antérieurement à la loi du 13 Mars 2000 et qui ne permettait pas de s'assurer d'une parfaite identification. En l'espèce, lors d'une procédure sans

²³ A la condition que l'utilisateur ne le laisse pas sur un *post-it* collé à l'écran de l'ordinateur (comme c'est malheureusement souvent le cas) ou ne le communique à des tiers.

²⁴ CA Besançon, ch. soc., 20 oct. 2000, *SARL Chalets Boisson c/ Bernard Gros*: JCP G 2001, II, n°10606, note E. Caprioli et P. Agosti ; Com. com. élec. janv. 2001, comm. 6, p.22, note J. -C. Galloux.

²⁵ T. Piette-Coudol, « *la signature électronique* », Ed. Litec, n°63.

²⁶ Sur le point de savoir si cette décision pourrait faire obstacle à la pratique de nombreuses grandes sociétés, telles que les banques ou les compagnies d'assurance, qui utilisent une signature numérisée pour signer les chèques, il convient de répondre par la négative. En effet, le chèque est un support physique, papier : la condition d'identification est assurée, et le consentement présumé par la pratique.

²⁷ C. Cass. 2e civ., 30 Avr. 2003 ; *SARL Chalets Boisson c/ G.* : Juris-Data n° 2003-018798

représentation obligatoire, la Cour d'appel avait reçu un acte dit de "déclaration d'appel" qui ne comportait pas la signature manuscrite de son auteur mais une signature électronique. Après avoir relevé qu'il existait un doute sur l'identification de la personne qui avait usage de ce procédé, les juges du fond ont parfaitement refusé la validité de cet acte.

De plus cette décision apporte une précision sur l'application de la loi dans le temps. Sur le fondement de l'article 2²⁸ du Code civil, la deuxième chambre civile a estimé qu'une signature électronique effectuée pour authentifier une déclaration d'appel (formalité à effectuer par pli recommandé) ne pouvait être valablement admise durant le régime antérieur à la loi du 13 mars 2000. Ainsi, il convient de s'inquiéter du sort qui sera réservé aux actes signés électroniquement avant la loi du 13 Mars 2000.

Aussi, il faut noter que certains types de signatures électroniques ne permettent pas d'assurer une parfaite identification de l'auteur. Ainsi, les procédés faisant appel aux téléphones mobiles ne paraissent pas en mesure d'assurer une identification suffisante du signataire, car l'envoi de pièce d'identité, même par courrier recommandé ne permet pas une réelle identification du signataire. De même, le recours à un téléphone mobile peut permettre de douter du fait que le moyen soit sous le contrôle direct du signataire.

Parallèlement, plusieurs grands opérateurs de téléphonie mobile²⁹ testent actuellement des services de signature électronique via les SMS – *Short Message Service*- permettant aux utilisateurs de pouvoir faire des achats via les sites partenaires. Ce procédé ne satisfait pas, selon nous, aux conditions exigées d'une véritable signature électronique sécurisée, un téléphone pouvant être utilisé par un tiers, et l'identification n'étant fondée sur aucune autre preuve tangible que les éléments fournis lors de l'ouverture de la ligne³⁰.

L'identification doit, donc, absolument correspondre à celle de la personne, auteur intellectuel selon le droit. Afin de pouvoir s'assurer que la clé publique est réellement celle du détenteur prétendu, que celle-ci n'a pas été usurpée, ou que le bi-clé n'a pas été tiré frauduleusement, il convient de le faire certifier par une tierce partie : le prestataire de services de certification électronique³¹, qui va émettre un certificat.

²⁸ « La loi ne dispose que pour l'avenir ; elle n'a point d'effet rétroactif », Code civil, Article 2.

²⁹ SFR avec la société *Médiacert* et Orange avec la société *Verisign*.

³⁰ Que penser alors des cartes « entrée libre » que l'on peut se procurer chez n'importe quel buraliste ? Cette technique peut favoriser un e-commerce sur téléphone mobile mais en aucun cas constituer en l'état un procédé fiable de signature électronique.

³¹ Aussi appelé PSC ou PSCE.

Section 2 - Le certificat : « pièce d'identité » dématérialisée.

Le certificat est au cœur du processus de signature électronique. Il est porteur d'une valeur juridique puisqu'il va permettre l'identification de la personne, mais il a également une définition technique. Selon la définition qui en est donnée par l' « ISO », c'est « *un objet informatique qui permet de lier de façon intangible une identité d'entité (une personne, une ressource) à certaines caractéristiques de cette entité* ».

Le certificat est, ainsi, un message électronique par lequel un témoin privilégié, le certificateur, contrôle la concordance et l'adéquation entre l'identité du signataire et la clé publique. La loi du 13 Mars 2000 en son article 1316-1 suggère le recours au certificat dans la mesure où elle exige que la personne puisse être *dûment identifiée*, et dans son article 1316-4 lorsqu'elle ajoute que l'identité du signataire doit *assurée*.

Le certificat possède une structure interne, c'est-à-dire certains champs qui doivent – obligatoirement, pour lui accorder une force- être renseignés. Cette structure interne est définie par une norme internationale nommée *recommandation X-509 V.3* de l'Union internationale des télécommunications. Cette norme a été reprise et développée par l'organisation de normalisation du monde Internet, l'*Internet Engineering Task Force* (IETF) qui a décliné la norme de certificats pour l'appliquer à la technologie de signature numérique. En pratique, l'utilisateur va transmettre sa clé publique au certificateur³². Après certaines vérifications sur l'identité et la capacité de la personne, le certificateur va garantir son identité en confectionnant puis émettant un certificat électronique qui contiendra la clé publique et les informations permettant l'identification de la personne. Aussi, pour assurer le destinataire que le certificat n'est pas un faux, le certificateur va devoir signer ce certificat de sa signature électronique.

Le décret du 30 Mars 2001 reconnaît deux types de certificats : le certificat électronique simple et le certificat qualifié. Le premier est un document qui se présente sous la forme électronique et qui atteste du lien entre les données de vérification de signature électronique et

³² Sauf le cas répandu où le certificateur sera aussi à l'origine du tirage du bi-clé, cas qui sera à notre avis majoritaire car beaucoup plus commode pour les utilisateurs.

un signataire. Le certificat électronique qualifié doit répondre à une série de critères définis par le décret.

Selon le décret 2001-272 du 30 Mars 2001, le certificat électronique qualifié doit avoir été délivré par un prestataire capable de délivrer ce type de certificats et comporter certaines indications (article 6) telles que :

- a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;
- b) L'identité du prestataire de services de certification électronique ainsi que l'état dans lequel il est établi ;
- c) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;
- d) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat est destiné ;
- e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;
- f) L'indication du début et de la fin de la période de validité du certificat électronique ;
- g) Le code d'identité du certificat électronique ;
- h) La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;
- i) Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.

Il existe plusieurs catégories de certificats en fonction de la gravité des actes à passer. En général, on peut distinguer trois classes³³, allant de la simple signature de mail sans portée juridique³⁴ (qui ne requiert qu'une simple déclaration par courrier électronique), à la télédéclaration de TVA pour les personnes morales (qui requiert la présence physique d'un agent assermenté c'est-à-dire un contrôle physique de la personne).

³³ Dans les certificats dédiés à la signature électronique, c'est par exemple, ce que propose la société *Certinomis*.

³⁴ On peut toutefois s'interroger sur la nécessité de signer un mail sans portée juridique?

Ainsi, la certification et la gestion des certificats constituent «la pierre angulaire³⁵» du système, car dans le cas d'un certificat qualifié, associé à d'autres conditions énumérées ci-dessous, la fiabilité de la signature sera présumée. La charge de la preuve sera alors inversée : il incombera à celui qui conteste le document de la rapporter.

En effet, la présomption de fiabilité³⁶ du procédé de signature électronique n'est accordée qu'à la triple condition que :

- La signature électronique mise en œuvre soit une signature sécurisée.
- Cette signature électronique sécurisée soit établie grâce à un dispositif de sécurisé de création de signature électronique.
- La vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié.

Selon l'article 3 du décret du 30 Mars 2001, seul le PSC qualifié peut délivrer une signature électronique sécurisée, car il est le seul à mettre en œuvre un dispositif de création sécurisé.

Ce dispositif doit, en effet, avoir été certifié conforme soit par un organisme désigné par un Etat membre³⁷ de la communauté européenne, soit par un service du Premier Ministre, la Direction centrale de la sécurité des systèmes d'information (DCSSI) dans les conditions prévues par le décret du 18 avril 2002³⁸. La certification sera l'aboutissement d'une longue série de vérifications et de tests. En effet, le procédé de création de signature électronique devra d'abord faire l'objet d'une évaluation, puis d'une certification par un centre d'évaluation, devant lui-même être préalablement agréé³⁹.

Certains observateurs⁴⁰ préconisaient, pour pouvoir réduire les coûts de la signature électronique, et ainsi la rendre accessible au plus grand nombre, de recourir au modèle de la « toile de confiance », ou « web of trust ». Ainsi, des particuliers pourraient s'identifier mutuellement pour former une toile de certificats. L'identité de chaque personne pourrait être vérifiée plusieurs fois par des personnes différentes, ce qui augmente alors les risques de

³⁵ Selon E. Joly-Passant, « Le décret du 30 Mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique », Rev. Lamy Dt des Aff., Juillet 2001, n°40, p.21.

³⁶ Article 2 du décret 2001-272 du 30 Mars 2001.

³⁷ La signature s'inscrit donc dans un cadre trans-national, communautaire qui peut alors permettre une reconnaissance mutuelle du procédé entre les états membres.

³⁸ Décret n°2002-535 du 18 Avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

³⁹ Voir en ce sens l'article très détaillé de F. Coupez avec la participation de C. Gailliègue, « Vers une signature électronique juridiquement maîtrisée », Comm. com. électr. Nov. 2001, n°25.

⁴⁰ Voir en ce sens un article anonyme sur le site <http://parodie.com/monétique/signelec>.

vraisemblance de l'identification si les « certificateurs » sont fiables. Le modèle serait ainsi similaire à celui qui a été mis en place grâce au logiciel « *Pretty Good Privacy* », ou *PGP*. En effet, le prestataire est, selon l'article 2 al. 11 de la directive du 13 Décembre 1999⁴¹, « toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques ». L'exercice de l'activité de prestataire de services de certification n'est, en effet, soumis à aucune réglementation spécifique, à aucune autorisation préalable⁴². Ce système, bien qu'audacieux, reste utopique car il ne permet en aucun cas de s'assurer de l'identité de la personne, puisque l'identification ne peut se faire que par Internet, et sans aucun contrôle réel ni sérieux. Il reste inapplicable à l'échelle mondiale dans la mesure où l'on ne pourra pas, en pratique, aller rechercher la responsabilité d'un particulier - prestataire de services de certification- à l'étranger.

En revanche, ce système de « toile de confiance » pourrait être retenu pour un usage en entreprise : le responsable informatique pourrait, ainsi, certifier en interne tous les employés de l'entreprise, ce qui éviterait de recourir à un prestataire de services de certification externe pour l'obtention du certificat, et également permettre une meilleure gestion des certificats délivrés aux employés et une révocation plus rapide de ceux-ci en cas de départ de l'employé.

Ainsi, cela nous amène à se poser la question de savoir si une entreprise peut être son propre prestataire de services de certification⁴³ ?

Certaines grandes entreprises - on pensera en particulier à *La Poste* - peuvent être amenées à signer électroniquement en recourant à leur propre prestataire de services de certification. Il convient, ici, de savoir si la preuve ainsi préconstituée aura une valeur ? Juridiquement, rien n'interdit à une entreprise d'être son propre prestataire de services de certification. Cependant, l'administration de la preuve risque d'en être rendue plus délicate, car la jurisprudence, sur le fondement de l'article 1315 du Code civil, en a déduit que « nul ne peut se constituer une preuve à lui-même⁴⁴ ». Cependant, on peut imaginer que le recours à son propre prestataire de services de certification puisse être envisageable dans le cadre d'un groupe de sociétés, dès

⁴¹ Directive 1999/93/CE, 13 Déc. 1999 sur un cadre communautaire pour les signatures électroniques : JOCE L. 13, 19 janv. 2000, p. 12.

⁴² Art. 1 alinéa 11 du décret du 30 Mars 2000.

⁴³ Voir en ce sens I. Renard, « *Vive la signature électronique* », Ed. Delmas, p.43.

⁴⁴ Civ 1^{ère}, 2 Avril 1996: Bull. Civ. I, n°170 ; D. 1996, Somm. 329 obs. Delebecque; Contrats Conc. Consom. 1996, 119, note Leveneur.

lors que la filiale est une personne morale distincte. Il n'y aurait alors pas constitution de preuve à « *soi-même* ».

Cependant, la fragilité subsiste et rien n'empêche le juge de mettre en lumière les conditions dans lesquelles a été constituée la preuve pour faire application de la jurisprudence de l'article 1315 du Code civil. La preuve ainsi constituée demeure donc faible.

De plus, les exigences mises à la charge du prestataire de services de certification par le Décret du 30 Mars 2001 sont lourdes et un régime spécial de responsabilité est créé par le projet de loi sur la confiance en l'économie numérique.

Ainsi, rien ne semble interdire à une entreprise d'être son propre prestataire de services de certification mais la preuve ainsi obtenue risque de souffrir de faiblesses, et la nature des moyens à mettre en œuvre ne semble pas justifier cette solution.

Chapitre II - Nécessité de garantir l'intégrité du document.

L'un des traits caractéristiques de la signature électronique réside en ce qu'elle fait l'objet d'une télétransmission. Or, pendant cette transmission, la signature peut être altérée, comme, d'ailleurs, le message lui-même. Cette altération peut être due aux conditions techniques ou à l'intervention de personnes mal intentionnées. Le message, à son arrivée, peut ne pas correspondre exactement à celui qui a été envoyé. Ce sont ces risques qui expliquent la nécessité d'une garantie, voulue par les utilisateurs, de l'intégrité des messages électroniques et donc de la signature, qui en est l'une des données.

Cette intégrité devra être permanente : de la création jusqu'à la vérification par le destinataire (Section 1), puis lors de l'archivage de la signature (Section 2).

Section 1 - Intégrité et vérification de la signature : le lien avec l'acte.

Le terme « *intégrité* » est peu usité en droit⁴⁵. Techniquement, l'intégrité signifie l'état d'une chose qui a toutes ses parties, qui n'a pas subi d'altération⁴⁶. Ainsi, le terme « *intègre* » qualifie l'état d'un objet qui n'a pas été modifié, intentionnellement ou non, par rapport à un

⁴⁵ Voir par exemple la notion « *d'intégrité du territoire national* » dans la Constitution française.

⁴⁶ Définition selon le *Petit Larousse* Edition 1988.

état antérieur. C'est, dans le cas de la signature électronique, la transmission qui pourra être à l'origine de la modification du fichier, ce qui explique la nécessité de contrôler le bon état du fichier à l'arrivée. Egalement, le destinataire pourrait être tenté de modifier la teneur du contrat pour, par exemple, limiter son engagement. Il ne faut pas se limiter à ces exemples : la signature électronique tend également à protéger le destinataire car elle va sceller l'engagement contractuel de l'expéditeur. En ce sens, la signature électronique se veut protectrice de toutes les parties au contrat.

L'introduction de la notion d'intégrité en droit peut être perçue comme une innovation. Cependant, il existait déjà avec le support papier un contrôle de l'intégrité du document. En effet, l'utilisation des paraphes⁴⁷ sur les pages d'un contrat et la mention indiquant le nombre de mots ou de phrases supprimés ou ajoutés permet un contrôle de l'intégrité du document.

L'intégrité recourt, en informatique, à l'utilisation de la technique. Elle sera mise en œuvre par le contrôle du condensé ou « *hash* ». En effet, le message à signer va tout d'abord être haché par un logiciel. De ce hachage va résulter un condensé⁴⁸, sorte de chaîne alphanumérique, qui sera le résultat du contenu même du message. Ainsi, à chaque message correspond un condensé numérique unique. Toute modification du message, jusqu'à la suppression d'une virgule, engendrerait un condensé différent. Ensuite, grâce à un dispositif de création de signature électronique, le condensé va pouvoir être chiffré par la clé privée de l'expéditeur. Il en résultera un cryptogramme. Ainsi, c'est pourquoi l'on emploie généralement le terme de « *signature numérique* ». Le lien avec l'acte, exigé par l'article 1316-4 du Code civil, est donc respecté parce que la signature est le condensé du document à signer. Techniquement, ce lien est donc indiscutable.

Toutefois, il convient de prendre en considération les interrogations soulevées par Madame Isabelle de Lamberterie⁴⁹ et reprises par Mademoiselle Elizabeth Passant⁵⁰ quant à l'imprécision du terme employé : « *intégrité* ». En effet, des critères matériels permettent de

⁴⁷ Sorte de « *signature dégradée* ».

⁴⁸ Le logiciel emploie pour cela un algorithme spécialisé qui condense le texte en une chaîne alphanumérique de longueur fixe, quelle que soit la longueur du texte traité.

⁴⁹ I. de Lamberterie, « *Preuve et signature : les innovations du droit français* », Cahiers Lamy Informatique et réseaux, Mars 2000, n°123, K, p.9.

⁵⁰ E. Passant, « *La loi du 13 Mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique : nouvelle donne pour le droit de la preuve.* », Cahiers Lamy Informatique et réseaux, Mai 2000, n°125, B, p.7.

garantir l'immutabilité de l'écrit électronique. Il faut se référer à l'arrêt rendu par la chambre commerciale de la Cour de cassation le 2 Décembre 1997⁵¹. Ici, la cour suprême avait jugé qu'un écrit pouvait être établi et conservé sur tout support, y compris par télécopies dès lors que son intégrité et l'imputabilité de son contenu à l'auteur désigné ont été vérifiées ou ne sont pas contestées.

L'écrit constituant, aux termes de l'article 6 de la loi du 2 janvier 1981, l'acte d'acceptation de la cession ou de nantissement d'une créance professionnelle, peut être établi ou conservé sur tout support, y compris par télécopies, dès lors que son intégrité et l'imputabilité de son contenu à l'auteur désigné ont été vérifiées ou ne sont pas contestées.

Le terme « *intégrité* » a été préféré à celui de « *fiabilité* ». On peut alors se demander si l'exigence d'intégrité s'applique au contenu du support ou au support lui-même ?

Si elle s'applique au contenu, il serait préférable de parler « *d'immutabilité* » de l'écrit: le contenu de celui-ci est fixé définitivement au moment de sa rédaction et ne risque pas d'évoluer au fur et à mesure des témoignages.

Si elle concerne le support, le terme « *inaltérabilité* » semble plus précis. Ce terme est souvent attaché à des supports qui ne peuvent être altérés, qui présentent un caractère constant et immuable, comme le bronze ou la pierre.

Lors de la réception du message, les données de la signature électronique devront être vérifiées. On utilisera, pour ce faire, un dispositif de vérification de la signature électronique, qui permettra de s'assurer de l'identité du signataire (grâce au certificat) et de l'intégrité du message. Il va falloir ainsi défaire ce qui a été fait par le signataire.

Le cryptogramme sera déchiffré grâce à la clé publique de l'expéditeur, ce qui va permettre de retrouver le résumé du message ou « *hash* », garant de l'intégrité. Parallèlement à cela, le message sera haché par le destinataire. Il suffira alors de comparer les deux résumés : s'ils coïncident, la signature est validée, sous réserve de la validité du certificat et de la non répudiation du bi-clé.

⁵¹ C. Cass. com., 2 Déc. 1997, JCP éd. G 1998, Actualité p.905, obs. P. Catala et P.-Y. Gautier; D. 1998, jur., p.192, note D.-R. Martin ; JCP éd. E 1998, II, 10097, note L. Grynbaum.

Les systèmes de vérification de la signature électronique sont également soumis au décret du 30 Mars 2001. Ces dispositifs sont définis comme « *un matériel ou un logiciel destiné à mettre en application les données de vérification de signature électronique*⁵² ».

En vertu de l'article 5 du décret, il est prévu une certification de ces matériels ou logiciels de vérification. Pour obtenir la certification, il faut que ces produits répondent à des exigences, dont on citera ci-dessous les plus pertinentes:

- Garantir l'exactitude de la signature et donner au vérificateur un résultat sécurisé sans altération possible (b),
- Garantir au vérificateur le contenu de l'acte signé (c),
- Garantir au vérificateur, sans fraude possible, que le contenu de l'acte et la signature sont liés (d),
- Donner au vérificateur, sans falsification possible, l'identité précise du signataire et le prévenir lorsque le signataire use d'un pseudonyme (f),
- Permettre au vérificateur de détecter toute falsification ou toute modification d'un des éléments précités (g).

Ainsi, si l'intégrité peut être assurée lors de la réception du document, encore faut-il que celle-ci perdure, pour pouvoir assumer son rôle de preuve lorsque cela sera nécessaire. En effet, il faut que le fichier informatique représentatif de l'*instrumentum* connaisse un état fixe pendant le temps juridiquement nécessaire, au minimum celui requis pour l'exécution des obligations, au maximum celui imposé par les règles de prescription⁵³.

Section 2 - L'intégrité dans le temps : l'archivage.

La question de la conservation est révélatrice du fait que la technique doit servir le droit. Elle démontre l'ascendant du droit sur la technique. Parmi les Etats membres de l'Union européenne, le Portugal⁵⁴ est l'un des premiers pays à s'être interrogé sur la question de la conservation, la nécessité de garantir l'intégrité du document, et les changements apportés à

⁵² Article 1^{er} du décret, n°8.

⁵³ Selon MM. X. Linant de Bellefonds et P.-Y. Gautier, l'écrit informatique, pour s'aligner sur l'écrit papier en ce qui concerne les garanties, a besoin d'un « plus » que l'on pourrait définir ainsi. In «De l'écrit électronique et des signatures qui s'y attachent, JCP éd. E, 3 Août 2000, n°31-34, p.1273.

⁵⁴ Les bases de l'analyse juridique portugaise sur la conservation des actes et des documents sont exposées dans le chapitre 9 d'un document officiel, *le Livre Vert sur la Société de l'Information au Portugal* d'Avril 1997.

ceux-ci durant le temps de la conservation, lesquels sont susceptibles de les transformer en un nouveau document.

La durée de la conservation ne doit pas se limiter à la durée de vie des matériels techniques d'archivage mais à la durée, fixée par la loi, durant laquelle doivent être conservés les documents. En effet, la finalité est de détenir un véritable écrit électronique pouvant être produit en justice.

Le Conseil d'Etat, dans son rapport intitulé « *Internet et les réseaux numériques* », de Septembre 1998, indique que la conservation doit être « *durable* ».

...lorsqu'un message électronique est présenté pour établir la preuve d'un acte, il est présumé doté de la force probante d'un écrit sous signatures privées s'il est accompagné d'un certificat délivré par un tiers certificateur accrédité, indépendant du signataire, dans des conditions précisées par décret, qui garantissent l'intégrité du message, l'imputabilité à l'auteur désigné et sa conservation durable.

Le Code civil, en son article 1348 alinéa 2, définit la durabilité comme engendrant une modification irréversible du support, ce qui ne paraît pas adapté à un stockage informatique sur disques durs. Ainsi, la conservation doit uniquement être fiable.

La réforme du Code civil a tranché la question en recourant à la notion « *d'intégrité* ». En effet, selon l'article 1316-1 du Code civil, l'écrit électronique doit être *conservé dans des conditions de nature à en garantir l'intégrité*.

L'obligation d'archivage peut résulter d'une obligation prescrite par la loi. En effet, le prestataire de services de certification doit, selon le décret du 30 Mars 2001, conserver les caractéristiques et références des documents présentés pour justifier de l'identité et de la qualité du titulaire du certificat. L'archivage peut également avoir pour origine la volonté des parties lors de la conclusion ou du choix d'un des contractants.

Ainsi, dans le cadre d'une infrastructure à clé publique mettant en œuvre une signature électronique, il faut archiver beaucoup de données et de documents. En effet, il faudrait conserver le certificat, les différents contrats signés et ceux conclus avec le prestataire, les

copies des pièces justificatives d'identité et de qualité⁵⁵, toutes les informations qui pourraient se révéler nécessaires pour faire la preuve en justice de la certification électronique⁵⁶ et les données à caractère personnel.

Les conditions de la conservation vont emporter des effets juridiques, c'est pourquoi il convient de sécuriser⁵⁷ au maximum cette conservation. Cette constatation avait été faite également par le *Conseil supérieur de l'ordre des experts comptables* dans un rapport de 1998 sur l'archivage électronique. Ainsi, un groupe de travail a été constitué avec le conseil des experts comptables et l'association IALTA France. Ce groupe a publié, en juillet 2000, un « *guide sur l'archivage sécurisé* », qui traite des échanges électroniques sécurisés par des signatures électroniques. Ces travaux ont permis, grâce au soutien de l'*Association des professionnels de gestion électronique des documents* (APROGED), d'implémenter dans le processus la norme AFNOR Z42-013 sur l'archivage électronique. Cette norme vise à assurer l'intégrité et la fidélité des documents électroniques archivés. Pour tendre vers ce résultat, elle décrit des procédures et des contraintes techniques à respecter.

La possibilité d'archiver en interne offre une faiblesse certaine car le fichier reste, pendant le temps de l'archivage, sous le contrôle direct de l'une des parties. Ainsi, il sera préférable de recourir à un *tiers archiviste*, distant, à qui l'utilisateur va transmettre les documents à archiver par voie électronique.

Dans un premier temps, l'utilisateur va préparer la mise en archivage. A cette fin, il va regrouper tous les fichiers informatiques relatifs au contrat et à la signature.

Ensuite, ces lots de documents⁵⁸ seront signés et expédiés par voie électronique. Il faut ici « signer la signature ». A cette occasion, l'horodatage, c'est à dire la certification de la date de la signature par un prestataire (le plus généralement, un tiers indépendant du PSC), pourra

⁵⁵ Plus exactement, « les caractéristiques et références des documents présentés pour justifier de cette identité et de cette qualité », art. 6, II, m du Décret du 30 Mars 2001.

⁵⁶ Article 6, II, k du décret du 30 Mars 2001. La Directive du 13 Décembre 1999 prévoyait que le prestataire de service de certification doit : « enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile, en particulier pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par des moyens électroniques ».

⁵⁷ MM. X. Linant de Bellefonds et P.-Y. Gautier, « De l'écrit électronique et des signatures qui s'y attachent », JCP Ed. E, 3 Août 2000, p.1273, n°7. Ici, les auteurs proposent de faire résider le contrat sur les ordinateurs des deux cocontractants.

⁵⁸ Le terme « lot » a été volontairement choisi par le groupe de travail (voir supra) car il renforce le caractère de neutralité dont doit faire preuve l'archiviste.

éventuellement permettre de donner « date certaine » au document électronique. L'horodatage tire tout son intérêt de la formation des contrats entre absents, où il est important de connaître avec précision le moment de la formation du contrat, et des téléprocédures, soumises à une date limite.

Puis, le *tiers archiveur* va vérifier la signature et procéder à l'archivage des données. Cette phase d'archivage peut durer très longtemps, et on en sait pas encore précisément comment conserver l'intégrité des documents durant ce temps. En effet, la durée de conservation sera variable en fonction du document à archiver. Les durées légales de conservation sont elles mêmes fluctuantes : 10 ans pour le délai de prescription entre commerçants, 30 ans au maximum pour la matière civile, et jusqu' à 100 ans pour l'acte authentique. Il pourrait donc être nécessaire d'effectuer des migrations⁵⁹ périodiques pour sauvegarder les archives, puisque le matériel informatique nécessite d'être renouvelé régulièrement. Mais, selon l'article 5 g du Décret du 30 Mars 2001, ces modifications entraînent l'échec du processus de vérification des signatures électroniques sécurisées.

Article 5 g du Décret du 30 Mars 2001 : « *Toute modification ayant une incidence sur les conditions de vérification de la signature électronique doit pouvoir être détectée.* »

Ainsi, selon certains auteurs⁶⁰, les contraintes techniques visant à assurer la vérification pérenne des signatures sont incompatibles avec celles visant à assurer la lisibilité pérenne des documents. Alors, des solutions de « re-signature » ou « sur-signature » peuvent être envisagée. Cependant, ces solutions ne permettent pas de réaliser simultanément les objectifs de lisibilité des documents et de vérification – on parlera ici d'intelligibilité – de la signature. Certains doutes peuvent alors être émis sur les moyens techniques et la possibilité d'assurer la pérennité de la signature.

Alors, si la technique ne peut répondre aux exigences légales, il faudra faire confiance à l'interprétation du juge, car une signature privée de force probante n'a pas d'intérêt. Il faut pour cela accorder une plus grande confiance au tiers archiveur qui aura pour tâche de conserver la preuve, sa responsabilité pouvant être engagée.

⁵⁹ En ce sens, I. de Lamberterie et J.-F. Blanchette, « *Le décret du 30 Mars 2001 relatif à la signature électronique : Lecture critique, technique et juridique.* », JCP Ed. E, 26 Juillet 2001, p.1269.

⁶⁰ Voir supra note n° 59.

Le tiers archiveur devra, d'ailleurs, être en mesure de restituer les archives lorsque cela lui sera demandé. L'intégrité, et non la confidentialité, sera assurée par l'apposition d'une nouvelle signature électronique.

Ainsi, selon l'exigence de l'article 1316-1 du Code civil, l'intégrité doit être préservée tout au long du cycle de vie de l'écrit électronique.

Dans la phase transactionnelle, l'intégrité est permanente grâce à la signature électronique.

Dans la phase post-transactionnelle, l'archivage garantit l'intégrité grâce à la signature électronique pour l'entrée et la sortie de l'archive, tandis que les règles de la norme NZ42-013 ont pour but de préserver l'intégrité tout au long de la conservation.

Cet ensemble de règles permet de conférer à la signature électronique une valeur probatoire, qui pourra s'exercer lors de sa mise en œuvre.

TITRE II

La mise en œuvre de la signature électronique

La signature électronique pourra permettre d'apporter la preuve en justice, c'est pourquoi il convient d'étudier, dans un premier temps, sa force probante (Chapitre I).

Aussi, l'élément central qu'est le prestataire de service de certification pourra être mis en cause, c'est pourquoi il conviendra, dans un second temps, d'étudier son régime de responsabilité (Chapitre II).

Chapitre I - Force probante de la signature électronique.

Il convient désormais d'analyser les questions touchant à la force probante et même à la validité des documents obtenus ou transférés par des techniques de reproduction et de communication à distance.

La jurisprudence a su faire preuve d'une grande faculté d'adaptation en reconnaissant par exemple la validité des conventions de preuve accompagnant la délivrance d'une carte magnétique de crédit⁶¹. De même, la cour de cassation a posé les conditions nécessaires à la valeur probatoire d'un document produit par télétraitement⁶². Devant une telle jurisprudence, la question de la nécessité d'une législation s'est posée.

Cependant, la banalisation de l'Internet et l'utilisation croissante de l'électronique dans un but juridique sont des phénomènes qui ne sauraient se satisfaire d'une valeur probante incertaine qui dépendrait de la sagesse des magistrats.

C'est dans cette optique qu'une loi « *relative à l'adaptation du droit de la preuve aux nouvelles technologies* » fut votée le 13 Mars 2000 (ci-après dénommée L-2000).

Afin de mener à bien cette analyse, nous commenterons, dans un premier temps, l'affirmation selon laquelle la preuve informatique fournit la même garantie que le papier (Section 1), avant

⁶¹ C.Cass. 1^{ère} civ., 8 Nov. 1989, Bull. Civ. 1^{ère}, n°342, JCP G 1990 II 21576, note G. Virassamy.

⁶² C.Cass. com. 2 Déc. 1997, JCP G, 1998 Act. P. 905, obs. P. Catala et P.-Y. Gautier.

de nous intéresser, dans un second temps, à la détermination du champ d'application (Section 2).

Section 1 - L'écrit électronique équivaut à l'écrit sur support papier (présomption de fiabilité).

L'un des premiers éléments pour l'analyse de la portée d'un texte juridique est en principe son emplacement dans le code au sein duquel il est intégré, même si cela doit être, bien entendu, souvent complété et nuancé par d'autres éléments d'appréciation.

Or nous constatons que les nouveaux articles issus de la loi L-2000 à savoir les articles 1316 à 1316-4 ont été intégrés dans le Titre III traitant « *des contrats et des obligations conventionnelles en général* », dans un chapitre VI ayant trait à « *la preuve des obligations et de celle du paiement* ». Ce qui est, en revanche, plus remarquable est que les articles sus cités constituent le paragraphe premier intitulé « *dispositions générales* », d'une section première dénommée « *de la preuve littérale* ». Nous démontrerons ci-dessous l'importance de la place de ces textes au sein de cette section première.

En effet, un rapport du Conseil National du Crédit et du Titre (CNCT) avait préconisé une réforme siégeant à l'article 1347 ou à l'article 1348⁶³ du Code civil. L'article 1341 du Code civil affirme l'exigence d'un écrit pour faire la preuve d'un acte juridique. Il reçoit plusieurs exceptions dont notamment celles énoncées aux articles 1347 et 1348. Le premier de ces textes, l'article 1347 du Code civil, parle des commencements de preuve par écrit.

Or, introduire les messages électroniques dans ce texte eût soulevé plusieurs difficultés : d'une part, il eût fallu s'ingénier à inventer le complément de preuve corroborant le commencement de preuve et, d'autre part, elle eût posé, en principe, que ces messages ne constituent pas une preuve complète.

La seconde possibilité évoquée par le CNCT, à savoir rajouter un troisième alinéa à l'article 1348, prévoyant une nouvelle exception au principe de la preuve littérale lorsque le titre est établi et conservé sous forme électronique, eût présenté l'avantage d'introduire cette forme dans le droit civil, mais l'inconvénient de le faire d'une manière dédaigneuse car il aurait été

⁶³ Conseil National du Crédit et du Titre : « *Problèmes juridiques liés à la dématérialisation des moyens de paiement et du titre* », Mai 1997, rapport P. 55 à 80, annexes p.43 et 44.

pour le moins paradoxal de vouloir consacrer une nouvelle notion par le biais d'une simple exception. Il en eût résulté que la loi ne considère pas le titre électronique comme un acte écrit sous signature privée.

C'est pourquoi, le législateur a considéré que les messages électroniques peuvent laisser des traces suffisantes pour faire preuve pleine et entière des actes juridiques sous des conditions posées par la loi ; d'où l'idée de ne pas tenir compte des suggestions émises par le CNCT et de considérer l'écriture électronique comme une des formes légalement reconnue de la preuve littérale. Ce qui a conduit le législateur à introduire les nouveaux articles au sein de la section première sus-évoquée ayant trait à la preuve littérale.

Avant l'introduction de l'article 1316 nouveau, le Code civil ne définissait pas le terme « preuve littérale ». Pour les auteurs l'adjectif littéral désignait une écriture apposée en signes lisibles sur un support tangible⁶⁴. C'est de cette idée d'une définition générale que résulte la définition qui figure à l'article 1316 : « *La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible quels que soient leur support et leur modalités de transmission.* » Cela met un terme au règne sans partage du papier ; de même la volonté peut se manifester par tout moyen fiable et compréhensible.

Par ailleurs, l'article 1316-1 énonce que « *l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ». Ces conditions mises en place pour reconnaître une force probante à l'écrit électronique nous renvoient aux termes employés par la chambre commerciale de la Cour de cassation dans son arrêt rendu le 2 Décembre 1997⁶⁵, c'est-à-dire l'imputabilité de l'acte et sa nécessaire intégrité. Ce n'est que si ces conditions sont satisfaites que l'écrit électronique peut prétendre être placé au même niveau que la preuve littérale. Il s'agit donc bien de l'intégration de la preuve informatique au sein du système probatoire traditionnel afin de conserver l'unité des règles de preuve pour éviter toute opposition stérile entre la nouveauté et la tradition.

⁶⁴ Voir supra.

⁶⁵ Voir supra note n°51.

Cependant, pour que cette assimilation puisse prospérer sans créer de difficultés majeures, il faut tout d'abord que les utilisateurs retrouvent dans la preuve informatique les mêmes garanties qu'offre le support papier et, ensuite, que les règles régissant la preuve sur support papier s'appliquent sans modification à la preuve informatique.

Il a toujours été de bon ton d'opposer le papier à l'informatique sur la question des garanties offertes par l'un et l'autre. La durabilité, l'intégrité, la possibilité d'apposer une signature sur le même support matériel que le texte de l'engagement : voici les garanties offertes par le papier, alors que l'informatique ne présente aucune d'entre elles⁶⁶.

Ainsi, la durabilité d'un document, son intégrité, sa liaison avec un fichier sont subordonnés à l'efficacité des systèmes. Cela nous amène à nous interroger notamment sur la portée de la signature électronique. Nous savons que, sur le support papier, la signature prouve l'identité de celui qui a signé, sauf hypothèse de dénégation de signature.

Reste une deuxième question qui est celle de l'adhésion du signataire au contenu de l'acte : en présence du support papier, cette adhésion n'est que présumée par cette signature.

Or, sur ce point, nous pouvons affirmer que la signature électronique est juridiquement supérieure. En informatique, le procédé de signature électronique peut garantir que celui qui l'actionne valide le contenu du document. Ainsi on pourrait soumettre l'apposition de la signature électronique à une relecture obligatoire, par exemple en obligeant le signataire à déplacer le curseur en bas de document, ce qui laisse présumer qu'il en a pris connaissance. Selon Xavier Linant de Bellefonds, une « validation page par page⁶⁷ » peut être aussi un moyen de présumer l'information.

L'écrit électronique s'inscrivant dans la continuité de l'écrit papier, on peut envisager d'appliquer les règles propres au papier à l'écrit électronique. Toutefois, certaines d'entre elles sont susceptibles de poser des difficultés en raisons des différences entre le papier et l'électronique.

⁶⁶ X. Linant de Bellefonds, « *Internet et la preuve des actes juridiques* ».

⁶⁷ X. Linant de Bellefonds, P.-Y. Gautier, « *de l'écrit électronique et des signatures qui s'y attachent* », JCP Ed. E., 2000, n° 3134, p.1273.

Il existe un seuil, dont le montant est fixé par la loi, en deçà duquel les parties n'ont pas besoin de se préconstituer de preuve par écrit. Ce seuil est fixé à 800€ selon le décret n° 80-533 du 15 Juillet 1980 modifié par le décret n° 2001-476 du 30 Mai 2001⁶⁸.

Cette disposition est justifiée par le fait que pour les petites opérations, il n'est pas nécessaire de prévoir un écrit, car il est nécessaire de simplifier et fluidifier les échanges commerciaux, tout en protégeant le consommateur pour les opérations les plus importantes.

Il ne faut pas voir en l'introduction de la preuve électronique une modification de cette règle : l'obligation de recourir à la signature électronique et à l'écrit électronique devra être soumise à ce seuil. Il ne serait pas justifié de fixer un second seuil, propre à l'écrit électronique, tant les deux écrits tendent à se rapprocher. Toutefois, certains auteurs⁶⁹ attirent l'attention sur le fait que, sur l'Internet, les possibilités de contracter sont beaucoup plus aisées, et qu'il faut pouvoir limiter les engagements à la légère.

Selon l'article 1325 du Code civil, *«les actes sous seing privé qui contiennent des conventions synallagmatiques, ne sont valables qu'autant qu'ils ont été faits en autant d'originaux qu'il y a de parties ayant un intérêt distinct»*. On peut alors se demander si cette règle du double original a vocation à s'appliquer dans un environnement numérique.

En effet, si concernant un support papier la copie n'est jamais identique à l'original car elle utilise un procédé tel que la photocopie ou le papier carbone qui va dégrader l'original, en informatique, la copie numérique va résider le plus souvent en un clonage du fichier.

Le procédé informatique du « copier/coller » va, alors, créer une copie qui sera en tous points identique à l'original. Ainsi, l'exigence d'un double original reviendrait en pratique à apposer deux fois une signature électronique sur deux documents réputés identiques.

Cependant, dans le cadre d'échanges dématérialisés à distance, une simple copie informatique du fichier signé sera satisfaisante dès lors qu'elle contient toutes les données permettant de vérifier l'authenticité de la signature.

De même, on pourrait penser que le message signé électroniquement arrivant sur la messagerie du destinataire ne soit qu'une « copie » de l'original. En effet, le signataire va expédier - via le réseau Internet - un message signé électroniquement. Pour ce faire, il va recourir à un logiciel de messagerie, *Microsoft Outlook Express* sur un environnement PC ou

⁶⁸ J.O. 3 Juin 2001.

⁶⁹ Voir supra note n°57.

Entourage pour un environnement Apple, pour prendre les plus répandus d'entre eux. Ce logiciel va permettre d'apposer sa signature sur le message avant l'expédition. Après expédition, le message originel va résider dans une boîte dénommée « éléments envoyés ». Le destinataire va recevoir le message signé et pouvoir vérifier l'exactitude de la signature, notamment grâce aux renseignements fournis par le prestataire de service de certification électronique.

La question se pose alors de savoir si l'original n'est pas le document envoyé, par opposition avec le document reçu, qui ne serait qu'une copie de l'original ?

Cette question est encore plus évidente si le document est signé avant l'expédition. Ici, le signataire va procéder à la rédaction du document avant de le signer grâce à un logiciel spécifique. Ensuite seulement le message sera expédié.

Dès lors, l'original est sans conteste le document signé de trouvant sur le disque dur de l'expéditeur, le destinataire possédant une copie. L'informatique nécessite un traitement de l'information qui nécessite une reproduction en chaîne – du disque dur à la RAM, traitement par le microprocesseur-, ce qui pose la question de savoir où se trouve le véritable original.

Ainsi, on pourrait retenir ici une définition de l'original comme un document offrant toutes les garanties de l'article 1316-1 du Code civil. Le prestataire de service de certification ou le tiers archiveur pourront alors être considérés comme étant en possession d'un original.

Aussi, il faut considérer que l'impression sur support papier d'un document signé électroniquement constitue une copie, de même qu'un document informatique signé électroniquement mais dont les données permettant la vérification de la signature auraient été détachées de l'acte⁷⁰.

Selon une jurisprudence se fondant sur l'article 1347 du Code civil, « *les copies peuvent valoir comme commencement de preuve par écrit*⁷¹ ». Selon l'étude menée par Messieurs P.-Y. Gautier et X. Linant de Bellefonds⁷², la formalité du double original est en soi remplie dès que la consultation d'un document n'est possible que par l'action simultanée des deux parties. Que le document soit stocké chez une partie ou chez l'autre revient alors au même que si il était stocké chez les deux.

⁷⁰ Encore faut-il ici que l'intégrité de l'acte soit préservée.

⁷¹ Civ 1^{ère}, 27 Mai 1986 : bull. I, n°141 ; Gaz. Pal. 1987. 1. Somm. 54 obs. Croze et Morel; RTD Civ. 1987. 765. obs. Mestre.

⁷² Voir supra n°48.

D'autre part, il existe des cas où il sera impossible de se procurer un écrit. Ces cas sont prévus par l'article 1348 du Code civil : « *les règles ci-dessus [relatives à la preuve testimoniale] reçoivent encore exception lorsque l'obligation est née d'un quasi-contrat, d'un délit ou d'un quasi-délit, ou lorsque l'une des parties, soit n'a pas eu la possibilité matérielle ou morale de se procurer une preuve littérale de l'acte juridique, soit a perdu le titre qui lui servait de preuve littérale, par suite d'un cas fortuit ou d'une force majeure* ».

L'impossibilité peut ainsi être physique, morale, ou résider en la perte de l'écrit informatique.

L'impossibilité physique semble, en premier lieu, ne pas trouver à s'appliquer à l'écrit électronique. En effet, les circonstances classiques telles que la guerre ou un naufrage semblent difficilement transposables à l'univers informatique. Cependant, il faudra rapprocher cette impossibilité de l'évolution du matériel et de la technique. Ainsi, un document qui aura été archivé depuis un certain temps ne sera pas forcément lisible par le matériel dans le futur, le format du document n'étant plus pris en charge. Alors, la conversion en un format supporté peut entraîner une modification de la structure du document, et ainsi, une perte de l'intégrité.

C'est pourquoi, on pourrait envisager un format standard⁷³ pour la conservation des documents électroniques, à l'instar de ce qui est proposé pour la conservation de l'acte authentique électronique⁷⁴. Ici, le prestataire de services de certification ou l'archiviste pourraient faire foi de la concordance entre le document archivé et l'original. On pourrait aussi imaginer que cette situation se rapproche de la perte du document, car il ne serait plus exploitable.

L'impossibilité morale peut dépasser, dans l'environnement numérique, les liens de famille. Ainsi, certains contractants pourraient être opposés au recours à la signature électronique. Cependant, il faut imaginer qu'à terme, ces comportements ne seront plus acceptables. Seules les incertitudes sur la force probante de la signature électronique mise en œuvre pourront justifier l'établissement, en parallèle, d'un écrit papier.

⁷³ Il est envisagé de convertir un document en une image, au sens premier. Ainsi, il en résulterait une sorte de « photographie » du document qui ne serait pas susceptible de modifications. On pense notamment au format *Bitmap*, qui ne serait pas abandonné et constituerait un standard pour la conservation de tous les documents électroniques. L'avantage d'une photographie est évidemment que cela s'adapte à tous les documents écrits. Mais que penser si l'objet de l'engagement est un fichier sonore? Dans ce cas la technique se révélerait inefficace.

⁷⁴ Voir à ce sujet le très détaillé mémoire de S. Bettini sur *l'acte authentique électronique*, mémoire de DESS de Droit du Multimédia et de l'Informatique, promotion 2002-2003, Université Paris II Panthéon Assas.

La perte de l'écrit est l'hypothèse qui risque de se rencontrer le plus fréquemment, les fichiers informatiques étant vulnérables aux pannes de disque dur, aux attaques des virus, aux effacements accidentels et autres sabotages ou piratages.

La loi du 13 Mars 2000 a apporté un changement d'une importance capitale dans notre droit civil en modifiant profondément ses règles de preuve. Cette loi refonde la notion de preuve écrite et s'attaque à l'écrit lui-même.

Cependant, les changements apportés par cette loi sont limités car ils n'ont trait qu'à l'aspect probatoire et la signature des actes juridiques. Les questions concernant la validité desdits actes n'ont pas été abordées. Bien qu'il faille souligner le caractère audacieux des innovations apportées par les nouveaux textes insérés dans le Code civil, nous ne pouvons pas ne pas soulever certaines critiques à propos de certains éléments adoptés par le législateur et ce à la suite de certains membres⁷⁵ du groupe ayant élaboré ce texte.

Pour ce faire, nous allons nous arrêter, dans un premier temps, sur les dispositions de l'article 1316-1, d'après lesquelles « *l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier...* ». Le groupe d'universitaires sus évoqué n'a pas manqué d'insister sur la nécessité de supprimer cette formule, notamment à cause de son inutilité.

En effet, l'écrit électronique n'est pas assimilable à « l'écrit papier » à cause de sa nature différente. L'information portée sur le papier est imprimée de manière irréversible.

En revanche, la même information portée sur le support électronique peut faire l'objet d'une manipulation par toute personne ayant des connaissances ciblées en informatique.

Ensuite, le législateur a inséré l'article 1316-3 dans le Code civil attribuant à l'écrit électronique la même force probante qu'à l'acte sous seing privé.

Ce texte suscite plusieurs remarques.

Tout d'abord, cette disposition vient en redondance avec l'article 1316-1, qui, comme nous l'avons vu plus haut, reconnaît déjà l'équivalence du support papier et du support électronique.

⁷⁵ J. Huet, « *Vers une consécration de la preuve et de la signature électronique* », D. 2000, n°6, p.95.

Ensuite, il ne faut pas perdre de vue l'article 1322 du Code civil, selon lequel l'acte sous seing privé, dès lors qu'il n'est pas contesté, est assimilé à l'acte authentique ; comme de son côté, l'écrit électronique est assimilé à l'acte sous seing privé, rien n'empêche d'assimiler l'écrit électronique qui ne fait l'objet d'aucune contestation à l'acte authentique. De nombreux auteurs nous enseignent le manque de qualité pédagogique de la rédaction de l'article 1322. L'article 1316-3 qui doit lui être relié trouble encore un peu plus. En tout cas, nous devons insister lourdement sur le caractère absolument inadmissible de l'assimilation entre l'écrit électronique et l'acte authentique.

L'arrêté du 31 mai 2002 précise les règles pour reconnaître la qualification d'un prestataire de certification électronique. Cette qualification est importante car elle permet la présomption de la fiabilité d'une signature électronique. L'arrêté du 31 mai 2002 complète le décret du 30 mars 2001 pris en application de l'article 1316-4 du Code civil. Ainsi, le Comité français d'accréditation (COFRAC) et les organismes signataires d'un accord européen sont chargés d'accréditer, pour une durée de deux ans, les organismes qui procéderont à l'évaluation des prestataires.

Dans notre étude sur l'adaptation du droit de la preuve aux technologies de l'information, après avoir abordé la consécration de la preuve électronique, il convient de s'attarder désormais sur la charge de la preuve.

Le nouvel article 288-1 du nouveau Code de procédure civile traite de la signature électronique et dispose : « *Lorsque la signature électronique bénéficie d'une présomption de fiabilité, il appartient au juge de dire si les éléments dont il dispose justifient le renversement de cette présomption* ».

Cette règle de procédure est, à première vue, le prolongement de la présomption de fiabilité de l'article 1316-4 du Code civil, qui est une présomption simple. La signature qui est nécessaire à la perfection de l'*instrumentum* a pour unique résultat d'en faire un acte sous seing privé semblable à un acte sur support papier. Cette présomption de fiabilité ne porte que sur la signature électronique sécurisée. Nous pouvons donc nous interroger sur la valeur d'une signature électronique simple, c'est-à-dire qui ne satisferait pas aux critères de l'article 1316-4 alinéa 2, ou bien d'une signature avancée mais viciée. Il ne fait aucun doute que cette

signature n'est pas dénuée d'une portée juridique. A l'image de la télécopie⁷⁶ ou de la photocopie⁷⁷ à qui ont été reconnues une force probante, la signature électronique simple peut valoir commencement de preuve par écrit. En effet, si la signature électronique ne bénéficie pas de la présomption d'équivalence avec l'écrit papier, elle n'en reste pas moins recevable en justice et peut constituer un commencement de preuve par écrit qui pourra, dès lors, être complété par tous moyens.

C'est à ce stade que l'on retrouve l'article 1322 du Code civil d'après lequel l'acte sous seing privé, sur support papier ou électronique, n'a force probante quant à sa signature et à son écriture que si il est vérifié par le juge ou est reconnu par celui à lequel on l'oppose.

Dans l'hypothèse d'une dénégation de signature ou d'écriture, on applique les principes du droit de la preuve et plus particulièrement ceux concernant la charge de la preuve.

La première chambre civile de la Cour de cassation répète constamment qu'en présence d'une contestation de l'acte sous seing privé, il appartient au juge de procéder à la vérification et il ne peut retenir l'acte contesté que si il a constaté qu'il émane de la partie qui l'a désavoué⁷⁸. La cour suprême vise au grès des arrêts les articles 1315, 1322, 1323, 1324 du Code civil et 287 et 288 du NCPC.

Le nouvel article 288-1 du NCPC cité ci-dessus pose la solution exactement inverse. Remarquons, tout d'abord, que cet article de procédure pose une règle concernant la charge de la preuve et par là même attribue le risque de la preuve, question, qui, en principe relève du fond plus que de la procédure.

De plus, la règle qui l'édicte est contraire à celle qui résulte de la jurisprudence constante de la Cour de cassation et aux articles du Code civil. Elle est propre à l'acte sous seing privé électronique dont le régime est inverse de celui de l'acte sur support papier. Plus grave, ce régime est aligné sur celui de l'acte authentique.

Ainsi la boucle est bouclée et les angoisses des membres du groupe ayant élaboré la loi se révèlent, malheureusement, fondées.

⁷⁶ C. Cass. com., 2 Déc. 1997, JCP éd. G 1998, Actualité p.905, obs. P. Catala et P.-Y. Gautier; D. 1998, jur., p.192, note D.-R. Martin; JCP éd. E 1998, II, 10097, note L. Grynbaum.

⁷⁷ C. Cass. 1^{ère} civ., 14 Fév. 1995 : D. 1995. 340, note S. Piedelièvre; JCP 1995. II. 22402, note Chartier; RTD civ. 1996, 174, obs. Mestre.

⁷⁸ C. Cass 1^{ère} civ. 6 mars 2001, D. 2001, jp p. 1316, obs. Avena-Robardet, 15 Juin 1999, D. 2000, jp p. 359, obs. Libchaber.

Section 2 - Champ d'application.

Il convient de s'interroger sur le domaine d'application de la signature électronique.

Dans un premier temps, nous pourrions penser que ce champ est extrêmement large car il comprend, d'une part, tous types de contrats synallagmatiques qu'ils traitent des choses corporelles ou incorporelles, qu'ils portent sur des droits réels ou personnels ; d'autre part, sont également concernés les actes et contrats unilatéraux. Nous pouvons, à ce titre, citer les reconnaissances de dettes, les différents titres de créance et cautionnements. A cet égard, nous pouvons relever la modification apportée à l'article 1326 du Code civil relatif à la mention manuscrite exigée pour ce type de contrat où la mention « *de sa main* » a été remplacée par les mots « *par lui-même* ».

Cependant, malgré les efforts de l'Union Européenne, notamment dans sa directive *commerce électronique*, pour supprimer les obstacles à la conclusion de contrats en ligne, nous sommes tout de même en droit de constater que nous ne sommes pas passés du jour au lendemain sous le règne du « tout numérique⁷⁹ ». La simple lecture des travaux préparatoires de la loi du 13 Mars 2000 nous apprend que ni le parlement ni le gouvernement, n'ont cherchés, par le biais de cette réforme, à mettre un terme à l'une des distinctions les plus importantes du droit des obligations entre l'écrit requis à titre probatoire (*ad probationem*) et l'écrit exigé à titre de validité (*ad validitatem ou solemnitatem*). Dans cette dernière hypothèse, il est bien entendu qu'en l'absence d'écrit, le contrat est frappé de nullité⁸⁰.

L'exigence de l'écrit *ad validitatem* a pour objectif principal, comme toute autre forme de solennité, la protection du consentement d'une partie, souvent celle considérée comme étant la plus faible.

Néanmoins, cette exigence ne se limite pas aux seuls contrats conclus avec les consommateurs. Elle est également présente pour certaines conventions conclues entre professionnels.

Citons comme exemple la signature des statuts d'une société qui matérialise la conclusion du contrat de société⁸¹, les opérations sur les fonds de commerce telles les ventes, le

⁷⁹ Voir supra note n°67.

⁸⁰ Voir, par exemple, F. Terré, Ph. Simler et Y. Lequette, « *Les obligations* », 8^{ème} éd. D. 2002, n° 136 et s.

⁸¹ Article 1835 du Code civil.

nantissement ; de même, dans le droit cambiaire, l'aval porté sur une lettre de change⁸² ou l'endossement de cette lettre⁸³.

Enfin, on ne peut ne pas évoquer les actes portant cession de brevets⁸⁴ ou de marques⁸⁵.

Il faut relever, dans le même domaine, en matière de contrats de représentation, d'édition et de représentation audiovisuelle, malgré la lettre de l'article L.131-2 du Code de la propriété intellectuelle qui impose une constatation par écrit de ce type de contrat, la jurisprudence a considéré que l'écrit était requis *ad probationem*⁸⁶.

Nous pouvons préciser que cette dichotomie de l'écrit a été conservée pour la simple raison que la loi nouvelle ne précise à aucun moment qu'elle y met fin.

Par ailleurs, un projet d'amendement ayant pour objet la fin de cette distinction a été rejeté. Nous pouvons donc conclure qu'après la loi du 13 Mars 2001, la reconnaissance de l'écrit électronique s'arrête qu'au cas où l'écrit n'est exigé qu'à titre probatoire.

Donc, le papier devait conserver pour un certain temps son monopole car la directive européenne « *commerce électronique* » adoptée en Mai 2000 et traitant, comme son nom le laisse supposer, des contrats électroniques, interdit aux états membres de mettre des obstacles à la pleine reconnaissance de la validité de ce type de contrats (article 9). De là à considérer que la distinction entre l'écrit exigé *ad probationem* et l'écrit exigé *ad validitatem* constitue un tel empêchement, il n'y a qu'un pas qui sera certainement franchi, à n'en pas douter, lors d'une action en manquement contre la France si cette distinction est maintenue telle qu'elle.

Les points de repère ayant ainsi été posés, nous pouvons désormais nous consacrer à l'analyse du projet de loi « *confiance en l'économie numérique* » déposé devant le bureau de l'Assemblée Nationale.

Le chapitre III de ce projet est consacré aux « *contrats par voie électronique* ». L'article 14 de cette loi propose l'insertion dans le Code civil d'un article 1108-1 rédigé comme suit :

⁸² Article L.511-21 du nouveau Code de commerce.

⁸³ Article L.511-8 du nouveau Code de commerce, même si l'hésitation est permise. En effet, la loi impose que la signature de l'endosseur soit apposée à la main alors même que le texte permet que la signature soit apposée par tout procédé non manuscrit.

⁸⁴ Article L.613-8 du Code de la propriété intellectuelle.

⁸⁵ Article L.714-1 du Code de la propriété intellectuelle.

⁸⁶ Cass. civ. 1^{ère} 28 Mai 1963, JCP, II, 13347, note Malaurie.

Lorsqu'un écrit est exigé pour la validité d'un acte juridique, celui-ci peut être établi et conservé sous forme électronique dans les conditions prévues aux articles 1316-1 et 1316-4 et, lorsqu'un acte authentique est requis⁸⁷, au second alinéa de l'article 1317.

Pour des motifs semblables, le projet prévoit l'adoption d'une définition des mentions manuscrites exigées *ad validitatem* par le législateur dans le but de les adapter à un environnement électronique :

Lorsqu' est exigée une mention écrite de la main même de celui qui s'oblige, ce dernier peut l'apposer sous forme électronique si les conditions de cette apposition sont de nature à garantir que la mention ne peut émaner que de lui-même.

Par ailleurs, en conformité avec l'article 9-2 de la directive sur le commerce électronique, le projet propose d'introduire des exceptions dans un article 1108-2 :

Il est fait exception aux dispositions de l'article 1108-1 pour:

- 1° Les actes sous seing privé relatifs au droit de la famille et des successions ;*
- 2° Les actes soumis à autorisation ou homologation de l'autorité judiciaire ;*
- 3° Les actes sous seing privé relatifs à des sûretés personnelles ou réelles, de nature civile ou commerciale, sauf s'ils sont passés par une personne pour les besoins de sa profession.*

Nous avons vu, plus haut, que la doctrine considère, dans sa grande majorité⁸⁸, que le législateur, en l'an 2000, n'avait pas voulu viser les écrit exigés *ad validitatem*. C'est pourquoi, pour les contrats où la présence d'un écrit est une condition de validité, le recours à l'écrit électronique n'aurait pas été possible.

Comme cette interprétation n'était pas conforme à la directive européenne sur le commerce électronique, le gouvernement a décidé de faire évoluer la législation en ce domaine en supprimant toutes interdictions ou restrictions concernant l'utilisation de contrats

⁸⁷ Voir supra note n° 74.

⁸⁸ Voir supra note n° 75 ; L. Grynbaum, « *Projet de loi sur la société de l'information : le régime du « contrat électronique* » », D. 2002, n°4, p.378 ; P. Catala, « *Le formalisme et les nouvelles technologies* », Defrénois 2000, p.897, V. Contrats J. Passa, « *Commerce électronique et protection du consommateur* », D. 2002, n° 6, doct. p. 562.

électroniques, comme l'y enjoint la directive sus évoquée, sans pour autant oublier le cas de certains contrats particuliers qui ne seront pas touchés par cette réforme.

A titre d'exemple, nous pouvons évoquer le cas des contrats de mariage qui sont, en application de l'article 1397 du Code civil, soumis à une homologation judiciaire. Cette intervention du juge a pour fonction de préserver l'intérêt de la famille, c'est-à-dire, faire en sorte que le changement de régime matrimonial des époux ne porte pas atteinte aux intérêts de chaque membre du couple, tout en essayant de concilier cela avec l'intérêt des enfants, sans oublier l'intérêt des créanciers à qui la loi permet d'intervenir pour empêcher toute fraude à leurs droits. De plus, ce contrat de mariage, pour être valable, doit être notarié. Donc, le contrat de mariage recouvre l'*exception numéro 2°* de l'article 1108-2 projeté. L'*exception numéro 3°* vise des contrats tels le cautionnement signé par un consommateur.

Il convient d'expliquer la cause de ces exceptions prévues par la directive et reprises par le gouvernement dans le projet. Prenons le cas des exceptions visées au numéro 1° de l'article 1108-2 et citons, à l'appui de notre démonstration, le cas d'un testament olographe, dont la définition est donnée à l'article 970 du Code civil, selon lequel : « *Le testament olographe ne sera point valable s'il n'est écrit en entier, daté et signé de la main du testateur : il n'est assujetti à aucune autre forme* ». Un testament doit retranscrire l'expression des dernières volontés du testateur. Le formalisme de l'article 970 du Code civil, s'il est respecté garantit l'imputabilité du texte à son auteur. Il faut savoir que ce type de testament est le plus utilisé par les français, car il a le mérite d'assurer une discrétion que ne fournit pas le testament authentique, certes dicté par le testateur mais rédigé par le notaire, en présence de deux témoins (article 971 du Code civil). La jurisprudence, malgré une certaine souplesse pour admettre d'autres types de signature que la signature habituelle, tes les paraphes, n'a néanmoins jamais dérogé à l'*exigence* de l'existence d'une autre signature, car c'est grâce à elle que le testateur fait siennes les mentions qu'il a porté au cœur de l'acte.

Pourquoi alors exclure ce testament du domaine du nouvel article 1108-1 ? Car nous pourrions soutenir que ce qui compte est la signature par le testateur. Dès lors qu'on admet la validité d'une signature électronique, de manière générale, il suffirait de changer la rédaction de l'article 970 et de supprimer la mention « *de la main du testateur* » et la remplacer par la mention « *par le testateur lui-même* », comme cela a été le cas pour l'article 1326.

Or, qui peut prétendre qu'un testament contenu dans un fichier informatique, avec une date, un contenu clair et une signature électronique à bien été conçu par celui à qui on veut l'attribuer ? Il ne faut pas perdre de vue qu'un testament a pour effet de prévoir la dévolution des biens au sein des membres de la famille. Par ailleurs, le testament olographe est celui pour lequel les litiges sont le plus nombreux. Or, admettre la validité d'un testament composé sur un fichier informatique ne pourrait que faire croître les conflits au sein de la famille, après le décès du testateur, par exemple, lorsque l'écriture pose un problème dans un testament olographe, on procède à un examen graphologique. Ceci aurait été, bien entendu, impossible si on avait accepté ce nouveau type de testament. On peut donc raisonnablement penser que les difficultés de preuve et les liens qui unissent les membres d'une famille sont emprunts de sensibilité, parfois de fragilité, parfois exacerbée en période de décès ou de conflit et la modernité de la signature électronique n'a pas pesé lourd face au maintien de l'équilibre complexe qui unit une famille.

Après avoir évoqué le cas de l'écrit électronique *ad validitatem*, attardons nous sur le problème des règles concernant ce que la directive nomme le « *consentement complet et éclairé* ». En effet, l'article 10 de la directive précise les informations qui doivent être fournies afin d'obtenir un tel consentement. Pour atteindre cet objectif, le projet de loi prévoit d'insérer dans le Code civil un nouvel article 1369-1.

Quiconque propose, par voie électronique, la fourniture de biens ou la prestation de services, transmet les conditions générales et particulières applicables d'une manière qui permet leur conservation et leur reproduction. L'auteur de l'offre est tenu par sa proposition tant qu'elle reste accessible par voie électronique.

Par ailleurs ce texte précise les informations à fournir lorsque l'offre est faite à titre professionnel. La directive sur le commerce électronique précise que ces informations doivent être fournies « *de manière claire, compréhensible et non équivoque* », avant que le destinataire ne passe sa commande. Nous ne pouvons que regretter l'absence de précisions dans le projet de loi sur la manière de fournir ces informations. Espérons que les débats parlementaires corrigeront cet oubli.

Cependant, le projet de loi ne s'arrête pas à ce stade, car non seulement il contraint le prestataire à signaler les étapes de la conclusion du contrat et, de plus, il fixe certaines étapes obligatoires. Pour ce faire, le projet souhaite insérer dans le Code civil un nouvel article 1369-2 rédigé comme suit : « *Le contrat proposé par voie électronique est conclu quand le destinataire de l'offre, après avoir eu la possibilité de vérifier le détail de sa commande et son prix total, ainsi que de corriger certaines erreurs confirme celle-ci pour exprimer son acceptation.*

L'auteur de l'offre doit accuser réception sans délai par voie électronique de la commande qui lui a été ainsi adressé. La commande, la confirmation de l'acceptation de l'offre et l'accusé de réception sont considérés comme reçus lorsque les parties auxquelles ils sont adressés peuvent y avoir accès ».

Ce texte suscite plusieurs remarques. Concernant le formalisme, nous pouvons relever que le poids des formalités est allégé par l'intervention de l'informatique.

Néanmoins, nous pouvons d'ores et déjà prévoir, avec peu de risques d'être contredit en pratique, que l'incompréhension du système aura pour conséquence l'existence de nombre d'opérations inachevées. Dans ce cas, les parties, en toute bonne foi, procéderont à l'exécution totale ou du moins partielle des obligations engendrées par le contrat qui, croient ils, les lie.

Quel sort pourra t'on réserver à ces contrats dont la conclusion parfaite sera contestée par la suite ?

Ensuite, nous ne pouvons que constater qu'un contrat sur support papier ne nécessite, pour sa validité, que l'échange de volontés, sous réserves de la preuve de son existence et de son contenu⁸⁹. Dans le même temps, le contrat électronique nécessite plus de formalités que le simple échange des volontés.

Notons, cependant, qu'un nouvel article 1369-3 est prévu, pour permettre, par dérogation, au deux premiers alinéas de l'article 1369-2, que les contrats de fourniture de biens ou de prestations de services puissent être conclus exclusivement par échanges de courriers électroniques, et ce, conformément au droit commun des obligations. De même, le même article prévoit que si les parties en relations d'affaires le conviennent, elles pourront, conclure

⁸⁹ « *Idem est non esse e non probari* » ; ce qui n'est pas prouvé n'existe pas.

entre elles des contrats par voie électronique sans que le prestataire doive proposer un système de « *double clic* » suivi d'un accusé de réception. Là encore, on constate un retour au droit commun des obligations.

Nous avons, ainsi, relevé que l'intérêt de ce texte, ainsi que ces lacunes.

Il convient alors d'étudier les conventions de preuve et le conflit de preuves littérales dans le cadre d'un recours à la signature électronique.

Le dispositif ainsi mis en place a été complété par des règles supplétives applicables aux conflits de preuves littérales. Ainsi, l'article 1316-2 du Code civil dispose :

Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérales en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support.

La concision de cette phrase peut étonner mais cette phrase unique apporte plusieurs enseignements. L'étude de cette phrase peut être menée en trois temps.

Le premier consiste en son caractère supplétif. C'est le législateur qui doit, en premier lieu, organiser la hiérarchie des forces probantes. Cette affirmation découle du début de l'article : « *lorsque la loi n'a pas fixé d'autres principes...* ». On peut trouver bien d'autres exemples dans d'autres matières que celle dont nous traitons : l'article 322 alinéa 2 du Code civil, lu à l'endroit, met en place le caractère irréfragable de la filiation légitime en présence d'une possession d'état conforme au titre de naissance de l'enfant ; l'article L.131-10 alinéa 1^{er} du Code monétaire et financier affirme la priorité de la somme écrite en lettre sur les sommes écrites en chiffres en cas de mention différente apposée sur un chèque.

Ces premiers mots de l'article 1316-2 laissent le champ libre au pouvoir législatif ou réglementaire pour l'adoption d'une réglementation particulière dont la nécessité se fera jour au fur et mesure que des mutations techniques affecteront la fiabilité des modes de conservation de données et de communication.

Le deuxième temps est celui de l'introduction des conventions sur la preuve comme source de dispositions ayant pour objectif de prévenir les conflits de preuves littérales. L'article 1316-2 du Code civil n'affirme à aucun moment la validité de principe de ce type de conventions. Conformément à l'article 1134 alinéa 1^{er}, elles ne peuvent déroger aux règles légales impératives. L'appréciation de leur validité, aujourd'hui comme demain, incombera au juge. La jurisprudence avait déjà reconnu un rôle à ce type de conventions élaborées par les parties. La disposition contenue dans l'article 1316-2 peut être considérée comme un texte de consolidation car ce type de convention, conforté désormais par un article du Code civil, aura la possibilité d'avoir, dans l'ordre probatoire, le même rôle que celui que lui a déjà accordé la jurisprudence.

Nous savons que les professionnels et une partie de la doctrine ont prôné la solution contractuelle comme étant la mieux adaptée à l'échange électronique de données. Ceux-ci insistent sur l'avantage conféré par l'apparente souplesse de ce mode de preuve qui laisse les parties elles-mêmes organiser leurs relations. Cependant, cet avantage est contrebalancé par nombre de faiblesses. Prenons le cas d'une opération pour la réalisation de laquelle un ordre est donné à un établissement boursier, et ce, en dehors de toute relation d'affaire régulière. En ce cas, comme dans bien d'autres, aucune convention ne lie préalablement les parties à l'échange électronique. Malgré la naissance d'un contrat, il n'existe aucune stipulation régissant la manière dont l'échange pourra se prouver. Quand bien même il existerait une convention organisant les relations entre les parties, une simple étude sommaire nous permet d'affirmer qu'elle se limite généralement à l'affirmation selon laquelle « *les enregistrements informatiques feront foi de leur contenu*⁹⁰ ». Ceci signifie que l'un des deux contractants aura la charge de la preuve du caractère erroné de ces enregistrements. Encore pire, si nous interprétons littéralement une telle clause, elle aurait pour conséquence⁹¹ l'interdiction pure et simple de la démonstration de leur caractère erroné. Ce type de convention ne constitue qu'un pis aller. En effet, nous pouvons nous demander quels sont les moyens qui sont à la disposition de celui qui doit apporter la preuve contraire, pour établir la réalité des faits.

⁹⁰ Cependant, les systèmes informatiques, aussi fiables soient ils, ne sont pas à l'abri de dysfonctionnements. Dans de telles clauses, ceux-ci ne sont pas envisagés. Même si l'on peut concevoir que rapporter la preuve du dysfonctionnement pourra faire échec à une telle clause, cela sera quasiment impossible en pratique.

⁹¹ J. Huet, « *Formalisme et preuve en informatique et télématique : éléments de solution en matière de relations d'affaire continues ou de rapports contractuels occasionnels* », JCP éd. G, I, 1989, n°33-37, p.3406.

Par ailleurs, rares sont les conventions qui mettent en place les obligations d'information réciproques pour prévenir les incidents. Il est évident qu'il serait contraire à l'ordre public d'imposer de tenir toujours pour exacts les enregistrements informatiques dont on allègue l'existence. C'est pourquoi, une lecture littérale de ce type de clause, qui interdirait que soit apportée une preuve de la réalité de ce qui s'est passé, est à rejeter. Le règlement des conflits de preuves par des clauses telles celles que nous venons d'évoquer, apparemment très claires, ne font qu'attiser les oppositions et les conflits entre les parties. Ceci revient à surcharger les tribunaux, ce qui n'est bien entendu pas ce qui est recherché par les parties qui s'en remettent aux moyens informatiques pour réaliser des échanges d'informations ou de données.

Enfin, en troisième lieu, il convient de s'interroger sur l'hypothèse où il n'existe ni règle légale, ni convention valable entre les parties. En ce cas, les tribunaux retrouvent leur entière liberté pour régler le conflit de preuves. Le texte précise qu'ils doivent déterminer : « ...*par tous moyens le titre le plus vraisemblable, quel qu'en soit le support* ». Nous retrouvons ici une recommandation, déjà largement éprouvée dans d'autres domaines du droit.

Nous citons à l'appui de cette affirmation la formule utilisée dans l'article 311-12 du Code civil qui a trait au règlement des conflits de filiation selon laquelle les tribunaux règlent ces conflits « *en déterminant par tous moyens de preuve la filiation la plus vraisemblable* ». De même, dans les conflits sur la propriété, la jurisprudence affirme constamment le pouvoir du juge de la revendication pour dégager les présomptions de propriété « *les meilleures et les plus caractérisées* » dans sa recherche du droit le plus probable⁹².

En l'absence de loi et de contrat dont les dispositions permettraient de régler ce conflit de preuves littérales, il n'existe plus que l'intime conviction du juge, sinon, nous serions en présence d'un déni de justice en la matière.

La validité des conventions de preuve électronique a été reconnue par le juge à l'occasion d'une affaire *Crédicas*⁹³. Il s'agissait ici de l'utilisation d'un code secret pour l'utilisation d'une carte bancaire. Selon la convention de preuve, la saisie du code en complément de l'utilisation de la carte permet de présumer que l'ordre de paiement a bien été effectué par le titulaire de la carte. Cette décision reconnaît la validité des conventions de preuve envisagées

⁹² Cass. 3^{ème} civ., 12 juillet 1977, Bull. Civ. III, n°311.

⁹³ Voir supra note n°5.

précédemment et, par voie de conséquence, prend en compte le procédé de signature électronique choisi comme mode de preuve.

Cette preuve sera administrée par le prestataire de services de certification dont il convient à présent d'étudier le régime de responsabilité.

Chapitre II - La responsabilité des prestataires de service de certification électronique.

Le prestataire de service de certification est un des éléments clés de la signature électronique. La délivrance du certificat va permettre d'identifier la personne physique ayant apposé la signature. En effet, cette délivrance est effectuée après un contrôle d'identité, plus ou moins renforcé, en fonction du type de signature envisagé.

De même, les services cryptographiques offerts par les prestataires de service de certification vont permettre d'assurer l'indéfectibilité de la signature avec l'acte, et l'intégrité.

Le décret du 30 Mars 2001 ne traite pas du régime de responsabilité des prestataires de services de certification électronique. C'est une de ses lacunes. Le régime de leur responsabilité n'est abordé que dans la directive du 13 Décembre 1999. Nous pouvons donc penser que, durant cette période transitoire, le droit commun de la responsabilité fondé sur les articles 1147 et 1382 du Code civil s'appliquera aux prestataires de services de certification.

Le prestataire de service de certification est appelé à être un des acteurs essentiels de la signature électronique. A ce titre, le prestataire de service de certification, qui est avant tout un prestataire de services, est soumis au régime commun de la responsabilité civile, que celle-ci soit contractuelle (Section 1) ou délictuelle (Section 2), pour les fautes qu'il pourrait commettre à l'occasion de son activité.

Section 1 - Responsabilité contractuelle (le porteur du certificat).

Le prestataire de service de certification et le signataire, a qui est remis le certificat, ont préalablement conclu un contrat. Ce contrat sera généralement qualifié de contrat d'abonnement par le prestataire et va définir les conditions de délivrance du certificat.

Selon le principe de non cumul des responsabilités délictuelles et contractuelles, l'article 1382 du Code civil est inapplicable à la réparation d'un dommage se rattachant à l'exécution d'un engagement contractuel⁹⁴. Ainsi, un signataire victime d'un dommage ne pourra pas engager la responsabilité délictuelle du prestataire. Seule sa responsabilité contractuelle pourra être engagée.

Dès lors, l'existence du droit à réparation dépend de trois conditions : une faute contractuelle, un dommage et un lien de causalité entre cette faute et ce dommage.

La faute consiste en une inexécution -fautive- d'une obligation contractuelle.

Ainsi, il faudra connaître la nature de l'obligation du prestataire, obligation de moyen ou de résultat, pour déterminer la charge de la preuve. Pour ce faire, il faut se référer au contrat conclu entre le prestataire et le signataire.

Plus généralement, le contrat ayant pour objet la délivrance d'un certificat pourra s'analyser en un contrat d'entreprise. Ainsi, les obligations à la charge du prestataire seraient plutôt des obligations de moyen, et la preuve devrait, alors, être rapportée par le signataire.

La qualification en un contrat d'entreprise peut paraître favorable aux prestataires de services de certification.

Cependant, une interprétation extensive du premier alinéa de l'article 40 du projet de transposition de la directive de 1999 pourrait entraver cette qualification protectrice.

« Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes physiques ou morales prestataires de services de certification électronique ou fournissant d'autres services liés aux signatures électroniques sont présumées responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats qu'elles délivrent. »

⁹⁴ Civ. 2^{ème}, 9 Juin 1993 : JCP 1994, II, 22264, note Roussel, Civ. 11 Janv. 1922, GAJC, 11^{ème} éd., n°177 ; DP 1922. 1. 16 ; S, 1924. 1. 105, note Demogue.

Elles ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites aient été clairement portées à la connaissance des utilisateurs dans le certificat. »

Ici, le signataire pourrait être considéré comme « *une personne se fiant raisonnablement aux certificats qu'elles délivrent* ».

Cependant, l'usage du pluriel pour « les certificats » peut laisser penser que cette disposition s'adresse aux destinataires. En effet, les destinataires vont être amenés à vérifier régulièrement les signatures grâce aux certificats, tandis que l'expéditeur –signataire- ne disposera que d'un certificat, le sien. Plus vraisemblablement, l'usage du pluriel vise l'activité du prestataire tournée vers la délivrance de certificats.

Dans ce cas, le prestataire aurait la charge d'apporter la preuve de son absence de faute intentionnelle ou de négligence.

De plus, de nombreuses obligations sont mises à la charge du prestataire par les textes réglementaires et législatifs. Ainsi, la précision et le caractère impératif de ces dispositions pourrait tendre à faire peser sur le prestataire une obligation de résultat.

En effet, le Décret du 30 Mars 2001, en son article 6, II fixe de nombreuses obligations aux prestataires de services de certification délivrant des certificats qualifiés:

- a) faire la preuve de la fiabilité des services de certification électronique qu'il fournit ;*
- b) assurer le fonctionnement, au profit des personnes auxquelles le certificat électronique est délivré, d'un service d'annuaire recensant les certificats électroniques des personnes qui en font la demande ;*
- c) assurer le fonctionnement d'un service permettant à la personne à qui le certificat électronique a été délivré de révoquer sans délai et avec certitude ce certificat (...)*

Toutefois, l'aménagement contractuel peut être un moyen pour le prestataire de limiter sa responsabilité, en particulier pour l'usage du certificat. En effet, les conditions d'utilisation du certificat peuvent être précisées, et limitées, dans le contrat. Dans ce cas, une information claire du signataire permettra de démontrer qu'il en avait eu connaissance.

Dès lors, il peut y avoir un partage ou une exclusion de la responsabilité du prestataire si le signataire commet une faute dans l'utilisation qu'il fera du certificat⁹⁵.

La négligence fautive du prestataire peut, par exemple, permettre à un tiers de signer frauduleusement ou entraîner la création d'un certificat dont les informations seraient erronées. La faute de l'utilisateur peut avoir pour origine une utilisation non conforme du certificat, notamment lorsque l'usage qui en est fait dépasse les limites des transactions pour lesquelles il était prévu.

En cette matière, le dommage subit doit être direct et certain. Selon l'article 1150 du Code civil, « *le débiteur n'est tenu que des dommages et intérêts qui ont été prévus ou qu'on a pu prévoir lors du contrat, lorsque ce n'est point par son dol que l'obligation n'est point exécutée* ». Nul doute que les contrats du prestataire – contrats d'adhésion pour les consommateurs- tenteront de limiter ce champ de prévisibilité. Aussi, au cas où l'algorithme viendrait à être brisé, ceci pourrait s'apparenter, dans un premier temps, à un cas de force majeure. En effet, selon l'article 1148 du Code civil, à l'impossible nul n'est tenu : « *Il n'y a lieu à aucuns dommages et intérêts lorsque, par suite d'un cas de force majeure ou d'un cas fortuit, le débiteur a été empêché de donner ou de faire ce à quoi il était obligé, ou fait ce qui lui était interdit* ». Cependant, dans un second temps, le prestataire négligent qui continue à utiliser un procédé technique dont les failles ont été démontrées pourrait voir sa responsabilité engagée.

La validité des clauses limitatives de responsabilité a été admise sur le fondement de l'article 1150 du Code civil. Les contrats des prestataires feront donc recourt à ces clauses limitatives de responsabilité.

Cependant, selon certains auteurs⁹⁶, la validité de telles clauses est relative, notamment dans trois cas de figures :

- Tout d'abord, il existe une exclusion générale en cas de faute lourde ou dolosive,
- Ensuite, depuis l'arrêt Chronopost, les clauses limitatives ou exonératoires de responsabilité ayant pour effet de priver de cause l'une des obligations essentielles du

⁹⁵ Cette situation est à rapprocher du contrat porteur des utilisateurs de cartes bancaires, d'après lequel le possesseur de la carte ne doit pas conserver son code et sa carte au même endroit, ni même divulguer son code à quiconque.

⁹⁶ B.Liard, « *La responsabilité des prestataires de services de certification* », Comm. com. électr., Nov. 2002, n°26, p. 14.

contrat doivent être réputées nulles et non écrites. Ici, une disposition limitant la réparation du préjudice subi du fait du non respect des délais de livraison au prix du transport avait été annulée.

Ainsi, une clause limitant la responsabilité du prestataire au prix payé pour l'obtention du certificat devra être réputée nulle si elle a pour conséquence de priver le certificat de sa valeur dans le processus de création de la signature.

- Enfin, il convient de faire attention aux clauses abusives qui pourront être insérées dans les contrats des prestataires. En cas de déséquilibre significatif entre les droits et obligations des parties au contrat, la clause en question sera réputée nulle et non écrite. Ces dispositions issues des articles L. 132-1 à L. 134-1 du Code de la consommation ont vocation à s'appliquer aux rapports entre les professionnels et consommateurs ou professionnels n'agissant pas dans la même spécialité.

Enfin, il convient de préciser que le prestataire de services de certification est soumis à une exigence de protection des données personnelles. Les données afférentes à la personne seront le plus généralement celles du signataire. Ainsi, le recours à un pseudonyme ne devra pas laisser transparaître l'identité réelle du signataire, et le « droit à l'anonymat » devra être préservé. Aussi, le prestataire se doit de prendre toutes les mesures utiles pour éviter une intrusion frauduleuse dans ses bases de données.

Le mécanisme de la responsabilité civile contractuelle du prestataire ayant été étudié, il convient à présent d'envisager sa responsabilité à l'égard des tiers, c'est-à-dire sa responsabilité délictuelle.

Section 2 - Responsabilité délictuelle (l'utilisateur du certificat).

Nous avons vu précédemment que le prestataire de service de certification et le signataire, porteur du certificat, étaient liés par un contrat. En revanche, les relations entre l'utilisateur du certificat (le destinataire) et le prestataire ne ressortent pas du domaine contractuel. Ainsi, le destinataire qui serait victime d'un dommage (en relation avec l'utilisation d'un certificat) pourra engager la responsabilité civile délictuelle du prestataire sur le fondement de l'article 1382 du Code civil.

Sur le modèle de la responsabilité civile contractuelle, le destinataire devra démontrer l'existence d'une faute, d'un préjudice et d'un lien de causalité entre la faute et le préjudice.

Contrairement à la responsabilité civile contractuelle, le destinataire devra apporter la preuve du dommage dû à la faute du prestataire. En effet, il ne pèse pas sur le prestataire d'obligation de moyen ou de résultat dans la mesure où les parties ne sont liées par aucun contrat. Ainsi, la loi du 13 Mars 2000 et le décret du 30 Mars 2001 déterminent les obligations du prestataire à l'égard du destinataire. De plus, le manquement aux obligations contractuelles, c'est-à-dire vis-à-vis de l'émetteur peut avoir des incidences sur le destinataire. Ainsi, la faute à l'égard de l'émetteur pourra permettre, dans certains cas, de justifier le dommage subi par le destinataire⁹⁷.

La preuve de la faute sera vraisemblablement difficile à rapporter. En effet, la signature électronique met en œuvre des dispositifs informatiques complexes, c'est pourquoi, il sera la plupart du temps nécessaire de recourir à une expertise judiciaire. De plus, le destinataire n'a pas accès au système et infrastructures du prestataire, si bien qu'il ne pourra pas directement démontrer la faute du prestataire.

Alors, pour faciliter l'administration de la preuve par le destinataire, la directive n°1999/93/CE du 13 Décembre 1999 prévoit en son article 6 une responsabilité quasi automatique - presque une garantie - du prestataire délivrant des certificats qualifiés dans la mesure où ce sera à ce dernier de démontrer une absence de négligence de sa part. Ces dispositions sont donc, à priori, favorables aux utilisateurs de la signature électronique, et le prestataire semble astreint à un régime particulier de responsabilité.

Toutefois, il dispose de certains moyens de s'exonérer de sa responsabilité. Le prestataire pourrait opposer au destinataire le non respect fautif des limites⁹⁸ d'utilisation du certificat. Cependant, quelques inquiétudes peuvent naître de l'absence de dispositions fixant une « *ligne de conduite* » à tenir par le destinataire. En effet, les limitations contenues dans le certificat pourraient ne pas être opposables au destinataire dans la mesure où aucun contrat ne le lie avec le prestataire.

⁹⁷ Voir en ce sens, mais dans le domaine médical, un exemple de l'application de la responsabilité d'un débiteur contractuel à l'égard des tiers victimes d'une inexécution contractuelle, *Cass. Civ. 1^{ère}, 13 Fév. 2001 : KCP G, II, 10099, note C. Lisanti-Kalczynski*.

⁹⁸ Les limites du certificat sont généralement définies par le montant maximal autorisé pour une transaction, ou la date de validité entre autres.

Alors, le destinataire auquel ne pourrait être reproché aucune faute n'aurait qu'à prouver son préjudice réparable, c'est-à-dire direct et certain. Il est possible d'envisager dès maintenant certains des préjudices qui pourraient être subis par le destinataire : virus ou vice de conception entraînant un défaut dans le certificat, certificat erroné entraînant une erreur sur la personne, etc. Les exemples sont nombreux.

Le préjudice subi par le destinataire doit lui être propre, c'est-à-dire que celui-ci ne peut pas se prévaloir du préjudice subi par le signataire.

Ainsi, la responsabilité délictuelle exclu toute limitation de la responsabilité, par exemple à un montant fixé au prix du certificat. Ceci serait contraire à l'ordre public, et le prestataire devra réparer entièrement le préjudice subi par le destinataire.

Ainsi, on peut en conclure que l'activité de prestataire de services de certification soit, sur de nombreux points, risquée. En effet, ce sont des acteurs à responsabilité aggravée car celui qui subit un dommage peut engager la responsabilité du prestataire sans avoir à prouver sa faute. Le prestataire va donc devoir offrir certaines garanties financières, ou souscrire à une assurance civile professionnelle.

Alors, la solution pourrait être la contractualisation du rapport entre le prestataire et le destinataire. Cette solution permet d'en revenir à la responsabilité contractuelle et de limiter l'indemnisation au préjudice prévisible lors de la conclusion du contrat. De plus, cela peut permettre de limiter contractuellement la responsabilité du prestataire. Toutefois, une clause limitative ou évasive de responsabilité visant le destinataire ne pourra pas être insérée dans le contrat liant le prestataire et le signataire. En effet, l'article 1165 du Code civil pose le principe de l'effet relatif des contrats. Une telle disposition ne saurait donc s'imposer à un tiers tel que le destinataire. Alors, le lien contractuel recherché pourrait naître de l'utilisation du certificat. En effet, l'acceptation puis l'installation du certificat du signataire par le destinataire pourrait être l'occasion pour le prestataire de soumettre cette procédure à l'acceptation d'un contrat d'adhésion ayant pour finalité de limiter la responsabilité du prestataire.

Toutefois, ce serait soumettre la signature électronique à une nouvelle contrainte, cette fois-ci supportée par le destinataire, qui risque de nuire à son développement.

CONCLUSION

A l'issue de notre étude, nous pouvons en conclure que la signature électronique doit être perçue comme le prolongement de l'écrit papier. Ce type de signature s'inscrit dans la continuité et ne révolutionne rien en soi. Cependant, les possibilités offertes par la reconnaissance des signatures électroniques sont nombreuses. A titre d'exemple, la société Deedigital a récemment mis au point un logiciel de création de contrats électroniques. Pendant que l'internaute passe une commande via son explorateur internet, le logiciel crée des séquences vidéo qui seront ensuite signées numériquement. Les conditions générales de vente y seront également insérées. Le fichier peut alors jouer le rôle de contrat électronique selon l'article 1316 du Code Civil.

Enfin, il apparaît selon nous que le succès de la signature électronique est conditionné par la simplicité de sa mise en oeuvre. Or ce n'est pas le cas actuellement.

En effet, la procédure fait intervenir beaucoup trop d'acteurs (tiers certificateur, tiers archiveur, tiers horodateur, autorité d'enregistrement, autorité de certification, ...) et beaucoup trop de textes, tant législatifs que réglementaires, qui, toutefois, paraissent nécessaires. Il faut, ainsi, tendre vers la simplification car le modèle ne serait, selon certains experts, pas viable économiquement. De même, tout cet échafaudage juridico-technique ne repose aujourd'hui, de facto, que sur la cryptographie à clés asymétriques. Or, lorsque l'on connaît la vitesse avec laquelle l'état de l'art est susceptible d'évoluer en informatique, ainsi que la rapidité quasi exponentielle avec laquelle la puissance de calcul des ordinateurs augmente, on est en droit de douter de la pérennité du système. La preuve en est que le protocole SSL- Secure Socket Layer-, utilisé pour les paiements en ligne et le commerce électronique, a été cassé par des chercheurs suisses. Certes ce protocole a été rapidement patché pour combler la faille découverte, mais cela démontre la fragilité des systèmes.

Ainsi, technicité et sécurité risquent d'être les deux obstacles majeurs au développement de la signature électronique. Cependant, la solution se trouve peut être dans le recours à la biométrie. Ce procédé pourrait, en effet, modifier le rôle du prestataire de services de certification qui n'aurait qu'à certifier la coïncidence entre les données biométriques et

l'identité de la personne, à moins que ces services soient gérés par le biais des nouvelles cartes d'identité nationale dématérialisées, ce qui ferait de l'Etat le plus grand prestataire de services de certification de France.

Dès lors, le problème de la sécurité persiste : à l'image des contrefaçons de cartes bancaires par captation des données contenues par la bande magnétique, il pourrait être possible par un expert en informatique de capter les données biométriques de l'individu pour usurper son identité, ce qui apparaît extrêmement grave.

BIBLIOGRAPHIE

OUVRAGES

- *La signature électronique, Introduction technique et juridique à la signature électronique à la signature sécurisée. Preuve et écrit électronique*, par T. PIETTE-COUDOL, Ed. Droit@Litec, Coll. Découvrir, 1ère édit.
- *Vive la signature électronique*, par I. RENARD, Ed. Delmas Express, éd. Avril 2000.
- *Sécuriser ses échanges électroniques avec une PKI : solutions techniques et aspects juridiques*, par T. AUTRET, L. BELLEFIN, M.-L. OBLE-LAFFAIRE, Ed. Eyrolles, Coll. Solutions d'entreprises, éd. Janv.2002.

PRINCIPAUX ARTICLES (Classés par ordre alphabétique des auteurs) :

- *La signature électronique en France, Etat des lieux*, par T. ABALLEA, D. 2001, p. 2385 ;
- *Signature électronique : la réforme aura-elle accouchée d'une « souris » ?* , par Y. BRULARD et P. FERNANDEZ, Petites affiches, 25 Oct.2001, p 8 et 26 Oct. 2001, p. 4 ;
- *La loi française sur la preuve et la signature électronique dans la perspective européenne*, par E. CAPRIOLI, JCP Ed. G, 3 Mai 2000, n°18, p.787 ;
- *La directive européenne n°1999/93/CE du 13 Décembre 1999 sur un cadre communautaire pour les signatures électroniques*, par E. CAPRIOLI, Gaz. Pal. 29-31 Oct. 2000, p.1842.
- *L'introduction de la preuve électronique dans le Code civil*, Etude par un « groupe d'universitaire »: CATALA, GAUTIER, HUET, DE LAMBERTERIE, LINANT DE BELLEFONDS, LUCAS, LUCAS DE LEYSSAC, VIVANT, JCP éd. G 1999, I, p.182 ;

- *Transactions en ligne, preuve et signature électronique : le nouveau cadre juridique*, par L. COSTES, Bull. Lamy, Fév. 2000 (J), n° 122, p.1 ;

- *La mise en œuvre effective du nouveau dispositif relatif à la signature électronique conditionnée à la parution de différents arrêtés et aux apports attendus de la future loi sur la société de l'information*, par L. COSTES, Bull. Lamy, Mai 2001, n°136, p.1 ;

- Vers une signature électronique juridiquement maîtrisée (à propos de l'arrêté du 31 Mai 2002)*, par F. COUPEZ, avec la participation de C. GAILLIEGUE, Comm. Com. élect. Nov. 2002, p.8 ;

- *Révolution Internet: le dédoublement de l'écrit juridique*, par P.-Y. GAUTIER, D. 2000, n°12, p.V ;

- *De l'écrit électronique et des signatures qui s'y attachent*, par P.-Y. GAUTIER et X. LINANT DE BELLEFONDS, JCP Ed. E 2000, p. 1273 ;

- *Vers une consécration de la preuve et de la signature électronique*, par J. HUET, D.2000, n°6, p .95 ;

- *Droit de la preuve et signature électronique : Rapport de M. Charles JOLIBOIS au nom de la commission des lois du Sénat*, Bull. Lamy, Fév. 2000 (J), n° 122, p.13 ;

- *Le décret du 30 Mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique*, par E. JOLY-PASSANT, Sup. Bull. Lamy, Juin 2001, n°137, p.1 et revue Lamy Aff., Juillet 2001, n°40, p.21 ;

- *Preuve et signature: les innovations du droit français*, par I. DE LAMBERTERIE, Bull. Lamy, Mars 2000 (K), n°123, p.9 ;

- *Le décret du 30 Mars 2001 relatif à la signature électronique : lecture critique, technique et juridique*, par I. DE LAMBERTERIE et J.-F. BLANCHETTE, JCP éd. E, 2001, p.1269 ;

- *Le nouveau droit civil et commercial de la preuve et le rôle du juge*, par P. LECLERCQ, Comm. com. électr. Mai 2000, p.11, Chron. 9 ;

- *Commerce électronique : vers la sécurité juridique dans le Marché intérieur*, par S. MUNOZ, Cahiers Lamy Inf. (K), n°123, Mars 200, p.2 ;

- *La loi du 13 Mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique : nouvelle donne pour le droit de la preuve*, par E. PASSANT, Bull. Lamy, Mai 2000 (D), n°125, p.7 ;

- *Les « noces » du droit et de la technique : présentation du décret du 30 Mars 2001 relatif à la signature électronique*, par C. RETORNAZ, Cahiers Lamy (B), Mai 2001, n°136, p.7 ;

- *Signature électronique et acte authentique : le devoir d'inventer*, par B. REYNIS, JCP éd. N, 12 Oct. 2001, p.1494 ;

- *Un projet de loi sur la preuve pour la « société de l'information »*, par M. VIVANT, Bull. Lamy, Août Sept. 1999 (E), p.1 ;

PLAN

INTRODUCTION	3
TITRE I	7
LA CREATION DE LA SIGNATURE ELECTRONIQUE	7
CHAPITRE I - NECESSITE DE GARANTIR L'IDENTIFICATION DU SIGNATAIRE. ..	7
<i>Section 1 - Un moyen sous le contrôle direct du signataire.</i>	7
<i>Section 2 - Le certificat : « pièce d'identité » dématérialisée.</i>	11
CHAPITRE II - NECESSITE DE GARANTIR L'INTEGRITE DU DOCUMENT.	15
<i>Section 1 - Intégrité et vérification de la signature : le lien avec l'acte...</i> ..	15
<i>Section 2 - L'intégrité dans le temps : l'archivage.</i>	18
TITRE II	23
LA MISE EN ŒUVRE DE LA SIGNATURE ELECTRONIQUE	23
CHAPITRE I - FORCE PROBANTE DE LA SIGNATURE ELECTRONIQUE	23
<i>Section 1 - L'écrit électronique équivaut à l'écrit sur support papier</i> <i>(présomption de fiabilité).</i>	24
<i>Section 2 - Champ d'application.</i>	33
CHAPITRE II - LA RESPONSABILITE DES PRESTATAIRES DE SERVICE DE CERTIFICATION ELECTRONIQUE.	42
<i>Section 1 - Responsabilité contractuelle (le porteur du certificat).</i>	43
<i>Section 2 - Responsabilité délictuelle (l'utilisateur du certificat).</i>	46
CONCLUSION	49
BIBLIOGRAPHIE	51