PREUVE ET SIGNATURE

La preuve est le moyen d'invoquer la réalité d'une prétention pour en obtenir, le cas échéant, la protection et la reconnaissance en justice afin de s'en prévaloir et de la faire valoir. La loi énumère et réglemente les moyens de preuve admissibles et leur force probante : écrits, titres, témoignages, aveux, serments, présomption de fait...

La première distinction se fait entre la preuve du fait et celle de l'acte juridique. En droit français, la preuve des faits juridiques est libre. Peu importe le caractère numérique ou informatisé de la preuve, l'essentiel étant de distinguer le fait de l'acte[1]. Quant à la preuve de l'acte juridique, notamment du contrat, elle est encadrée par des dispositions normatives.

Ainsi, **l'article 1341 du code civil** dispose que dès l'instant où l'enjeu d'une affaire dépasse **le seuil de 5.000 Francs**[2] et met en scène, soit une **convention entre particuliers, soit un acte mixte, seules les preuves écrites seront recevables** dans le cadre du débat judiciaire[3]. En revanche, la preuve est libre dans le cadre de relations entre commerçants[4] .

L'écrit permet donc de se pré-constituer des preuves, notamment relatives à la relation contractuelle. Pourtant, une fois encore une large place est laissée au principe d'autonomie de la volonté puisque les parties peuvent organiser conventionnellement les modalités probatoires qui régiront leur relation contractuelle :

> **Article 1316-2 :**
> « *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 littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support.* »

Les règles de preuve ne sont donc pas d'ordre public. Il importe cependant d'analyser la place de l'écrit dans le droit de la preuve français à la lumière des nouvelles dispositions introduites par la loi du 13 mars 2000[5] modifiant le chapitre VI du titre III du livre III du code civil qui a trait à la preuve des obligations. En effet, l'écrit qui fut toujours appréhendé par rapport à son

---

[1] Pour des illustrations voir : Catala.N, « *la nature juridique du paiement* » LGDJ 1961 et X.Linant de Bellefonds, « *rapport introductif à l'informatique et droit de la preuve* », éd Parques, 1987, p.17.
[2] Décret 80-533 du 15 juillet 1980. J.O.R.F du 16 juillet.
[3] C'est l'idée exprimée exprimée par l'adage : « *Idem est non esse aunt non probari* » : « ne pas être ou ne pas être prouver, c'est tout un »
[4] Article 109 du Code de commerce.
[5] Loi 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique in J.O.R.F 14 mars 2000 p.3968.

support physique, le papier, peut désormais recouvrir de nouvelles formes, notamment électroniques.

Il faut donc préciser les définitions d'écrit et de preuve écrite et leurs conséquences juridiques au regard des conflits de preuve littérale, de la notion d'écrit exiger « ad validitatem » et de l'acte authentique avant de consacrer des développement spécifiques à la signature électronique[6].

1. L'écrit et la preuve informatique

1.1 L'écrit en droit français

Grâce à la loi du 13 mars 2000, nous avons pour la première fois une définition de la notion de l'écrit :

> **Article 1316 :**
> « La preuve littérale ou 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 modalité de transmission. »

Cette définition permet d'englober les futurs écrits produits, à partir d'ordinateurs de nouvelle génération[7]. Elle consacre **une approche fonctionnelle de l'écrit.** Cette consécration était annoncée depuis un arrêt de la chambre commerciale de **la Cour de cassation du 2 décembre 1997**[8] qui jugeait qu'un écrit « *peut 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 respectées ou ne sont pas contestées.* »

L'écrit est désormais défini en droit français en termes généraux, sans liens avec le support ou avec les modalités de transmission.

Si l'écrit peut prendre des formes multiples exprimées sur des supports différents, il doit remplir plusieurs conditions pour être recevable comme preuve. En effet, le nouvel article 1316 du code civil dispose que l'écrit doit :

1. Etre intelligible.
2. Permettre l'identification de son auteur.
3. Garantir l'intégrité du contenu du message.

1.1.1 L'écrit doit être intelligible

Pour devenir une preuve, la suite de caractère, de signes ou de symboles composant un écrit doit être assortie d'une signification intelligible. Toutefois, l'écrit n'a pas à être directement compréhensible. Un écrit codé[9] peut constituer une preuve dès lors qu'il peut être restitué au juge en langage clair.

---

[6] Signature électronique : loi-type de la CNUDCI du 16 décembre 1996 : http://www.uncitral.org/french/texts/electcom/ml-elecsign.pdf
directive du 13 décembre 1999 : http://europa.eu.int/ISPO/ecommerce/legal/documents/signature/diresfr.doc
et enfin loi précitée du 13 mars 2000 : http://www.legifrance.gouv.fr/html/frame_lois_reglt.htm

[7] Ordinateurs biologiques et ordinateurs quantiques.

[8] Cass.com, 2 déc 1997, JCP éd G 1998, II, n° 100097, note Grynbaum, JCP éd E 1998, p.178 note Bonneau, D. 1998, jur, p.192 note Martin.

[9] Le codage peut notamment être réalisé à l'aide de moyens de cryptologie.

L'écrit peut donc sans difficulté se présenter sur un support papier ou sous une forme électronique. Il ne change alors pas de nature mais seulement de forme. C'est pourquoi il est préférable de parler « d'écrit sous forme électronique » que d'« écrit électronique » qui induit un changement de nature de l'écrit.

L'écrit s'entend alors d'un vecteur de communication graphique compréhensible. La définition française est toute entière tournée vers la fonction : Fonction de communication, d'identification et de préservation de l'intégrité du contenu du message[10].

1.1.2 Ecrit et identification

> Un écrit sera recevable en tant que preuve :
>
> *« 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**. »* [11]

L'écrit sous forme électronique doit pouvoir être rattaché à une personne déterminée. Cette condition est liée au fait que les signataires de l'acte ne sont pas présents physiquement et ne se voient pas mutuellement au moment de l'engagement. La difficulté n'est cependant pas insurmontable, des contrats entre absents sur support papier étant conclus chaque jour par des parties en relation d'affaires.

La vraie difficulté réside dans le rattachement d'un écrit à une personne alors que les parties au contrat n'ont pas lié de relations d'affaires préalables. Dès lors, comment s'assurer qu'un individu jouit bien de la qualité à laquelle il prétend et qu'il n'a pas usurpé d'identité ? La réponse est fournie par des procédés techniques tels que la signature électronique, les tiers certificateurs ou encore la cryptologie[12]… Si ces procédés ne sont pas absolument infalsifiables, il est important de noter qu'ils offrent potentiellement un lien de rattachement avec leur auteur, plus sûr que le papier dans bien des hypothèses[13]. La fraude reste marginale.

Le maintien de l'intégrité du contenu du document est une fonction attachée à l'écrit sur support papier qui doit se retrouver comme attribut dans son expression sous forme électronique.

1.1.3 Le maintien de l'intégrité

Le support papier, au regard de l'intégrité du contenu de l'acte, offre un certain nombre d'avantages. D'une part, les fraudes sont difficiles à dissimuler[14] et d'autre part, le papier est un support stable qui se dégrade peu.

En revanche, l'écrit sous forme électronique est immatériel et ne peut donc jouir des fonctionnalités du support physique. Deux paramètres nouveaux sont à prendre en considération. D'une part, la nature ouverte du réseau Internet sur lequel il ne peut exister de sécurité absolue à moyen terme et d'autre part, les moyens techniques par lesquels est réalisée la sécurisation qui s'est déplacée du support lui-même à la signature électronique du contenu du message.

---

[10] Une analyse des fonctionnalités anciennes et nouvelles de la signature sera développée dans la partie consacrée à la signature électronique. Cf : § 2.2 p.14.
[11] Article 1316-1 du code civil.
[12] La description technique de ces procédés sera réalisée dans la partie relative à la signature électronique. Voir § 2.3 p.16.
[13] Les contrats de vente à distance sont très souvent conclus sur simple appel téléphonique et peu de pièces justificatives de l'identité des personnes sont exigées lors de la confirmation écrite.
[14] Les ajouts ou les ratures se distinguent aisément.

L'intégrité du contenu d'un écrit sous forme électronique doit être assurée par des solutions techniques (signature électronique, certification, cryptologie…) dont le fonctionnement sera détaillé dans la partie consacrée à la signature électronique.[15]

L'écrit étant multiforme il importe d'évoquer l'hypothèse d'un conflit de preuve littérale.

1.2 Le conflit de preuve littérale

Ecrit sur support papier et sous forme électronique ont tout deux valeur probante. Dès lors, il peut exister un conflit de preuve. La difficulté peut être résolue de deux manières différentes :

1. Par l'institution d'une hiérarchie entre les différents modes de preuve,
2. En laissant au juge le soin de déterminer au cas par cas quel est le mode probatoire emportant sa conviction.

Si le Québec a opté pour un système de hiérarchisation des modes de preuve[16], la France a choisi l'autre voie. C'est ce qu'exprime l'article 1316-2 du code civil :

> *« Lorsque la loi n'a pas fixé d'autres principes, et à défaut de conventions valables entre les parties,* ***le juge règle les conflits de preuve littérale en déterminant par tout moyen le titre le plus vraisemblable, quel qu'en soit le support****. »*

En cas de conflits de preuve, tout reposera sur le juge qui a déjà à charge de déterminer la recevabilité de la preuve informatique. Ce dernier devra donc mesurer quel est le titre le plus vraisemblable. La mesure est souple mais nous laisse, pour le moment, dans l'incertitude de ce qui sera jugé prépondérant ou non par rapport à un écrit sur support papier[17].

Les entreprises souhaitant avoir une plus grande sécurité juridique quant à la valeur probante de leurs instruments peuvent organiser l'administration des modes preuve par l'intermédiaire des **conventions de preuve** dont la légalité est consacrée par l'article 1316-2 du code civil. Il est regrettable que cet article n'en fixe pas plus précisément les conditions de validité. Il faut donc se référer à la jurisprudence.

Les tribunaux et la cour de cassation ont traditionnellement qualifié l'article 1341 du code civil, qui exige la preuve écrite au-delà d'un certain montant, comme n'étant pas d'ordre public[18]. De la sorte, les parties peuvent aménager consensuellement le règlement des conflits de preuve. Elles sont libres d'imposer certaines exigences formelles ou de les alléger. Ainsi, les parties peuvent définir clairement la force probante des modes de preuve et instaurer une hiérarchie entre ces derniers afin d'accroître les capacités d'anticipation des litiges.

La liberté des parties est encadrée par le droit. En effet :

1. les parties ne peuvent déroger aux règles d'ordre public,
2. elles doivent se conformer aux règles de l'administration judiciaire de la preuve[19],

---

[15] Voir § 2 p.11.
[16] Pour plus de détails sur la « hiérarchisation des modes de preuve » voir : Catala P. Ecriture électronique et actes juridiques » in Mélanges Cabrillac, Dalloz et Litec, 2000, p. 91, spéc. N°10.
[17] Pour plus de détails sur les fondements du choix français voir : Leclerc P. « Le nouveau droit civil et commercial de la preuve et le rôle du juge » in Communication commerce électronique 2000, n° 5 p.11 actualités n°9.
[18] A cet égard voir : Cass com 8 novembre 1989 in rapport de la cour de cassation pour 1989, éd la documentation française, 1990, p.332.
[19] Par exemple : Action ad exibendum pour la communication forcée des preuves.

3. et garantir systématiquement la possibilité d'apporter la preuve contraire,
4. ainsi que respecter l'équilibre des intérêts des parties à la convention.

En outre, les parties devront être particulièrement vigilantes lors de la rédaction de la convention de preuve. Dans l'hypothèse d'un contrat conclu avec un consommateur, la convention pourrait être considérée comme une clause abusive. Au sens du droit de la consommation **sont abusives :**

> **« *les clauses*** *qui ont pour objet ou pour effet de créer, au détriment du consommateur ou du non professionnel un* ***déséquilibre significatif entre les droits et obligations des parties*** *au contrat.»*
> Ou encore
> Celles qui ont pour objet ou pour effet « *d'entraver l'exercice d'actions en justice ou des voies de recours par le consommateur, notamment (…)* ***en limitant indûment les moyens de preuve ou en imposant à celui-ci une charge de la preuve*** *qui, en vertu du droit applicable, devraient revenir normalement à une autre partie au contrat. »*

Ce large pouvoir d'appréciation donné au juge ainsi que la grande liberté laissée aux parties ne doivent pas nous faire oublier notre tradition juridique qui nous invite à distinguer l'écrit exigé à titre de preuve (ou **ad probationem**) de l'écrit exiger comme condition de l'existence du droit, c'est à dire **ad validitatem**.

1.3 L'écrit exigé ad validitatem et la notion de preuve

La loi du 13 mars 2000 a été introduite au chapitre VI du titre III du livre III du code civil qui a trait à la preuve des obligations. Ainsi, nombre d'auteurs se sont interrogés sur la signification de cet emplacement au regard de l'exigence de l'écrit ad validitatem. En effet, il semblait permis de déduire que les dispositions de la nouvelle loi ne concernaient que les règles de preuve et non celles relatives à la validité de l'acte. Il faut cependant considérer l'emplacement des dispositions nouvelles comme une maladresse du législateur. En effet, plusieurs arguments militent en faveur d'une application de la définition large de l'écrit à condition d'existence de l'acte :

1. Il est logique que l'écrit reçoive une définition unitaire au sein du code civil.
2. Une analyse téléologique de la loi permet d'affirmer que la définition de l'écrit s'applique même dans l'hypothèse d'un écrit exigé ad validitatem.
3. A défaut, la loi du 13 mars 2000 mettrait le droit français en contradiction avec le droit communautaire et notamment avec la directive du 13 décembre 1999[20]. Ainsi qu'avec la loi type de la CNUDCI[21].
4. A l'article 1326 du code civil, les mots « de sa main » ont été remplacés par « par lui même ».
5. Enfin, la loi permettant la réalisation d'actes authentiques électroniques, c'est à dire indépendamment de tout support physique, il est difficile d'imaginer que le législateur ait entendu mettre une restriction implicite de la définition de l'écrit quand celui-ci est exigé ad validitatem.

La Cour de cassation a également rendu des décisions portant à croire qu'un écrit sous forme électronique serait suffisant pour s'acquitter d'une exigence ad validitatem. Tel fut l'objet d'un

[20] Voir article 9 § 1 et le considérant n° 34 de la position commune (CE) n° 2/2000 arrêtée par le Conseil le 28 février 2000.
[21] Voir les articles 5, 5bis et 12 de la loi type.

arrêt rendu par la chambre commerciale rendu à propos de l'acceptation d'un bordereau Dailly par télécopie pour lequel l'écrit est exigé ad validitatem[22].

Ainsi, il est regrettable que la loi soit un facteur de trouble et non d'éclaircissement. Pourtant, le droit français ne pourra retenir une autre interprétation, celle-ci doit donc être tenue pour acquise. D'autant que le **projet de loi sur la société de l'information** propose de clarifier la situation en assurant que l'écrit électronique sera recevable même quand l'écrit est exigé ad validitatem. Au terme du projet de loi :

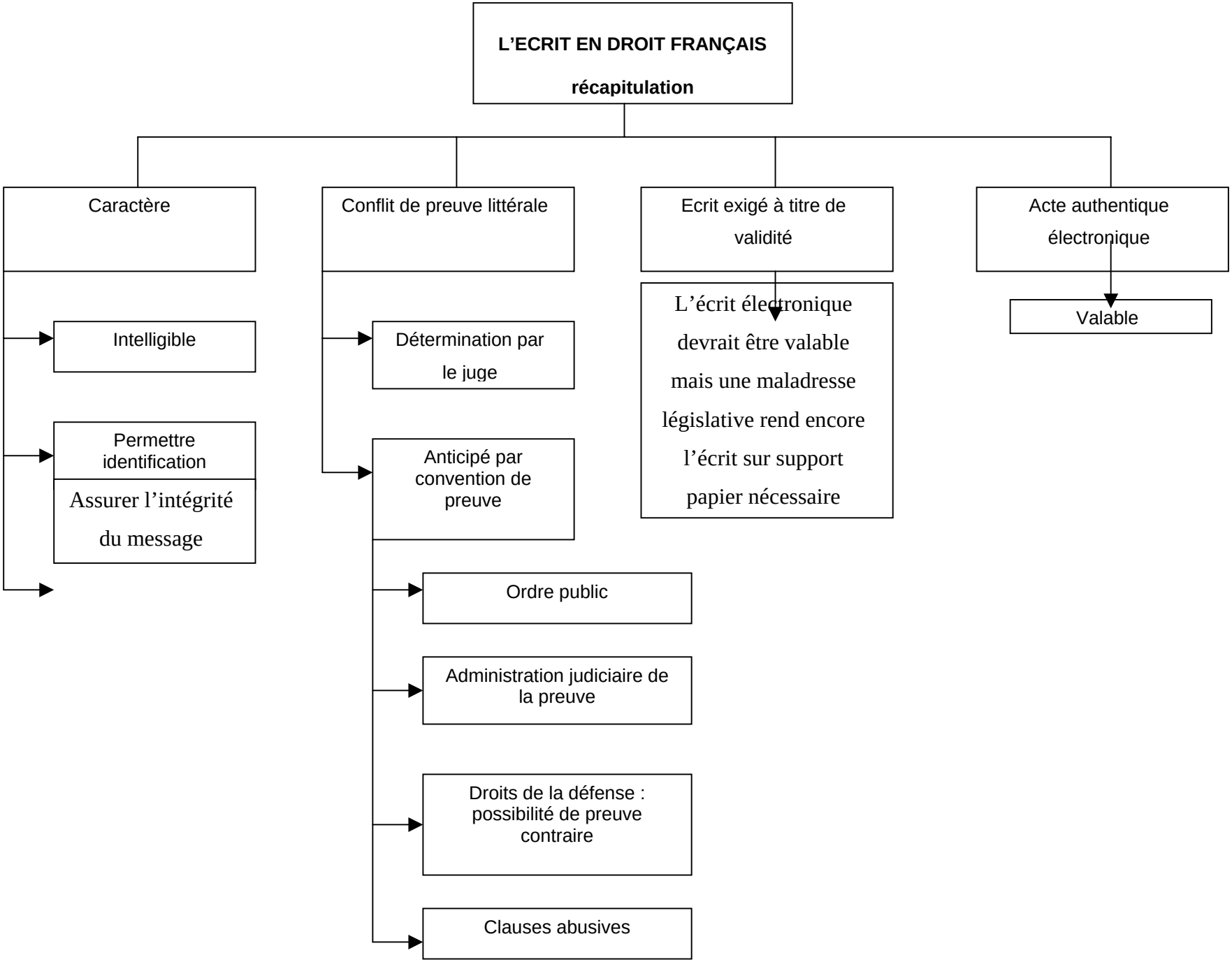
> *« Lorsqu'un écrit est exigé pour la validité d'un acte juridique, celui-ci peut être établi et conservé sous forme électronique dans les conditions prévues aux articles 1316-1 et 1316-4 et, lorsqu'un acte authentique est requis, au second alinéa de l'article 1317. »*

Cependant, pour quelques catégories de contrat l'écrit sous forme électronique reste prohibé, il s'agit :

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

Néanmoins, dans l'attente de l'adoption puis de la publication de la loi nouvelle, les actes pour lesquels l'écrit est requis à titre de validité devront, par prudence, être passés sur support papier.[23]

[22] Cass com. 2 décembre 1997, D 98, p. 192 note : D.Martin ; RTDcom. 1998 p.187, obs : M.Cabrillac ; JCP E, 1998, p. 178, Note : T.Bonneau.
[23] Par exemple : acte de caution.


L’ECRIT EN DROIT FRANÇAIS
récapitulation
Caractère
Conflit de preuve littérale
Ecrit exigé à titre de validité
Acte authentique électronique
Intelligible
Permettre identification
Assurer l’intégrité du message
Détermination par le juge
Anticipé par convention de preuve
Ordre public
Administration judiciaire de la preuve
Droits de la défense : possibilité de preuve contraire
Clauses abusives
L’écrit électronique devrait être valable mais une maladresse législative rend encore l’écrit sur support papier nécessaire
Valable

1.4 Acte authentique et écrit sous forme électronique

Bien que les actes authentiques[24] soient **expressément exclus de la directive** relative à la signature électronique, **l'article 2 de la loi française** ajoute un second alinéa à l'article 1317 du code civil :

> *« Il peut être dressé [acte authentique] sur support électronique s'il est établi et conservé dans les conditions fixées par décret en Conseil d'Etat[25]. »*

Néanmoins, le législateur a été prudent. Dans un premier temps seuls les actes notariés pourront être réalisés sous forme électronique, à la condition qu'un notaire soit présent aux cotés de chaque partie, ce qui permet la vérification de l'ensemble des signatures électroniques figurant à l'acte et le respect des autres solennités requises. Il est important de noter qu'un notaire n'est pas un tiers certificateur au sens de la loi de mars 2000 ni même au sens du projet de loi sur la société de l'information.

L'intégrité de l'écrit devra être maintenue tant au regard du support que du contenu ce qui constitue une nouveauté pour les notaires. En effet, d'après l'article 1er de l'ordonnance du 2 novembre 1945 le notaire reçoit les actes pour les « conserver en dépôt » cent ans après leur date d'établissement, puis « les minutes et répertoires doivent être déposés aux archives départementales ou aux archives nationales pour le notaire parisien. »[26] L'ensemble de la profession s'est donc mis en branle pour assurer le mieux possible la continuité de leur mission en dépit des évolutions technologiques, notamment grâce au réseau REAL[27].

Naturellement, toutes les modalités d'une conservation aussi longue ne sont pas encore déterminées et sont soumises à l'état de la technique. Il ne serait pas étonnant, dans un premier temps, de signer à nouveau l'acte à intervalles réguliers de façon à assurer de manière certaine sa pérennité.

2. La signature électronique

La définition législative de l'écrit englobe l'écrit électronique. Toutefois, cette définition étant fonctionnelle, il importe que l'écrit sous forme électronique puisse remplir convenablement les fonctions jusqu'alors assurées par l'écrit sur support papier. Pour remplir cette exigence, le recours à la signature électronique est essentiel. Ainsi, nous devons dresser une typologie des différentes formes de signatures électroniques avant de confronter leur fonctionnalité à la signature manuscrite.

Une fois ces précisions apportées nous pourrons envisager les modalités pratiques et juridiques de la mise en œuvre d'une signature électronique.

2.1 Typologie des différentes formes de signature électronique

Différents procédés techniques se voient affublés du qualificatif de signature électronique. Une clarification s'impose.

---

[24] L'acte authentique est un document rédigé par un officié public (officié d'état civil, notaire, greffier...) qui doit être compétent matériellement et territorialement.
[25] Non encore adopté.
[26] Citation de E .Caprioli in JCP cahier de l'entreprise n° 2 année 2000p.5.
[27] Droit & patrimoine, n° 73, juillet-août 1999 p.20.

2.1.1 La signature numérisée

Nombre d'auteurs considèrent que la reproduction par numérisation de la signature manuscrite constitue une signature électronique[28]. Une conception aussi large ne peut pourtant pas être retenue à la lumière de la loi du 13 mars 2000. En effet, ce procédé est loin de pouvoir assurer la fonction de rattachement de l'écrit à son auteur tant sa falsification est simple.

2.1.2 L'utilisation combinée d'une carte et d'un code secret

Toujours dans l'esprit d'une approche fonctionnelle de la signature, l'utilisation d'une carte à puce couplée à un code secret permet non seulement d'identifier l'individu qui est seul détenteur du code secret mais aussi de rattacher directement cette identification à un acte déterminé. Cette adéquation fonctionnelle suffit-elle à en faire une signature électronique ? Plusieurs arguments militent contre une telle acception.

« Ces éléments associés constituent bien plus une d'autorisation d'accès à un système informatique propriétaire, qu'un mécanisme de signature susceptible de permettre non seulement la réalisation des mêmes fonctions que la signature manuscrite, mais également de réaliser ces fonctions dans la quasi-totalité des situations où se manifeste la signature classique, et ce, tant dans le cadre des réseaux ouverts que fermés[29].»

La combinaison d'une carte à puce et d'un code secret ne doit donc pas être assimilée à une signature électronique :

1. D'une part, ni le code ni la carte ne sont vraiment liés à la personne.
2. D'autre part, la fonction d'adhésion au contenu de l'acte est assurée seulement si l'approbation est donnée au terme de l'opération, ce qui n'est pas toujours le cas.
3. Enfin, l'intérêt de la notion de signature électronique est de pouvoir considérer un acte sous seing privé comme ayant une valeur probante.

2.1.3 Les signatures biométriques

La science, rattrapant la fiction, s'intéresse aux caractéristiques uniques des individus pour les identifier et leur permettre de rattacher cette identification à un acte. Ces procédés techniques sont nombreux, il peut s'agir de la dactyloscopie[30], de la rétinoscopie[31] ou encore de la reconnaissance vocale ou dynamique de la signature[32].

Pourtant, force est de constater que ces procédés ne sont pas encore très développés en pratique. Cette situation s'explique par des techniques qui en sont encore à leurs balbutiements ainsi que le coût et la lourdeur de leur implémentation. En outre, il est encore permis de s'interroger sur la qualité de l'expression de l'animus signandi, les techniques actuelles devant être affinées.

Ainsi, en l'état actuel de la technique, le seul procédé de signature électronique devant retenir l'attention est celui de la signature numérique, encore appelée, signature digitale.

---

[28] Concrètement il s'agit de scanner une signature manuscrite.
[29] D.Gobert et E.Montero, DA/OR, avril 2000, n°53, p.17 à 39. Voir aussi : S. Parisien et P.Trudel, L'identification et la certification dans le commerce électronique, Ed. Yvon Blais inc., 1996, p.99.
[30] Identification par les empreintes digitales.
[31] Analyse de la rétine.
[32] Se distingue de la graphologie au profit d'une analyse de la vitesse, du mouvement… pour plus d'information à ce sujet voir : M.Fontaine, la preuve des actes juridiques et les techniques nouvelles in La preuve, colloque UCL ., 1987 et D.Syx, vers de nouvelles formes de signature ?, Dr ; INFORM 1986/3 P ;133-147 ;

2.1.4 La signature numérique (ou digitale)

Les procédés de signature numérique s'organisent autour d'algorithme de cryptage[33]. Deux procédés sont à distinguer : les procédés à clé unique et les procédés asymétriques.

2.1.4.1 les procédés à clé unique

Dans ce système, la même clé sert à la fois à coder et à décoder. Le destinataire doit recevoir la clé pour pouvoir décoder le message. D'une part, une fois en possession de la clé il pourra coder à son tour des documents et d'autre part, il faut bénéficier de transmission particulièrement sûre pour envoyer la clé au destinataire.

Le système n'offre pas les garanties exigées tant par la loi française que par la directive de 1999 et ne doit donc pas être considéré comme pouvant intervenir dans le cadre de la signature électronique.

2.1.4.2 Signature et clés asymétriques

Le système des clés asymétrique offre les garanties nécessaires à la signature d'un document électronique. Il repose sur l'utilisation d'une paire de clés, l'une secrète et l'autre publique, unies entre elles par une formule mathématique[34].

Le message est signé par son auteur à l'aide de sa clé privée, puis il est expédié au destinataire, qui pourra le déchiffrer uniquement au moyen de la clé publique complémentaire de la clé privée de l'émetteur. Ainsi, le destinataire est certain que le message émane bien de son auteur dûment identifié dans la mesure où un certificat confirme que la clé publique appartient bien à son auteur.

Pour assurer la confidentialité d'un échange de données la procédure est quelque peu différente puisque cette fois-ci, le message sera chiffré avec la clé publique du destinataire, dès lors seule la clé privée lui correspondant pourra permettre la restitution du message sous une forme intelligible. Il est donc intéressant de combiner les deux fonctions.

Reste cependant, pour assurer le bon fonctionnement pratique du système, à organiser la publicité des clés publiques et développer l'activité de prestataire de service de certification.

2.2 Les fonctions de la signature, du papier au numérique

Il convient de déterminer quelles sont les fonctions assurées par la signature manuscrite et de les confronter à la signature numérique.

1. Fonction d'identification.
2. Fonction adhésion au contenu
3. Fonction de garantie de l'intégrité.
4. Fonction de constitution d'un original
5. Fonction psychologique.

[33] Ces algorithmes servent également à garantir la confidentialité des échanges et n'ont pas pour seule fonction la mise en œuvre de la signature numérique.
[34] L'application la plus répandue est Pretty Good privacy téléchargeable sur le site : http://www.pgp.com/international/france/
et l'algorithme de référence est RSA : http://www.rsa.com/.

2.2.1 L'identification

L'identification de manière certaine de la personne est rendue possible par les signatures numériques reposant sur un système de clés asymétrique. Pourtant, il faut prendre conscience du bouleversement de la relation contractuelle. En effet, lors de la signature manuscrite d'un contrat, son rôle d'identifiant est résiduel alors que la signature électronique à en quelque sorte une finalité nouvelle : Régir des relations sur des réseaux ouverts par l'intermédiaire desquels des parties nouent à distance des relations contractuelles.

2.2.2 L'adhésion au contenu de l'acte

La signature manuscrite exprime le consentement du signataire au contenu d'un acte. Or la signature électronique, par le biais de l'application libre et volontaire de la clé privée, permet de considérer que le signataire a exprimé son consentement ou son adhésion à l'acte signé. Encore faut-il que le document et la signature soient liés logiquement l'un à l'autre, à défaut le consentement ne sera pas exprimé de manière certaine.

2.2.3 Le maintien de l'intégrité

Le maintien de l'intégrité d'un document signé de manière manuscrite est assuré par l'absence de rature ou de correction sur le document signé. En outre, sur le plan de la conservation, le papier est un support qui se dégrade peu. Dans le cadre de la signature numérique, le maintien de l'intégrité est assuré par la fonction dite de « hachage irréversible ». Cette fonction va appliquer au document une opération mathématique de manière à produire un condensé numérique du message[35]. Ce résumé est codé à l'aide de la clé privé : le résultat est alors une signature numérique. Cette signature est envoyée en accompagnement du fichier principal au destinataire. A la réception, la signature sera lue à l'aide de la clé publique qui lui correspond. En appliquant l'opération mathématique inverse, la fonction de hachage reconstitue le fichier condensé, qui pourra alors être comparé au fichier principal. Dès lors toutes atteintes à son intégrité seront décelables.

La signature numérique apporte donc des solutions plus fiables que le support papier qui est plus aisément falsifiable.

2.2.4 Signature électronique et original

La signature permet de conférer à un document le statut d'original qui est nécessaire à tout acte sous seing privé. Avec l'avènement de l'ère numérique, le statut du document est un peu bousculé même si l'écrit papier connaît l'hypothèse des originaux multiples[36]. Dès lors, la pluralité d'écrit sous forme électronique ne doit pas s'analyser forcément en terme de copie. Si le document est signé électroniquement, il constitue un original au même titre que les deux exemplaires d'un même acte signé réciproquement par les parties.

Cependant, le document signé numériquement se dégrade en copie si le certificat relatif à la clé publique se trouve révoqué ou frappé de caducité puisque alors la signature ne pourra être vérifiée.

2.2.5 La dimension psychologique de la signature

[35] L'intérêt de ne produire qu'un résumé du document est de gagner du temps lors du codage et du décodage.
[36] Formalité imposée par l'article 1325.

La dimension psychologique de la signature est considérable et ne figure que peu dans les textes. L'une de ses principales manifestations est l'exigence de l'écrit signé à titre de validité. En effet, nous sortons alors du cadre strict de la preuve pour entrer dans le domaine de la protection des personnes. L'attention des individus est alors appelée sur la gravité de l'acte par la signature manuscrite de leur engagement.

La signature numérique est encore loin de s'effectuer d'un simple « clic » et constitue une action positive qui n'est pas de nature à altérer la dimension psychologique inhérente au contreseing.

2.3 Signature électronique et présomption de fiabilité

La loi du 13 mars 2000 a consacré la validité de l'écrit sous forme électronique. Cependant le texte est large et comporte des zones d'ombre, notamment, au regard de la définition d'une signature électronique ***fiable***. Si le décret du 30 mars 2001 est venu apporter un peu de lumière, force est de constater que la législation française n'atteint pas encore un degré de clarté satisfaisant.

2.3.1 Conditions de fiabilité

Un écrit électronique ne sera recevable à titre de preuve uniquement dans la mesure où il a été crée par un procédé technique fiable. Les conditions relatives à la fiabilité d'une signature électronique sont fixées par le **second article** du décret qui dispose :

> *« La fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve contraire, lorsque ce procédé met en œuvre* ***une signature électronique sécurisée*** *établie grâce à un* ***dispositif sécurisé de création de signature*** *électronique et que la vérification de cette signature repose sur l'utilisation d'un* ***certificat électronique*** *qualifié.»*

ainsi que par l'article 1er qui établit qu'une signature électronique doit :

1. être propre au signataire ;
2. être créée par des moyens que le signataire puisse maintenir sous son contrôle exclusif ;
3. et garantir l'intégrité de l'acte sur lequel elle est appliquée.

Le système de signature électronique est associé à un processus de certification. C'est-à-dire que la personne désireuse d'avoir une signature électronique fiable va demander à un tiers certificateur de vérifier les informations relatives à son identité ainsi qu'aux modalités de création de la signature. Le certificat, qui se présente lui aussi sous la forme d'un document signé électroniquement, atteste que l'organisme de contrôle a pu s'assurer de l'exactitude d'un certain nombre d'informations relatives à la signature et au signataire. Dès lors, la valeur persuasive qui lui est attachée, est fonction du degré de confiance que peut avoir le destinataire dans l'établissement qui a établi le certificat.

2.3.1.1 La création de la signature

Le droit français reste très proche des dispositions de la directive, puisqu'il distingue signature simple et signature sécurisée. Même si le droit communautaire évoque la signature renforcée les deux ordres juridiques décrivent une même réalité.

Ainsi, un dispositif sécurisé de signature doit :

1. Garantir par des moyens techniques et des procédures appropriées que les données de création de signature ne peuvent être établies plus d'une fois, que leur confidentialité est assurée, qu'elles ne peuvent être trouvées par déduction, que la signature électronique est protégée contre toute falsification et qu'elles peuvent être protégées de manière suffisante par le signataire contre toute utilisation par des tiers.

2. N'entraîner aucune altération du contenu de l'acte signé,

3. Ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

Ces conditions réunies, le dispositif sécurisé de création de la signature devra être certifiée comme conforme aux exigences légales et réglementaires. La certification se fait alors soit :

1. Auprès des services du Premier ministre,
2. Par un organisme désigné à cet effet par un Etat membre de l'Union européenne.

Le contrôle de la mise en oeuvre de la procédure de certification incombe à un comité directeur de la certification.

2.3.1.2 La vérification de la signature électronique

La certification de la signature est, elle aussi, soumise à conditions qui ont pour objet de garantir l'identité du signataire ainsi que d'exprimer son consentement au contenu de l'acte. La fonction de la certification est de :

1. Garantir l'exactitude de la signature et transmettre au vérificateur le résultat de la vérification sans aucune altération.
2. Garantir au vérificateur le contenu de l'acte.
3. Assurer la vérification des conditions et la durée de validité du certificat électronique utilisé.
4. Garantir que le résultat de la vérification sera porté à la connaissance du vérificateur sans altération.
5. Donner sans altération au vérificateur l'identité du signataire et l'informer de l'utilisation éventuelle d'un pseudonyme.
6. Garantir la détection de toute modification ayant une incidence sur les conditions de vérification.

2.3.1.3 Certificats et prestataire de service de certification

2.3.1.3.1 Les certificats

Le certificat doit comporter certaines informations :

1. Informations relatives à l'identification du signataire : nom, pseudonyme, qualité éventuelle, origine de la signature…
2. Informations relatives au prestataire de service de certification (P.S.C) : identité, Etat d'origine, sa propre signature électronique sécurisée.
3. Informations relatives au certificat lui-même : titre du certificat, durée de validité, code d'identité du certificat, les conditions éventuelles d'utilisation du certificat.

L'objet des certificats est d'attester du lien entre les informations vérifiées et le signataire.

2.3.1.3.2 Les prestataires de service de certification(P.S.C)

Les prestataires de services de certification sont les seuls habilités à délivrer les certificats afférents aux signatures numériques. Leur rôle est essentiellement de vérifier que les informations qui leurs sont transmises correspondent à la réalité, ils contrôlent donc l'identité de la personne à laquelle le certificat est délivré, la fiabilité du procédé utilisé et le degré de confidentialité assuré. Ils assurent également la publicité des certificats par la mise en place d'un annuaire.

De surcroît, une mission d'archivage leur incombe afin de pouvoir produire des preuves écrites au cours d'une instance judiciaire. Ils doivent procéder à l'horodatage de la délivrance et de la révocation du certificat. Une mission de prévention contre la falsification leur échoit également.

Les P.S.C peuvent, sur le fondement du décret[37] demander une accréditation valant présomption de conformité aux exigences posées par les textes. Une telle procédure dérogatoire sera possible après évaluation par un organisme, sur le fondement d'un arrêté du Premier ministre qui n'a toujours pas été adopté.

Dans l'hypothèse où le certificat aurait été rendu par un P.S.C établit dans un pays non-membre de l'Union européenne, le droit français se contente de reprendre l'article 7.1 de la directive de 1999. En revanche, le P.S.C pourra bénéficier d'une égalité de traitement dans l'ensemble des pays membres.

Article 7-1 :

> *« Les Etats membres veillent à ce que les certificats délivrés à titre de certificats qualifiés à l'intention du public par un prestataire de service de certification établi dans un pays tiers soient reconnus équivalents, sur le plan juridique, aux certificats délivrés par un prestataire de service de certification établi dans la Communauté*
>
> *a) si le prestataire de service de certification remplit les conditions visées dans la présente directive et a été accrédité dans le cadre d'un régime volontaire d'accréditation établi dans un Etat membre ; ou*
>
> *b) si un prestataire de service de certification établi dans la Communauté, qui satisfait aux exigences visées dans la présente directive, garantit le certificat ; ou*
>
> *c) si le certificat ou le prestataire de service de certification est reconnu en application d'un accord bilatéral ou multilatéral entre la Communauté et des pays tiers ou des organisations internationales.»*

En conclusion, si le cadre législatif français commence à s'adapter aux nouvelles formes que peut recouvrir l'écrit, le droit positif n'est pas encore très clair. L'insécurité juridique règne encore sur la recevabilité d'un document électronique lorsque l'écrit est exigé à titre de validité. La prudence impose donc de passer ce type d'acte sur support papier. Un tel état du droit est de nature à mettre le système juridique français en contradiction avec l'ordre juridique communautaire.

Il est également regrettable que tous les actes réglementaires relatifs à la certification ainsi qu'aux prestataires de service de certification n'aient pas encore été adoptés. Il existe cependant déjà des prestataires qui proposent des offres de service de certification[38].

[37] Décret 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique. J.O.R.F 31 mars 2001. http://www.legifrance.gouv.fr/html/frame_lois_reglt.htm

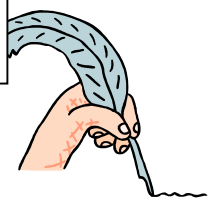
[38] Voir liste

LA SIGNATURE ELECTRONIQUE D'UN MESSAGE EN 5 ETAPES

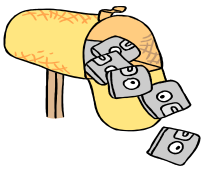
1.
Création de la signature

2.
certification de la signature

3.
Signature de l'écrit électronique avec la clé privée de l'expéditeur, garanti l'identification du signataire



4.
Cryptage du message avec la clé publique du destinataire.
Garanti la confidentialité et l'intégrité du contenu du message



5.
Réception du message

Vérification de la signature avec la clé publique de l'expéditeur et le certificat

Décrypte le message à l'aide de la clé privée du destinataire

Les principaux prestataires de service de certification français :

nom	en service	prix	pieces demandées	delivrance	clef privée	certificats distribués
altern http://ca.altern.org/	oui	gratuit	email	par le web	non stockée	21
Certinomis : http://www.certinomis.com/sas/sas.htm	oui	150ff par an	carte d'identité	courrier postal	non stockée	?
tribunal de commerce paris : http://www.greffe-tc-paris.fr/greffe71.htm	oui	gratuit	carte d'identité	sur place	non stockée	?

La signature électronique

Typologie

- Signature numérisée
- Carte & code secret
- Signature biométrique
- Signature numérique ou digitale

Fonction

- Identification
- Adhésion au contenu
- Maintien de l'intégrité
- Statut d'original
- Dimension psychologique

Créatio signa

Signature et certification

Signature simple

- Doit être propre au signataire
- Moyen de création propre au signataire
- Garantir l'intégrité

Signature sécurisée

Création

- Unicité
- Confidentialité
- Intégrité
- Pas d'obstacles à une connaissance exacte par le signataire

Certification

- Exactitude
- Garantie du contenu
- Identité du signataire
- Garantie du résultat