

LA SIGNATURE ELECTRONIQUE EN DROIT DE LA PREUVE

Exposé de Droit

INTRODUCTION

Le développement d'Internet et des communications numériques a suscité de nombreuses questions d'ordre juridique.

En effet, ce réseau ouvert à tous a besoin de toujours plus de sécurité. De plus les messages électroniques se substituent de plus en plus aux documents sur support papier.

Or la loi exige souvent des écrits en guise de preuve. Ces écrits électroniques ont-ils alors une valeur probante ? Comment leur donner une valeur juridique ? C'est ainsi que la signature électronique est devenue indispensable dans la constitution de ce cadre juridique. Toutefois, elle doit, elle aussi, être sécurisée pour garantir les impératifs d'intégrité et de fiabilité. Néanmoins, jusqu'à quel point peut-elle être fiable ?

PLAN

1. Droit de la preuve et NTIC

1.1. La signature électronique dans le droit de la preuve

1.2. Nouvelle définition de l'écrit et de la signature électronique

1.3. Définitions textuelles

2. Aspects techniques de la signature électronique

2.1. Le chiffrement asymétrique

2.2. La fonction de hachage

2.3. Application

3. Force probatoire et limites de la signature électronique

3.1. La force probatoire: définition

3.2. La signature électronique notariale certifiée

3.3. Limites de l'admissibilité et la force probatoire de l'écrit électronique

1. Droit de la preuve et NTIC:

1.1. La signature électronique dans le droit de la preuve:

La preuve est la manifestation de la vérité. Cependant, le législateur a réglementé les procédés de preuve autorisés pour préserver la **justice** et la **sécurité** des relations humaines et sociales.

L'admissibilité de la preuve est commandée par l'article 1341 du Code Civil. Ainsi, la preuve des actes juridiques doit être faite par écrit dès qu'ils excèdent une valeur fixée par décret qui est actuellement de 800 €. Il est alors demandé aux parties de préconstituer une preuve écrite.

Cependant, cet article présente des exceptions :

- Le principe ne s'applique pas aux faits juridiques.
- A l'égard des commerçants, les actes de commerce peuvent se prouver par tous les moyens, sauf exceptions. Cela est due aux nécessités de la vie commerciale (rapidité, relations de confiance).
- La preuve peut également être faite par tous moyens lorsqu'il existe un commencement de preuve par écrit. (article 1347 du Code Civil).
- La preuve peut aussi être faite par tous moyens en cas d'impossibilité de prouver par écrit (ex: impossibilité matérielle telle un incendie ou une inondation, ou morale comme dans la relation parents-enfants).(article 1348 du Code Civil).

Les moyens pour prouver un fait sont très nombreux mais ne sont pas tous admis par le droit français. Le Code Civil en mentionne cinq:

- Preuve littérale ou l'écrit.
- Preuve testimoniale.
- L'aveu.
- Le serment.
- Les présomptions.

Nous nous intéressons ici à la preuve littérale puisque c'est dans ce cadre que va émerger la signature électronique. En effet, la preuve littérale est celle qui résulte d'écrits émanant des parties, ces derniers étant destinés à servir de preuve.

Les écrits peuvent être classés sous cette forme:

- Actes authentiques (rédigé par un officier public et soumis à plusieurs formalités)
- Actes sous seing privé (écrits rédigés par des particuliers dont la seule exigence de forme est la signature, si aucune autorité extérieure ne prend part à l'acte).
- Autres écrits (signés ou non).

Comme le texte écrit, la signature a longtemps été assimilée à sa forme manuscrite. Ainsi aucun texte ne la définissait ou ne la réglementait, même si elle était exigée pour les actes sous seing privé (art. 1325, CV), pour les contrats synallagmatiques (art. 1325, CV), et pour la reconnaissance de la dette (art. 1326, CV). Lorsqu'elle se limitait à la forme manuscrite, sa notion semblait évidente.

Cependant, elle doit assumer deux fonctions:

- Identifier le signataire.
- Manifester sa volonté d'approuver le contenu d'un document.

➔ La signature apparaît comme un élément important en matière de preuve.

1.2. Nouvelle définition de l'écrit et de la signature électronique:

Toutefois, aujourd'hui, sous l'impulsion de nouvelles technologies telles que le multimédia et le réseau internet, on assiste à une véritable mutation du secteur de la distribution, à une modification des modes de commercialisation et à une évolution des rapports entre l'Etat et les citoyens et entreprises. Les échanges électroniques impliquent une dématérialisation totale des relations entre les différents acteurs économiques (banques, commerçants, sociétés, prestataires de services, Etats et citoyens). De plus, les messages électroniques se substituent désormais fréquemment aux documents sur support papier.

Cette évolution suscite de nombreuses questions juridiques:

- Les messages électroniques ont-ils une valeur probante?
- Toutes signatures électroniques peuvent-elles conférer à un écrit électronique une valeur juridique?

• C'est sous l'impulsion de la directive européenne 1999/93/CE du 13 décembre 1999, que le droit français va évoluer dans ses données fondamentales du droit de la preuve. En effet, la commission estimait que les réseaux ouverts comme internet n'étaient pas suffisamment sécurisés pour les affaires et voulait instaurer un environnement sûr en ce qui concerne l'authentification électronique.

Finalement, le but de la directive est d'aboutir à ce qu'en droit interne les Etats membres reconnaissent à la signature électronique :

- "la valeur juridique d'une signature manuscrite".
- le fait qu'elles soient "admissibles comme preuves en justice de la même façon que les signatures manuscrites".

La directive européenne définit donc la signature électronique comme "**une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification**".(Art.2-1 de la Directive).

De plus, en tant que signature électronique avancée, elle doit **“être liée uniquement au signataire; permettre d’identifier le signataire; être créée par 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 des données soit détectable.”**

➔ Finalement, c’est plutôt à cette définition que l’on rapporte lorsque l’on parle de signature électronique.

- Ainsi la loi du 13 mars 2000 est venue modifier le droit français relatif à la preuve, en reconnaissant l’équivalence du support papier et du support numérique dès lors qu’un certain nombre de conditions sont respectées.

- Redéfinitions et définitions légales de la preuve :

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, quelque soient leur support et leurs modalités de transmission”.**

Article 1316-1 : **“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.”**

Article 1316-4 **“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”.**

➔ La signature électronique se présentera alors sous la forme d’un code informatique infalsifiable. Inséré dans un document, il permettra à son destinataire de reconnaître l’identité de son auteur, l’authenticité et l’intégrité du document.

Remarque : Les outils nécessaires pour gérer les procédures liées à cette signature électronique seront fournis par des sociétés appelées prestataire de certification

1.3. Définitions textuelles:

La loi du 13 mars 2000 a eu besoin de décrets d'applications pour conférer un réel cadre juridique à la signature électronique.

- *Décret du 30 mars 2001 pris en conseil d'Etat:*

La fiabilité d'un procédé de signature électronique sera présumée, jusqu'à preuve du contraire sous les conditions données dans l'article 2 du décret du 30 mars 2001. C'est là qu'intervient la mise en oeuvre de la signature sécurisée.

→ Elle doit être établie grâce à un dispositif sécurisé de création de signature électronique.

→ La vérification de cette signature doit reposer sur l'utilisation d'un certificat électronique qualifié.

- *Décret du 18 avril 2002 pris en Conseil des Ministres*

Ce décret est relatif à l'évaluation et à la certification de la sécurité des produits et les systèmes des technologies de l'information. Il a pour finalité de créer une superstructure administrative qui encadre les technologies de l'information : La Direction Centrale de Sécurité des Systèmes d'Information (DCSSI).

Le Code Civil énonce désormais (Art. 1316-4):

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

➡ Cette loi innovante réfute désormais toute hiérarchie entre les supports, considérant que l'écrit sous forme électronique doit avoir la même force probante que l'écrit sur support papier. Il y a quatre conditions pour cette équivalence:

- Pouvoir identifier la personne dont émane l'écrit électronique au moyen d'un procédé fiable.
- L'écrit électronique a été créé dans des conditions de nature à en garantir l'intégrité.
- L'écrit électronique est conservé dans des conditions de nature à en garantir l'intégrité.
- Utiliser un procédé fiable garantissant le lien de la signature électronique avec l'acte auquel elle s'attache.

2. Aspects techniques de la signature électronique:

Ces problèmes d'identification, de fiabilité, et d'intégrité sont résolus grâce à un chiffrement asymétrique et à des fonctions de hachage.

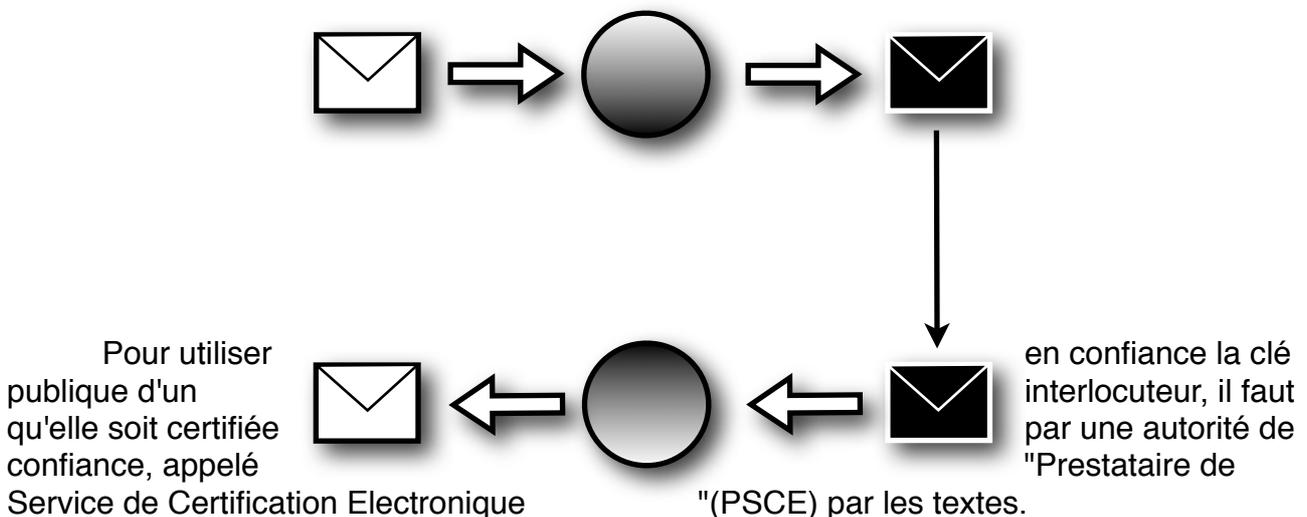
2.1. Le chiffrement asymétrique:

Le chiffrement asymétrique, ou cryptographie à clé publique est un processus de chiffrement qui applique un algorithme à un message afin d'en coder la signification.

Il utilise une fonction dite à sens unique et à brèche secrète, qui est difficile à inverser, à moins de posséder une information particulière, tenue secrète, nommée clé privée.

Le chiffrement asymétrique utilise deux clés complémentaires, la clé privée (uniquement connue de son propriétaire) et la clé publique (ouvertement diffusée).

Le fait que la clé privée soit uniquement connue de son propriétaire permet d'assurer qu'un document auquel on applique la clé publique ne pourra être ouvert que par le propriétaire de la clé privée (confidentialité) et que tout document généré depuis cette clé a nécessairement été généré par le propriétaire de la clé (identification).



Le certificat numérique est un document numérique qui identifie une personne (physique ou juridique) grâce à deux clés. Il contient l'information suivante :

- Identification du titulaire du certificat (nom du titulaire, numéro d'identification fiscale NIF, adresse e-mail...)
- Attributs du certificat : numéro de série, entité émettrice, date d'émission, période de validité du certificat, etc.
- Deux clés : une clé publique et une clé privée.
- La signature électronique du certificat avec la clé de l'autorité de certification émettrice.

2.2. La fonction de hachage:

L'empreinte d'un texte ou condensé ("hash" en anglais), est la forme abrégée de ce texte obtenue à l'aide d'une fonction de hachage.

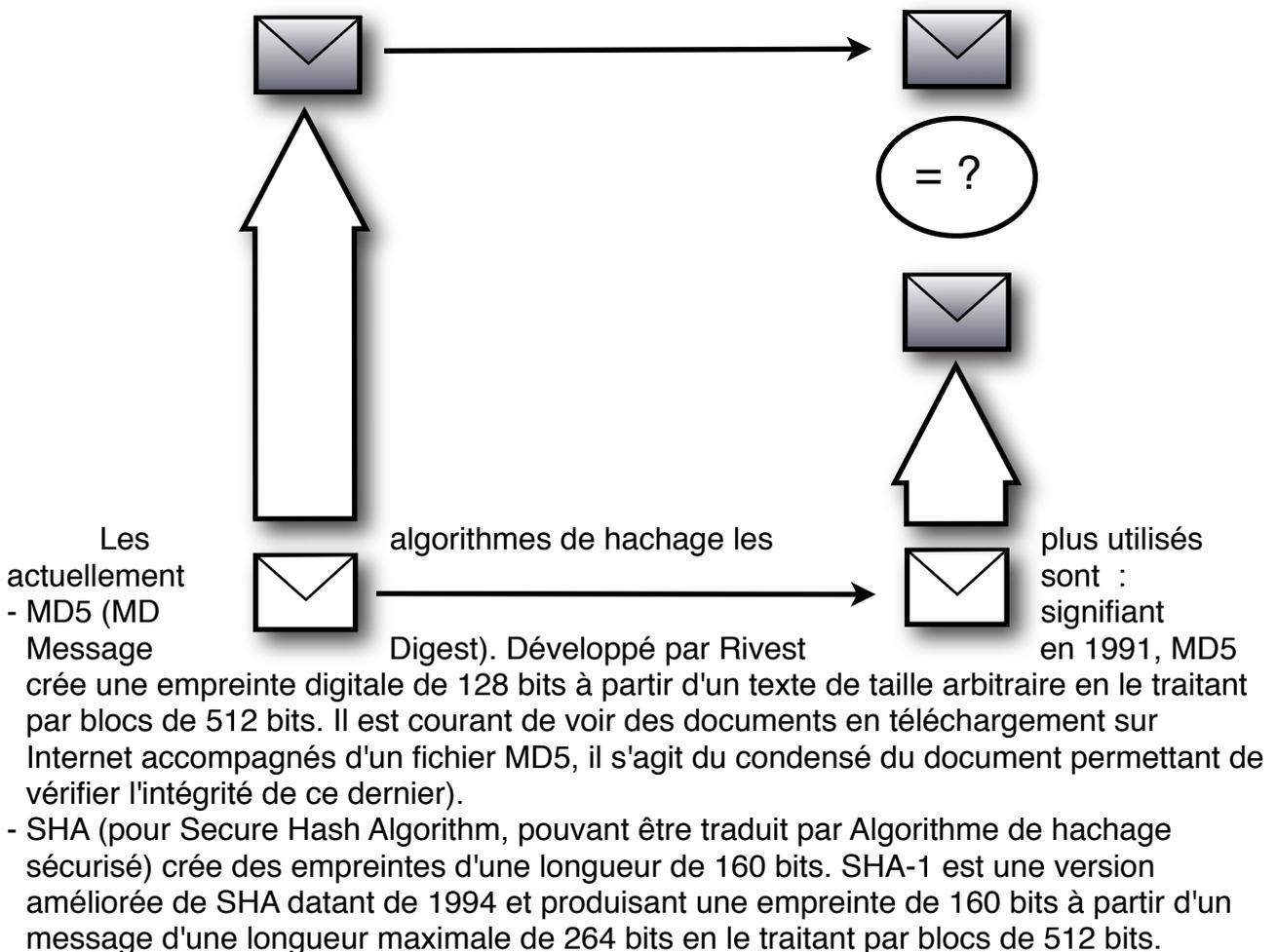
Il génère pour chaque document un nombre de 128 ou 168 bits, que les anglosaxons appellent "digest" et qu'en français, on appelle parfois résumé...

La fonction de hachage doit être telle qu'elle associe un et un seul condensé à un texte en clair (cela signifie que la moindre modification du document entraîne la modification de son condensé).

D'autre part, il doit s'agir d'une fonction à sens unique (one-way function) afin qu'il soit impossible de retrouver le message original à partir du condensé.

En expédiant un message accompagné de son haché, il est possible de garantir l'intégrité d'un message, c'est-à-dire que le destinataire peut vérifier que le message n'a pas été altéré (intentionnellement ou de manière fortuite) durant la communication.

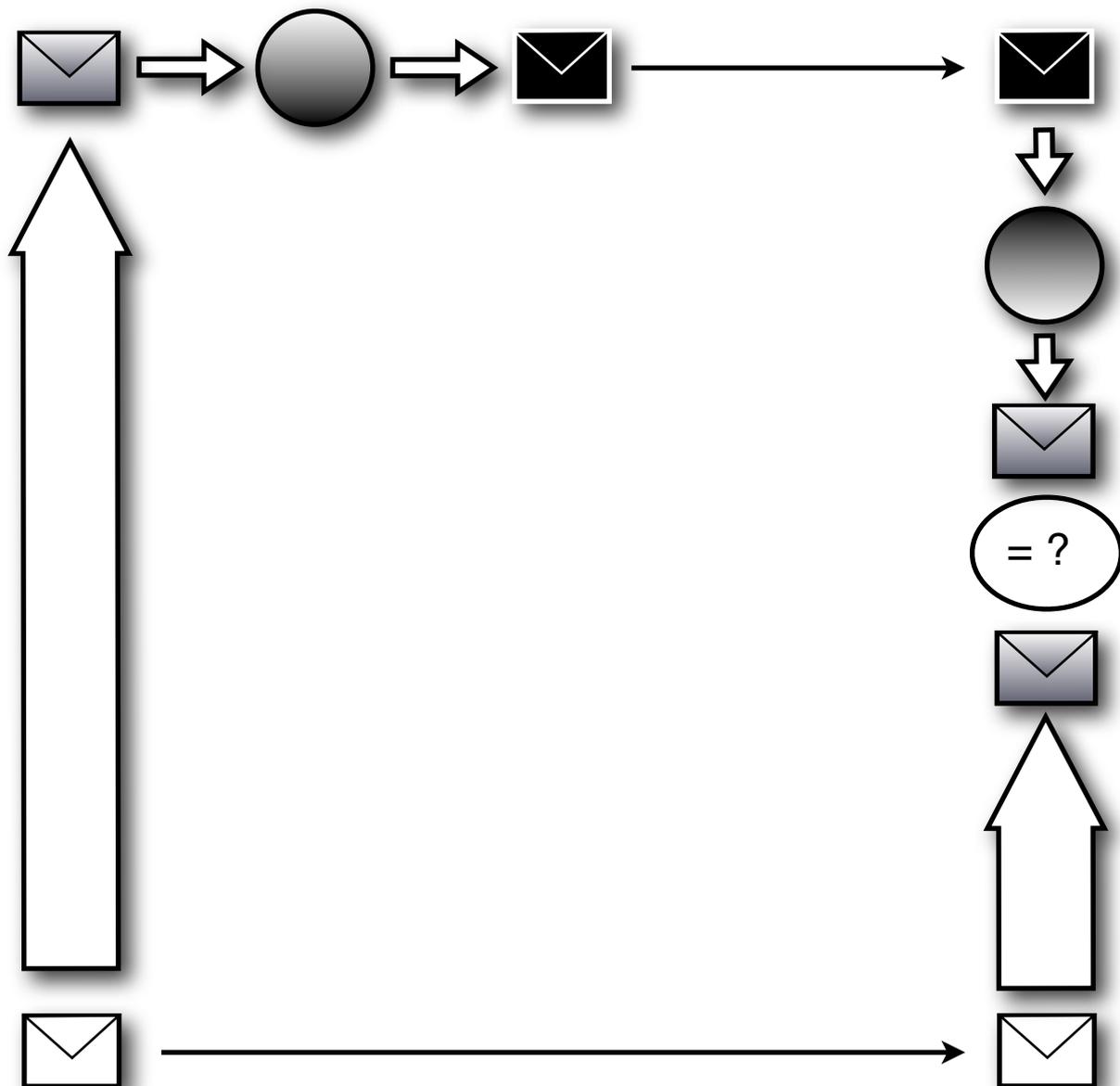
Lors de la réception du message, il suffit au destinataire de calculer le haché du message reçu et de le comparer avec le haché accompagnant le document. Si le message a été falsifié durant la communication, les deux empreintes ne correspondront pas.



2.3. Application:

L'utilisation d'une signature électronique se divise donc en six étapes:

- L'émetteur génère une empreinte du document à signer.
- L'émetteur procède ensuite au chiffrement de l'empreinte avec sa clé privée.
- L'émetteur envoie le document original, l'empreinte chiffrée et la partie publique du certificat.
- Le récepteur déchiffre l'empreinte chiffrée avec la clé publique.
 - ➔ Vérification de l'identité de l'émetteur.
- Le récepteur génère une nouvelle empreinte du document et la compare à l'empreinte envoyée.
 - ➔ Vérification de l'intégrité du document.
- Le récepteur consulte l'autorité de certification sur la validité du certificat.
 - ➔ Vérification de la fiabilité de la signature.



3. Force probatoire et limites de la signature électronique:

Même assimilé à l'écrit papier, l'écrit sous forme électronique se doit de respecter certaines conditions :

- Être intelligible
- Permettre d'identifier celui dont il émane
- Être établi et conservé dans des conditions de natures à garantir son intégrité.

3.1. La force probatoire : définition

L'acte authentique fait foi de son contenu, s'agissant des éléments constatés et vérifiés par le notaire. On ne peut rapporter la preuve contraire que par une procédure complexe, équivalente à celle de la contestation d'une décision judiciaire pour partialité du juge...

Pour définir la force probatoire de la signature électronique, on va s'appuyer sur plusieurs exemples tels que :

- l'acte sous seing privé:

L'acte sous seing privé est exigé par la loi (article 1341 du code civil) pour faire preuve de toute obligation souscrite par des personnes non commerçantes et dont la valeur excède 800 euros. L'on entendait traditionnellement par acte sous seing privé la réunion d'un écrit sur support papier et d'une signature manuscrite.

En effet, notre système probatoire a été élaboré dans un contexte où seules ces formes d'écriture étaient connues. Les règles de preuve classiques ont donc dû être adaptées à l'apparition des nouvelles technologies.

Sous l'influence des règles communautaires, des textes récents, au premier rang desquels la loi du 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, ont profondément bouleversé notre système de preuve.

Aujourd'hui, l'acte sous seing privé électronique est reconnu juridiquement et permet de faire pleine preuve des conventions pour lesquelles sa constitution est exigée. La loi bannit désormais toute hiérarchie entre l'acte sous seing privé sur support papier et l'acte sous seing privé dématérialisé : leur force probante est strictement équivalente, comme le reconnaît expressément l'article 1316-3 du Code civil.

Si un conflit de preuve survient, par exemple, si une convention a été souscrite par voie électronique, mais a été également rédigée sur support papier en des termes différents, c'est au juge qu'il appartiendra de trancher, en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support (article 1316-2 du Code civil).

Toutefois, tout comme pour son équivalent non dématérialisé, l'acte sous seing privé électronique doit réunir deux éléments : un écrit et une signature. Si la loi proclame aujourd'hui l'équivalence entre l'écrit et la signature électronique et leurs formes traditionnelles sur support papier, elle indique également avec précision les conditions de cette assimilation.

En effet, le document électronique, qui peut se révéler aisément falsifiable, doit offrir les mêmes garanties d'intégrité, d'authenticité et de durabilité que le document papier.

- l'acte authentique

L'acte authentique est l'acte reçu, avec les solennités requises, par un officier public ayant compétence pour instrumenter dans le lieu où il a été rédigé.

Il se différencie de l'acte sous seing privé signé seulement par les parties, qui n'implique pas la présence du rédacteur, et qui peut être régularisé en tout lieu, y compris à l'étranger.

3.2. La signature électronique notariale certifiée:

Le notariat Français est la première profession en Europe à s'être dotée d'une signature électronique propre, répondant à toutes les exigences de sécurité en la matière.

Le but de cette signature est justement de garantir l'intégrité des documents échangés numériquement concernant tous les actes notariés. La signature devient alors incontestable, puisque certifiée.

Il faut savoir que la mise en place d'un tel système était recommandée par le décret n° 2005-973 du 10 Août 2005, qui exigeait que le notariat se plie aux prescriptions de la loi du 30 Mars 2001 quant à la mise en place d'un procédé sécurisé permettant l'échange électronique sécurisé de données officielles.

3.2. Limites de l'admissibilité et la force probatoire de l'écrit électronique

L'écrit sous forme électronique est désormais admis comme 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.*" (code civil ; art. 1316-1).

Cette admissibilité est soumise à la double condition de l'identification de celui dont l'écrit émane et à la conservation de l'écrit dans des conditions de nature à en garantir son intégrité.

L'admissibilité de l'écrit électronique est par ailleurs étendue à l'acte authentique sous forme électronique. Celui-ci dispose de la même force probante que l'acte authentique sur support papier sous réserve, notamment, que la signature électronique apposée par l'officier public réponde aux conditions de fiabilité fixées par décret (à paraître).

Enfin, l'écrit sur support électronique "*a la même force probante que l'écrit sur support papier*" (code civil ; art. 1316-3).

NB : Le Pr Gautier, dans son article dans le recueil Dalloz du 23 mars 2000, précise que "*la (...) loi n'introduit au même rang que le papier que dans la mesure où la forme n'est requise qu'au titre probatoire, mais ne pourra donc pas être validé lorsque la forme de l'écrit sera indispensable pour valider l'acte (fonction solennelle)*".

CONCLUSION

Avec la mise en oeuvre de la signature électronique, le droit français a résolu en partie les questions de preuve générées par le développement des nouvelles technologies de l'information (Internet).

Sous l'impulsion de la directive européenne du 13 décembre 1999, la loi du 13 mars 2000 et ses décrets d'application confèrent aujourd'hui un véritable cadre juridique à la signature électronique.

En effet, grâce à la combinaison d'une fonction de hachage et d'un chiffrement asymétrique (clé privée/clé publique), cette dernière permet à son destinataire de reconnaître l'identité de son auteur, l'authenticité et l'intégrité du document.

La signature électronique constitue dès lors une valeur probante équivalente à celle de la signature manuscrite pour le support papier.

Concernant la force probatoire, l'écrit électronique n'est assimilé à l'écrit papier que sous des conditions de solennité (il en est de même en matière d'acte notarié), et l'écrit électronique n'a de force probatoire que si l'écrit papier n'est pas exigé.

BIBLIOGRAPHIE

- **Ouvrages:**

BOCQUILLON Jean-François et Martine MARIAGE, *Droit, BTS IUT AES Ecoles de commerce*, Paris, Dunod, 2001,464.

CODE CIVIL, Paris, Litec, 2006

BENSOUSSAN Alain, *Internet aspects juridiques*, Paris, Hermès, 1996

- **Sites Internet:**

<http://www.juriscom.net>

<http://www.signelec.com>

<http://www.notaires.fr>

<http://www.commentcamarche.net>

<http://www.SSI.gouv.fr>

<http://www.Fomento.es>

<http://www.linux-france.org>