Le droit de la preuve électronique
La signature électronique[1]

*Maître Alain BENSOUSSAN**

La problématique de la transmission par voie électronique, des feuilles de soins renvoie aux questions génériques qui concernent toutes les opérations utilisant ce moyen de transmission. Ces questions découlent du fait que, l'opération n'est pas conclue en présence des acteurs mais à distance et sur un support qui n'est plus le papier. Elles sont essentiellement de deux types :

- la preuve de l'engagement ;
- la sécurisation des échanges.

Il convient en effet de s'assurer d'une part que les moyens de preuve pourront être rapportés et donc conservés, alors même que les transactions se réalisent de façon incorporelle, d'autre part que la personne qui s'engage est bien la personne concernée, alors même que son existence ne peut être vérifiée par sa présence physique.

La dépersonnalisation des relations et la dématérialisation des opérations constituent les deux défis que pose l'administration de la preuve en matière informatique[2].

Nous constaterons une fois de plus que le Code civil a su édicter des principes fondamentaux qui continuent à s'appliquer malgré les multiples changements techniques, culturels et sociaux survenus depuis sa création.

C'est fondamentalement grâce à une absence de définition, laquelle aurait été nécessairement liée à l'état de la technique prévalant à l'époque, que les dispositions du Code civil permettent aujourd'hui, secondées par la technologie qui apporte à son tour des solutions aux problèmes qu'elle suscite, de répondre à ces deux questions.

* *ALAIN BENSOUSSAN, AVOCATS*

LA PREUVE DE L'ENGAGEMENT

Avant d'aborder le droit de la preuve électronique, un retour en arrière s'impose pour examiner l'évolution de la preuve dans notre droit.

La preuve est un élément déterminant du droit.
Revendiquer un droit sans en rapporter la preuve est souvent inopérant.
Le mécanisme de la preuve implique la création de la preuve, son administration et son caractère de force probante.

Traditionnellement, la preuve des actes renvoie à la notion d'original et plus précisément à la notion de documents écrits et signés : ainsi le testament olographe doit-il être intégralement rédigé de la main de son auteur.

Un original c'est un sujet, un texte et une signature. Or le Code civil ne définit ni la notion d'écrit ni celle de signature[3].

Si les règles qu'il institue en matière de preuve sont fondamentalement fondées sur la notion d'écrit, d'autres moyens de preuve ont été mis en place à défaut d'écrits. Ainsi, à côté de la preuve par acte authentique, forme solennelle imposée pour certains actes, notamment en matière patrimoniale, et outre

(1) Ce texte est la transcription de l'intervention de Me Alain BENSOUSSAN lors de la session de formation du CNEH le 22 octobre 1998.

(2) "Contribution théorique au droit de la preuve dans le domaine informatique : aspects juridiques et solutions techniques", Alain BENSOUSSAN, Gazette du Palais, *17 et 18 juillet 1991.*

(3) Un projet de loi daté du 29 octobre 1998, relatif à l'adoption du droit de la preuve aux nouvelles technologies, propose notamment une définition de la signature.

l'exigence de formalités particulières pour certains actes, il a été prévu qu'à défaut de pouvoir rapporter la preuve par écrit, celle-ci pourrait être rapportée par témoin, par les présomptions de preuve établies par la loi ou laissées à l'appréciation du juge, par l'aveu ou le serment. La preuve peut également être rapportée par la production d'une copie qui est la reproduction non seulement fidèle mais aussi durable d'un original non conservé.

En matière commerciale, la règle est très assouplie, la preuve entre commerçants pouvant être rapportée par tout moyen.

L'absence de définition, conjuguée à cette ouverture vers d'autres modes de preuves que l'écrit, a permis d'envisager d'autres formes en matière de preuve, formes indispensables pour sécuriser les opérations faites par des moyens électroniques.

L'APPROCHE CONTRACTUELLE

La nécessité de conserver les preuves trouve sa solution dans diverses formes :

Les règles de l'article 1341 du Code civil en matière de preuve pour les opérations excédant un certain montant ne sont pas d'ordre public. Les parties peuvent y déroger en aménageant elles-mêmes les conditions de preuve des opérations à intervenir entre elles. C'est ainsi que la Cour de cassation, par arrêt du 8 novembre 1989, a consacré la licéité de ce type de convention, validant ainsi le principe de la signature électronique composée de l'usage d'une carte bancaire assortie de la composition d'un code confidentiel.

Pour les contrats de carte bleue, les enregistrements des appareils automatiques constituent pour l'établissement émetteur, la preuve des opérations effectuées au moyen de la carte. Il en est de même pour la présomption de fonctionnement des compteurs (eau, gaz, électricité...).

À côté des conventions de preuve, se sont développés les accords d'interchange organisant les échanges de documents informatisés (EDI).

Ce type d'accord prévoit des clauses relatives à :

- la validation juridique des documents dématérialisés représentés par les messages EDI,
- la conservation et l'archivage des échanges électroniques,
- la responsabilité,
- la sécurité et la confidentialité des échanges.

Est associé aux conventions de preuve, le principe du contradictoire. Cet échange critique devant le juge permet de mesurer sa résistance à la contestation et donc la portée de sa force probante.

Les parties peuvent désigner un tiers certificateur qui authentifiera et certifiera l'échange électronique intervenu entre elles. Son rôle sera de sécuriser les transmissions de messages sans intervenir sur leur contenu et d'améliorer ainsi la qualité de la preuve.

L'APPROCHE NORMATIVE

L'AFNOR a élaboré en juin 1998 une norme portant sur la conception et l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des enregistrements stockés dans ces systèmes[2].

Cette norme vise à obtenir des systèmes d'archivage permettant de répondre aux critères de preuve fidèle et durable prévus par l'article 1348 du Code civil et détermine des critères de fiabilité du système d'exploitation.
Pour répondre à la définition de l'article 1348 du Code civil selon laquelle "est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support", la norme Z42-013 élaborée par l'AFNOR sélectionne exclusivement le disque optique numérique de technologie WORM, c'est-à-dire non réinscriptible. En ce qui concerne le critère de fidélité, celui-ci n'étant pas déterminé par le Code civil, la fiabilité des techniques de reproduction sera laissée à l'appréciation souveraine des tribunaux.

La norme prévoit des mesures de conservation telles que la traçabilité des opérations, l'horodatage, l'établissement d'un dossier de description technique du

(2) "Archivage électronique : une norme pour 1998" Isabelle Pottier, Les Echos, *3 février 1998*

système, l'enregistrement séquentiel des images sans aucun espace entre deux enregistrements successifs, des audits périodiques[3].

L'APPROCHE TECHNOLOGIQUE

Nous évoquions ci-dessus la notion de fidélité de la copie. En application de la théorie probabiliste des modes de preuve, la fidélité est obtenue dès lors que la preuve de la fraude tend vers zéro. Cette preuve est alors associée à la fiabilité d'un système technique de preuve, celui-ci étant fiable lorsque le processus de fabrication de copie de l'original a une probabilité d'erreur proche de zéro[4].

C'est ainsi que la technologie, eu égard à la nouveauté des moyens qu'elle représente, après avoir suscité des interrogations sur la preuve y apporte des solutions.

De fait, l'évolution des moyens techniques permet d'aboutir à des preuves juridiquement supérieures à certaines preuves classiques, un exemple évident étant l'identification par le test de l'ADN.

La signature électronique

La signature est le corollaire de la preuve écrite.
Elle n'est pas définie par le Code civil, laissant ainsi la liberté d'envisager d'autres formes.

C'est ainsi qu'a été admise par la jurisprudence, la signature électronique composée de l'usage d'une carte bancaire assortie de la composition d'un code confidentiel[5].

Au niveau européen, une proposition de directive vise à harmoniser le cadre juridique de la signature électronique. Celle-ci fait jusqu'à présent l'objet de réglementations disparates entre les différents pays membres de l'Union européenne.

L'objectif de la Commission est d'accroître les besoins de sécurité des usagers de l'internet.
Outre la sécurité, la proposition vise à assurer la reconnaissance juridique des signatures électroniques qui pourront, par ailleurs, ne pas être limitées à des signatures numériques basées sur la cryptographie à clef publique.

La cryptologie

La cryptologie est un ensemble technique de moyens, matériels ou logiciels, permettant, suivant les technologies, d'authentifier un message ou de protéger l'intégrité du contenu, d'assurer la confidentialité des informations et la non-répudiation par le destinataire de la réception du message. Basés sur des algorithmes et des conventions secrètes, ces systèmes permettent d'assurer une ou plusieurs desdites fonctions.

La cryptologie fut longtemps réservée aux applications touchant la défense nationale et la sécurité de l'État. Son régime s'est peu à peu assoupli pour aboutir, par la loi du 26 juillet 1996 et ses décrets et arrêtés de 1998, à une libération complète de son utilisation pour certaines opérations ainsi qu'à la réduction du nombre des opérations soumises à déclaration ou autorisation préalable. Cette libéralisation répond aux besoins liés au développement du commerce électronique. La cryptologie est désormais d'utilisation libre pour la protection des mots de passe, la signature, les preuves en matière d'authentification de l'émetteur ou du destinataire et d'intégrité des messages.

LA SÉCURISATION DES ÉCHANGES

Avoir la preuve de l'échange est indispensable.

Il est tout aussi nécessaire de sécuriser cet échange et d'en assurer la confidentialité.

En matière d'opération à distance, il est indispensable d'être sûr que la personne qui s'engage est bien la personne concernée.

Le deuxième impératif est que le message ne puisse pas être répudié par le récepteur.

L'identification, l'authentification et la non-répudiation règlent le problème du sujet de droit.

(3) "Le commerce électronique : aspects juridiques" Alain Bensoussan, Editions Hermès, 1998
(4) Alain Bensoussan, "Contribution théorique au droit de la preuve... " (précité)
(5) CA Montpellier, 9 avril 1987, JCP 1988, II, 20984. Cass civ 1ère 8 novembre1989 (précité) Bull civ n° 342.

La signature électronique apporte une réponse à ces trois préoccupations dès lors que, comme la preuve, elle a une force probante et répond à la fonction de signature manuscrite qui est d'identifier et d'authentifier le signataire.

L'article 2 du projet de directive susvisé précise que la signature électronique devra satisfaire aux exigences suivantes : 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 détectée.

Devançant la signature de cette directive, le décret du 9 avril 1998 relatif à la carte de professionnels de santé énonce que "la signature électronique produite par la carte de professionnel de santé est reconnue par les administrations de l'État et les organismes de sécurité sociale comme garantissant l'identité et la qualité du titulaire de la carte ainsi que l'intégrité du document signé".

Le décret ajoute : "ainsi signés, les documents électroniques mentionnés à l'article L.161-33 sont opposables à leur signataire".

L'arrêté du 9 avril 1998 relatif aux spécifications physiques de la carte de professionnel de santé fait appel à la cryptologie pour assurer notamment les fonctions de signature électronique, d'authentification de la carte et de sécurité et de protection des données.

La mise en place de ce système va permettre une sécurisation de la feuille de soins électronique à 10^{11} près.

Si l'on compare cette probabilité à celle existant en matière pénale, on constate que :

- deux personnes sont considérées comme identiques à 10^{4} près, par l'identification de leurs empreintes digitales ;
- deux personnes sont considérées comme ayant la même empreinte génétique à 10^{9} près.

Or, aujourd'hui, la carte SESAM-VITALE et, de manière générale, tous les systèmes utilisant la cryptographie (algorithmes de type DES et RSA) sont vrais à 10^{11} près.

Dans un tel contexte, une feuille de soins électronique est au moins égale, en termes de force probante, à la feuille de soins papier.

Ainsi qu'il est rappelé ci-dessus et conformément au décret du 24 février 1998, l'utilisation de la cryptologie pour l'authentification de la personne et l'intégrité du message est libre.

Il reste à être certain que l'intégrité du message sera respectée, que sa confidentialité sera conservée et que le document ne pourra pas être remplacé par un autre.

La feuille de soins électronique devra répondre à toutes ces exigences, d'autant que la sécurisation des échanges est ici de deux ordres :

- s'assurer que les informations transmises, les décisions prises, les éléments financiers indiqués ne seront pas déformés, détournés, perdus ;
- s'assurer que le secret professionnel est préservé de façon absolue.

Le secret professionnel est celui qui s'impose au médecin sur le fondement de l'article 4 du Code de déontologie médicale institué par le décret 95-1000 du 6 septembre 1995 en ces termes : "le secret professionnel, institué dans l'intérêt des patients, s'impose à tout médecin dans les conditions établies par la loi. Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris."

L'article 226-13 du Code pénal qui énonce que "la révélation d'une information à caractère secret par une personne qui en est dépositaire, soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 100.000 francs d'amende", étend le secret professionnel non seulement au médecin, mais également à d'autres catégories professionnelles du secteur de la santé, que ces dernières exercent dans ce secteur une activité médicale ou une activité administrative, financière ou organisationnelle.

Le décret du 24 février 1998 permet d'utiliser librement la cryptologie pour les fonctions assurant la confidentialité des messages à la condition toutefois que les clefs utilisées soient générées par un tiers dénommé "tiers de confiance", si les clefs de chiffre-

ment sont supérieures à 40 bits[4].

En l'espèce, les clefs de chiffrement de l'algorithme retenu par l'arrêté du 9 avril 1998, utilisées pour la mise en œuvre du service de confidentialité, seront confiées à un organisme agréé dans les conditions prévues par le décret susvisé.

Ces clefs permettront notamment d'assurer l'unicité des documents et, en cas de contestation, de pouvoir le vérifier ; une telle procédure dite procédure de "rejeu" a été mise en place dans le cadre du transfert dématérialisé des données fiscales et comptables à l'administration.

S'il apparaît aujourd'hui que les aspects identification, authentification, intégrité et non-répudiation, qui permettent d'être sûr du sujet et de son engagement, et les aspects sécurité et confidentialité, sont assurés par le recours à des moyens cryptologiques dont on a vu la force probante, il reste à s'interroger sur les déterminants fondamentaux du tiers de confiance devant permettre au monde médical de garder la maîtrise des informations médicales.

(4) Le décret N°99-200 du 17 mars 1999 porte ce seuil à 128 bits (J.O. du 19 mars 1999, p. 4051)