PREUVE ET SIGNATURE ELECTRONIQUES : DE LA LOI DU 13 MARS 2000 AU DECRET DU 30 MARS 2001

S'inscrivant dans un contexte international et communautaire[1], la loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et à la signature électronique et son décret d'application du 30 mars 2001 précisent d'une manière substantielle la situation juridique de la signature électronique.

La preuve informatique passe désormais du statut de commencement de preuve par écrit à celui de preuve parfaite. La loi reconnaît pleinement la preuve électronique (I). Cependant cette reconnaissance passe par la mise en œuvre de strictes conditions de validité (II).

I. La reconnaissance de la preuve et de la signature électroniques

Cette reconnaissance n'est pas nouvelle puisque la jurisprudence a déjà admis la licéité des conventions sur la preuve en matière de paiement dématérialisé par carte bancaire[2]. La loi nouvelle élargit simplement cette possibilité à défaut d'accord préalable. Plus récemment, la Chambre commerciale de la Cour de cassation[3] a naturellement aplani la hiérarchie des modalités probatoires en estimant qu'une télécopie était assimilable à un écrit sous certaines conditions.

La loi, pour la première fois, donne une définition de la **preuve littérale** qui peut résulter *« d'une suite de lettres, de caractères, de chiffres, ou de tous autres signes ou symboles dotés d'une signification intelligible »* (art. 1316).

L'écrit électronique possède désormais la **même valeur probante que l'écrit papier** (art. 1316-3). Pour ce qui concerne les conflits de preuve, le texte les soumet à l'appréciation du juge qui détermine *« par tous moyens le titre le plus vraisemblable »* (art. 1316-2). Autant dire que si les parties n'ont pas conventionnellement réglé ce problème, la preuve écrite primera - les premières années, tout au moins - sur la preuve électronique, même si nous considérons qu'il est plus aisé de falsifier un écrit papier que de transformer un écrit électronique sécurisé. Il faut en effet, pour le développement du commerce électronique, que les systèmes informatisés d'échanges jouissent d'une présomption de fiabilité.

Quant au champ d'application du texte, la loi n'exclut pas expressément les contrats pour lesquels l'exigence indispensable (*ad validitatem* disent les juristes) d'un écrit manuscrit est indispensable, telles de nombreuses relations juridiques entre professionnels et particuliers[4]. En effet, admettre une confirmation par l'écrit-papier pour de tels actes viderait la loi de sa substance. Il est à noter que la loi prévoit aussi l'acte authentique électronique (le notaire virtuel) ; *a fortiori*, tous les actes sous seing privé, fussent-ils solennels, doivent pouvoir être dématérialisés à condition de respecter le formalisme requis sous forme électronique.

La sécurité et l'efficacité juridiques commanderaient donc de manière plus pragmatique que de telles conventions puissent être passées électroniquement, sous réserve d'une éventuelle confirmation, elle aussi dématérialisée. D'ailleurs, la directive sur le commerce électronique du 8 juin 2000 dispose que *« les États membres veillent à ce que le régime juridique applicable au processus contractuel ne fasse pas obstacle à l'utilisation des contrats électroniques ni ne conduise à priver d'effet et de validité juridique de tels contrats pour le motif qu'ils sont passés par voie électronique* » (art. 9). Dans le même sens, la directive du 13 décembre 1999 relève que *« les États membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que la signature se présente sous forme électronique »* (art. 5, 2.).

La preuve électronique reconnue, reste à déterminer, techniquement, dans quelles conditions la signature du document dématérialisé devient réellement efficace. C'est l'œuvre du récent **décret**

1. La loi et le décret intègrent en effet certains points de la directive du 13 décembre 1999 relative au cadre communautaire pour les signatures électroniques.
2. Cass. civ., 1ère, 8 novembre 1989, Affaire CREDICAS.
3. Cass. com., 2 décembre 1997.
4. On pense notamment au droit formel de la consommation ou aux crédits immobiliers.

du 30 mars 2001, pris pour l'application de l'article 1316-4 du Code civil qui dispose, quant aux conditions de fiabilité de la signature électronique que *« 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. »*

II. Les conditions de la reconnaissance

Le décret du 30 mars 2001 a pour finalité de mettre en évidence les moyens techniques de sécurisation d'un échange électronique permettant de satisfaire les deux conditions fondamentales de validité d'une signature électronique : le respect de **l'intégrité** du message et la preuve de **l'imputabilité** de ce message.

Ces conditions d'efficacité conditionnent la validité de l'acte et visent la non-déformation du message en amont et en aval, c'est-à-dire pendant la rédaction, la transmission, la lecture et la conservation. Trois critères sont à prendre en compte : l'immutabilité quant à la transmission, quant à la date et quant à la conservation, soit, en d'autres termes, **l'authentification** globale du message. Pour réunir ces trois conditions, on aura recours de manière très classique à des procédés techniques tels la cryptologie, la tierce certification et l'archivage électronique.

Pour ce qui concerne la **fiabilité** du message, le décret édicte, dans son article 2, une disposition essentielle selon laquelle *« 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. »*

Tout le décret tient dans cet article. Sans vouloir être exhaustif, on retiendra trois critères de base.

- la signature doit être **sécurisée** : pour satisfaire cette exigence, seuls des outils de cryptologie semblent pouvoir être employés. Sans entrer dans des détails techniques, le système de cryptage repose sur un chiffrement asymétrique avec une clé privée et une clé publique utilisées de manière cumulative et identique pour chacune des parties à l'acte[5]. Il s'agit principalement de rendre l'acte infalsifiable.

A contrario, et tout à fait à l'encontre de l'esprit de la loi du 13 mars 2000, toute signature non sécurisée par de tels moyens sera présumée non fiable et donc aisément contestable en justice. La fiabilité de la signature passerait donc inéluctablement par l'intervention d'un tiers à l'acte.

- la signature doit être **certifiée** : une telle sécurité avancée passe aussi par le recours à des prestataires de certification. Ce seront des tiers qui fourniront non seulement des certificats de validité mais qui seront le plus souvent chargés de la conservation de la preuve.

Plus aberrantes sont les conditions d'existence de ces prestataires de certification : une procédure d'agrément des certificats délivré par les services du Premier ministre est mise en place (et l'agrément sera même publié au Journal Officiel !) doublée d'un contrôle *a posteriori* consistant en la mise en place d'un Comité directeur de la certification, toujours institué par les mêmes services. Il s'agit d'une réminiscence de l'époque (très récente, avant l'année 1996) où la cryptologie était exclusivement réservée aux services de l'Etat, en particulier au Ministère de la défense. Le retour de l'Etat gendarme est tout à fait inopportun, la qualité n'émanant pas à titre exclusif d'un centralisme exacerbé.

Nul doute, en tous cas, que les prestataires de services de certification seront de véritables agents de la preuve, avec la responsabilité et le système de garantie accolés à cette charge.

- la signature doit être **vérifiable** : à tout moment, il doit être possible d'établir le lien entre un document et son auteur, ce que nous avons appelé l'imputabilité du message. Cette vérification s'effectue par le truchement d'un certificat dit qualifié permettant la révélation, par le tiers certificateur, du contenu et de l'auteur du message ainsi que des moyens de cryptologie employés.

Enfin, aucune disposition du décret ne dévoile la durée pendant laquelle l'acte électronique devra être archivé. En sachant que la directive du 13 décembre 1999 n'est ni prolixe ni très

5. Pour un exemple pratique, voir H. BITAN, *La signature électronique : comment la technique répond-t-elle aux exigences de la loi ?*, Gaz. Pal., 19/20 juil. 2000, p.12.

éclairante sur ce point, puisqu'elle nous renvoie, dans son annexe II, à une conservation pendant le *« délai utile »*, on pourra en déduire que le délai d'archivage est rattaché aux documents papiers et pourra donc être d'un délai trentenaire.

En définitive, alors que le système de la carte à puce commence à présenter de sérieuses failles[6], l'avènement de la cryptologie ne convainc pas tout à fait, étant donnée la perpétuelle remise en cause des systèmes de sécurité (notamment des *firewalls*).

Très certainement, le décret d'application et surtout les arrêtés très techniques - qui ne manqueront pas de pallier les carences du décret - relatifs à la garantie de *"l'infalsifiabilité"* de l'acte devront être très régulièrement actualisés.

Jean LECLERCQ
Docteur en droit
Avocat
j.leclercq@avocat.org

6. Voir l'affaire HUMPICH, notament sur www.Legalis.net.