

Modernité et intelligibilité du droit de la preuve français*

Jean-François Blanchette

Assistant Professor

Department of Information Studies, University of California, Los Angeles

GSE&IS Bldg., Box 951520, Los Angeles, CA 90095-1520, USA

Tél: +1 310 267 5137; Fax: +1 310 206 4460

Email: blanc@ucla.edu; Web: <http://polaris.gseis.ucla.edu/blanchette>

Résumé: la loi du 13 mars 2000 « portant adaptation du droit de la preuve aux technologies de l'information et à la signature électronique » devait exprimer la force d'adaptation du droit français face à la nouvelle d'une mondialisation et informatisation des échanges commerciaux. Dans cet article, nous suggérons que les deux principaux éléments de cette réforme – définition de l'écrit et de la signature électronique – originent de problématiques distinctes, aux solutions ultimement incompatibles. Nous suggérons que l'incohérence de cette réforme menace, tant matériellement que conceptuellement, un fondement du droit de la preuve français, son intelligibilité. Nous présentons ensuite une série de principes généraux, issus de la communauté archivistique, à même d'inspirer des réformes législatives plus aptes à assurer une transition harmonieuse vers une ère où l'écrit électronique signé joue un rôle de plus en plus important dans la vie administrative et juridique des citoyens.

I – Introduction

Peut-être plus que tout autre développement technologique l'ayant précédée, l'explosion des nouvelles technologies de l'information et de la communication (NTIC) a semblé questionner tant la pertinence que l'efficacité du droit comme instrument de régulation de l'espace social. Par sa plasticité, sa reproductibilité et sa libre circulation au travers de réseaux toujours plus étendus et interconnectés, l'information numérique a semblé, pour un instant du moins, remettre en question certaines des institutions juridiques les plus importantes du monde industriel: propriété intellectuelle, contrat, régulation des télécommunications, etc.

Cette apparente capacité à défier le droit a justifié en 1997 la commande par le Gouvernement d'une étude au Conseil d'état, dans le but d'identifier les moyens s'offrant à l'État pour réguler efficacement ces médias.¹ Publié en 1998, le rapport a réaffirmé en toute confiance le rôle du droit comme « instrument privilégié de la construction de ce nouvel espace », soulignant que non seulement « les questions juridiques suscitées par le développement d'Internet et des réseaux numériques ne sont pas de nature à remettre en cause les fondements mêmes de notre droit », mais qu'au contraire, « elles confirment

* Cet article est le fruit d'une réflexion amorcée dans le cadre du groupe de travail « Actes authentiques électroniques », (voir Isabelle de Lamberterie (s.l.d.) *Les actes authentiques électronique – Réflexion juridique prospective*, Paris: La Documentation Française, 2001). J'ai particulièrement bénéficié de mes conversations avec Isabelle de Lamberterie, Françoise Banat-Berger et Luciana Duranti. Ces idées ont été présentées au séminaire de formation continue « Justice en Perspectives » organisé par Jean-Paul Jean à l'Ecole nationale de la magistrature, le 15 novembre 2002.

¹ Conseil d'état, *Internet et les réseaux numériques*, (Paris: La Documentation Française, 1998).

la pertinence de la plupart des concepts généraux, parfaitement transposables à ce nouvel environnement, même si certaines adaptations sont nécessaires² ».

Cet article discute les conditions de cette « transposition » et de cette « adaptation », dans le contexte du droit la preuve, contexte particulièrement intéressant parce qu'il n'est pas seulement territoire d'application du droit, il est également celui de son exercice: d'une part, le droit de la preuve est un mécanisme de régulation sociale constitué de règles simples — au premier chef, celle de la préconstitution de la preuve par confection d'un écrit papier signé — permettant aux contractants d'éviter ou de résoudre les contentieux; d'autre part, l'exercice même du droit est indissociable des multiples formes de l'écrit juridique — rédigé, signé, et archivé par les autorités compétentes. Cet article souligne que, dans un cas comme dans l'autre, la transposition et l'adaptation des principes du droit de la preuve au contexte des transactions électroniques, loin d'un simple aménagement mécanique, est synonyme de bouleversements profonds qui n'épargneront ni les principes qui sous-tendent, ni les pratiques qui entourent, le droit de la preuve.

Du point de vue législatif, trois dates marquent, à ce jour, la définition du nouveau cadre juridique du droit de la preuve:

- le 13 décembre 1999, avec la publication de la Directive européenne « sur un cadre communautaire pour les signatures électroniques³ »;
- le 13 mars 2000, avec la loi « portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique⁴ »;
- le 30 mars 2001, avec l'adoption du décret « pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique⁵ ».

Ces dates fournissent une grille de lecture supplémentaire au contenu juridico-régulatoire des textes en question : elles encadrent le début, milieu et fin de la fièvre spéculatrice sur les technologies de l'Internet, et son extraordinaire emprise sur le discours public en France et en Europe durant cette période. Cette euphorie dissipée, il devient à présent possible d'examiner plus sereinement la question des paramètres de cette transposition et de cette adaptation : quelles règles de droit sont susceptibles d'être transposées, quelles autres d'être adaptées? Quels principes doivent guider la main du législateur, lorsqu'il transpose et adapte? Dans les deux cas, de quelle façon peut-on

² Ibid. 12.

³ Directive 1999/93/CE du Parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, JOCE du 19 janvier 2000, L 13, p. 12.

⁴ 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, JO du 14 mars 2000, p. 3968.

⁵ Décret no. 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, JO du 31 mars 2001, p. 5070.

assurer que la transposition et l'adaptation ne menace pas la finalité du droit de la preuve, assurer la sécurité des échanges par la définition d'un cadre juridique stable et intelligible? Bien que quelques-unes des grandes lignes du paysage de la preuve électronique soient déjà tracées, ces questions demeurent toujours pertinentes, puisque nous savons désormais qu'elles ne se présentent pas dans le contexte d'une quelconque *révolution* du numérique, mais plutôt, dans celui d'une *mutation*, mutation somme toute assez lente et entamée depuis déjà plusieurs années.

Cet article propose de replacer en leur contexte certains des éléments de cette mutation et de la législation complexe qui en résulte, La loi du 13 mars 2000 résulte en fait de l'apposition de deux démarches distinctes (et, jusqu'à tout récemment, indépendantes) : d'une part, la réflexion de la communauté juridique française sur la notion d'*écrit électronique*; d'autre part, la définition mathématique d'un *modèle de la signature électronique* basée sur les technologies de la cryptographie, circulant à travers des instances réglementaires internationales (CNUDCI, OCDE, etc.) et introduit dans le droit français par le biais de la Directive Européenne de 1999. Une telle analyse ne permettra pas d'affubler la réforme de 2000 d'une cohérence qu'elle n'a de toute façon jamais possédée. Elle permettra par contre d'en dégager les logiques constitutives et de les contraster avec d'autres, possiblement plus pertinentes, issues de la confrontation de la science archivistique avec le problème de la préservation durable des écrits électroniques.

Cet article commence par décrire (II) l'état du droit de la preuve à la suite de la réforme de 1980; (III) le parcours du concept de l'écrit électronique tel qu'articulé par les juristes français; (IV) le parcours du modèle de la signature électronique tel qu'articulé par les cryptologues et présente (V) une réflexion indépendante sur le concept d'*écrit électronique authentique* menée par la communauté archivistique, pour conclure (VI) sur un certain nombre de principes à même de guider la transition du droit de la preuve français vers l'univers de l'écrit « dématérialisé » sans qu'il en soit lui-même dénaturé.

II — La réforme de 1980

La confrontation du droit de la preuve français aux nouvelles manifestations de l'écrit a débuté avec la réforme de 1980,⁶ occasion d'un examen du problème de la reconnaissance de la valeur probante d'écrits transmis à distance (télécopie), démultipliés (photocopie) et archivés sur support photographique (microfilm). Il faut souligner que ces nouvelles formes d'écrits posent à l'analyse doctrinale les mêmes défis conceptuels que ceux associés aux NTIC. Cependant, ils ne s'inscrivent pas dans une mouvance sociale comparable à celle si puissamment symbolisée aujourd'hui par l'Internet, et le législateur pourra se contenter de les soumettre à de simples régimes d'exceptions à l'exigence d'un écrit papier. En effet, les règles des articles 1341 et suivants, exigeant la constitution d'un écrit signé et sa primauté sur la preuve testimoniale,

« reçoivent ... exception lorsqu'une partie ou le dépositaire n'a pas conservé le titre original et présente une copie qui en est la reproduction non seulement fidèle mais aussi durable. Est réputée du-

⁶ Voir Michel Vion, "Les modifications apportées au droit de la preuve par la loi du 12 juillet 1980," *Desfrenois* (1980).

rable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support. »⁷

Bien que la valeur probante de telles reproductions ne soient pas précisée, celles-ci se voient accorder, en pratique du moins, la valeur d'original, puisque « la reproduction constitue un indice sérieux de l'existence antérieure du titre invoqué. »⁸ Si les objectifs pratiques de la réforme — au premier chef, apporter une solution aux problèmes d'archivage de plus en plus importants du secteur bancaire et des assurances — purent être atteints sans exiger une confrontation plus frontale de la doctrine aux nouvelles manifestations de l'écrit, une telle dérobade ne pouvait durer longtemps. Tout au cours des années 1980, des appels répétés se feront entendre pour que le droit positif prenne la pleine mesure des transformations induites par les déploiements des technologies de l'information et de la communication en un tissu pénétrant toujours plus profondément la vie quotidienne des citoyens. En 1988, dans une analyse pénétrante, le professeur Jacques Larrieu exposa les grands principes qui, selon lui, seraient à même de permettre une transition harmonieuse à un univers de transactions électroniques.⁹

Larrieu suggère que les deux principaux arguments contre l'admissibilité des documents électroniques — l'éphéméralité du média électronique et la difficulté d'assimiler un code électronique à la signature manuscrite — sont, en fait, sans fondements, puisque

« la loi ne fait pas entièrement dépendre la crédibilité d'un mode de preuve de ses qualités intrinsèques. La primauté de l'écrit ne repose pas, contrairement à ce qui est affirmé parfois, sur ses seules qualités techniques¹⁰. »

Suivant en cela l'analyse socio-historique de Levy-Bruhl¹¹, Larrieu propose que la prééminence de l'écrit dans le droit de la preuve français n'est aucunement dû à ses qualités matérielles (en tant que support infalsifiable), mais n'est plutôt explicable que par son important capital symbolique, lui-même dû à sa longue présence historique dans la société française et la protection étendue que le législateur lui accorde.

Larrieu suggère plutôt que la valeur probante d'un document est facteur de trois conditions : (a) les qualités de son auteur (par exemple, sa qualité d'officier public); (b) la procédure réglementant sa production et sa conservation; et (c) la sévérité de la punition qui menace celui qui le manipule incorrectement, soit intentionnellement, soit par acci-

⁷ CC. art. 1348.

⁸ Vion, op. cit., 1334.

⁹ Jacques Larrieu, "Les nouveaux moyens de preuve: pour ou contre l'identification des documents informatiques à des écrits sous seings privés?," *Lamy droit de l'informatique* H, I (1988).

¹⁰ Ibid., p. 10.

¹¹ Henri Lévy-Bruhl, *La preuve judiciaire — Etude de sociologie juridique* (Paris: Librairie Marcel-Rivière et Cie, 1964), une analyse qui a aussi fortement inspirée celle de Xavier Lagarde — Xavier Lagarde, *Réflexion critique sur le droit de la preuve*, ed. Jacques Ghestin, *Bibliothèque de droit privé* (Paris: Librairie générale de droit et de jurisprudence, 1994) et Xavier Lagarde, "Vérité et légitimité dans le droit de la preuve," *Droits*, no. 23 (1996)..

dent. Larrieu en déduit que les documents électroniques verraient leur valeur symbolique similairement rehaussée s'ils devaient se voir accorder une force probatoire égale à celle des écrits sur support papier. Quels sont les obstacles se posant, en l'état du droit positif et de la jurisprudence de 1988, à une telle reconnaissance? La conclusion de Larrieu pourra surprendre. Il propose que, d'une part,

« ... aucune des deux composantes de l'élément matériel de l'écriture (caractères d'une part, procédé et support d'écriture d'autre part) n'est définie en droit positif d'une manière qui justifierait l'exclusion des procédés modernes d'écriture et des supports nouveaux d'information. ... Sous le rapport de la logique, n'importe quel type de caractère ayant un sens, inscrit sur n'importe quel support, peut constituer une écriture du moment que les fonctions de l'écrit instrumentaire sont assurées : mémorisation de l'expression d'une volonté, c'est-à-dire préconstitution de la preuve, et fiabilité, c'est-à-dire résistance à la falsification. L'enregistrement sur une bande magnétique, une disquette, un microfilm, un disque CD-ROM, l'impression d'un film peuvent remplir cet office du moment qu'ils ne sont pas trop éphémères. »¹²

et que, d'autre part,

« ... n'importe quel type de signe suffisamment distinctif peut constituer une signature s'il remplit cette double fonction d'approbation et d'identification qui est traditionnellement dévolue à la signature. Une signature électronique peut jouer ce double rôle. »¹³

Il n'y a donc, selon Larrieu, aucun obstacle, ni juridique, ni intellectuel, à la reconnaissance de ces nouveaux moyens de preuve par le droit français. Plus encore, une intervention législative serait non seulement injustifiée d'un point de vue strictement juridique, mais elle ne suffirait pas, à elle seule, à « revêtir ces techniques modernes de l' "homologation sociale" qui, seule, fonde la confiance dans un moyen de preuve. »¹⁴ En effet, selon Larrieu, le pouvoir de la preuve émane ultimement du tissu de conventions sociales sur laquelle cette preuve repose :

« Quelle que soit l'autorité reconnue au sous-seing privé et plus spécialement à la signature, cette autorité n'est ni naturelle, ni rationnelle. Elle relève d'une convention sociale apparue à partir du XVI^e siècle. ... C'est d'une nouvelle convention sociale que dépend la force probante des nouvelles techniques de mémorisation et d'authenticité des données. »¹⁵

Ainsi, si le droit ne fait pas obstacle, il n'est pas non plus particulièrement en mesure d'agir comme moteur de cette nouvelle convention. Dans l'analyse de Larrieu, ni obstacle, ni moteur, le rôle du droit doit se résumer à celui d'une *escorte attentive*.

III — Vers l'acte sous seing privé électronique

En dépit de la lucidité de l'analyse de Larrieu, les appels à une intervention législative se feront entendre de façon répétée au cours des années 1990, et le Ministère de la justice

¹² Larrieu, 15, 30.

¹³ Ibid, p. 30.

¹⁴ Ibid., p. 10.

¹⁵ Ibid., p. 34.

constituera en 1996 un groupe de travail, formé d'universitaires éminents.¹⁶ Le groupe avec pour mission de prendre la pleine mesure des nouvelles manifestations de l'écrit et de suggérer les paramètres d'une éventuelle réforme du droit de la preuve.

Le rapport du groupe, remis au Ministère en 1997, forma, en octobre 1998, la matière d'un avant-projet de loi « *relatif à l'adaptation du droit de la preuve aux nouvelles technologies* » puis d'un projet de loi¹⁷ déposé au Sénat en septembre 1999 et adopté à l'unanimité par l'Assemblée nationale le 29 février 2000. Bien des différences substantielles existent entre les propositions des universitaires et le texte de la loi telle qu'elle fut adoptée, la notion la plus fondamentale de la réforme, celle de distinguer l'écrit de son support, est demeurée intacte au fil des réécritures.¹⁸

Quatre articles définissent à présent le cadre juridique de l'écrit électronique : tout d'abord, une définition de l'écrit où celui-ci est distingué de son support matériel¹⁹:

« 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 leurs modalités de transmission. » (CC. Art. 1316)

ensuite, une définition des règles selon lesquelles un écrit électronique peut être admis à titre de preuve:

« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifié la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. » (CC. Art. 1316-1)

Troisièmement, des règles enjoignant à un juge la manière de trancher en cas de conflit entre des écrits sur différents supports :

¹⁶ Les membres de ce groupe : Pierre Catala, Pierre-Yves Gautier, Jérôme Huet, Isabelle de Lamberterie, Xavier Linant de Bellefonds, André Lucas, Lucas de Leyssac, et Michel Vivant.

¹⁷ Voir Pierre Catala et al., "L'introduction de la preuve électronique dans le Code civil," *La Semaine Juridique Édition Générale* 47 (1999), pour une description et critique des différences entre l'avant-projet et le projet de loi.

¹⁸ Voir Isabelle de Lamberterie, "L'écrit dans la société de l'information," in *Mélanges en l'honneur de Denis Tallon -- D'ici, d'ailleurs: Harmonisation et dynamique du droit*, ed. Camille Jauffret-Spinosi & Isabelle de Lamberterie (Paris: Société de législation comparée, 1999), Isabelle de Lamberterie, "Preuve et Signature: Les innovations du droit français," *Cahiers Lamy droit de l'informatique et des réseaux* K, no. 123 (2000).

¹⁹ On doit déplorer que le concept de *dématérialisation* semble devoir découler de cette distinction. Loin d'être dématérialisé, jamais l'existence même de l'écrit n'a tant dépendu de son support matériel — logiciels, équipements informatiques, etc. Comme David Levy le note, « Digital documents are not immaterial. The marks produced on screens and on paper, the sounds generated in the airwaves, are as material as anything in our world. And the ones and zeros of our digital representations are equally material: they are embedded in material substrate no less than are calligraphic letterforms on a piece of vellum. It may be true that digital representations can move around extremely quickly, that they can be copied from one storage device to another, even when they are separated by thousands of miles. But at any one moment, the bits for a particular document are somewhere real and physical. » David Levy, *Scrolling Forward: Making Sense of Documents in The Digital Age* (New York: Arcade Publishing, 2001), p. 155-6.

« 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. » (CC. Art. 1316-2)

Finalement, une fois dûment qualifié, admis, et les conflits potentiels écartés, l'écrit sur support électronique se voit doter d'une force probante :

« L'écrit sur support électronique a la même force probante que l'écrit sur support papier. » (CC. Art. 1316-3)

Bien sûr, pour que ces règles puissent constituer un cadre cohérent et complet à même de pouvoir tenir compte de l'ensemble des règles relatives aux actes sous seing privé, il manque l'élément essentiel de la signature. Bien que le rapport original des universitaires ne discute pas du problème d'une signature adaptée au contexte de l'écrit électronique, une définition de celle-ci fait son apparition dans l'avant-projet de loi. Tout comme celle de l'écrit électronique, celle-ci émerge largement intacte du processus de réécriture du texte de loi. La définition reprend d'une part les fonctions génériques de la signature déjà identifiées par Larrieu — identification et manifestation de la volonté de consentir à des obligations :

« 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. » (CC. Art. 1316-4)

D'autre part, elle propose une définition d'un objet informatique à même de rencontrer les fonctions attendues d'une signature électronique: celle-ci doit pouvoir *identifier* le signataire; elle doit pouvoir être, d'une façon ou d'une autre, *liée* à l'acte auquel elle se rapporte; et ces fonctions doivent être assurées par le procédé de signature d'une façon *fiable* :

« 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. ... » (CC. Art. 1316-4)

La deuxième partie du second alinéa de l'article 1316-4 introduit un mécanisme qui permette de spécifier les conditions selon lesquelles un tel procédé sera non seulement considéré, mais de plus, *présumé, fiable* :

« La fiabilité de ce procédé est présumée, jusqu'à preuve du contraire, lorsque la signature est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'état. » (CC. Art. 1316-4)

Cette clause ne figure pas dans l'avant-projet de loi et rendre compte des logiques qui déterminent son apparition exige un travail de remise en contexte considérable, contexte qui trouve son origine dans la contre-culture américaine des années 1970.

IV — Définition techno-juridique de la signature électronique

En 1976, deux chercheurs de l'Université de Stanford, Whitfield Diffie and Martin Hellman, publiait un article qui allait révolutionner une branche des mathématiques dont la

pratique était, jusqu'à ce jour, réservée à un cercle restreint d'initiés, la cryptographie.²⁰ Cette science, que Ronald Rivest définit comme celle de « la communication en présence d'adversaires »²¹, a historiquement eu pour principale fonction de fournir aux Etats des moyens d'assurer la confidentialité des communications militaires ou diplomatiques. Ces moyens étaient, jusqu'en 1976, fondés sur un paradigme où l'émetteur et le récepteur d'une communication chiffrée se devaient de disposer d'une information commune, une *clé secrète* et où les problèmes relatifs au déploiement et à la mise en œuvre de systèmes de communication chiffrées se résument le plus souvent aux procédures d'échange de ces clés. Dans leur article, Diffie et Hellman proposaient un mécanisme mathématique inédit permettant à deux individus d'échanger des données chiffrées, avec la propriété étonnante qu'*il ne nécessite pas de s'entendre au préalable sur une clé secrète commune*.

Le mécanisme de *cryptographie à clé publique* proposé par Diffie et Hellman est fondé sur la séparation de la clé unique en deux clés distinctes, une clé *publique* pour le chiffrement et une clé *privée* pour le déchiffrement. La clé publique est rendue disponible aux autres utilisateurs par le biais d'un annuaire, alors que l'accès à la clé privée doit être limité à son seul propriétaire. Pour chiffrer un document, l'émetteur se procure la clé publique du destinataire et l'utilise pour chiffrer le document. Etant donné la relation mathématique qui unit les deux clés, seule la clé privée correspondante à la clé publique utilisée pour le chiffrement sera en mesure de déchiffrer et rendre intelligible le message. Tout l'intérêt de ce mécanisme repose dans le fait que même si la clé publique est une donnée connue de tous, il est « impossible » d'en déduire la clé privée correspondante.²²

Au-delà de ses applications au chiffrement des données, Diffie et Hellman suggèrent que leur mécanisme offre la possibilité de réaliser un « équivalent numérique » à la signature manuscrite, par simple inversion des clés : l'émetteur utilise sa clé privée pour chiffrer (« signer ») le message; de son côté, le récipiendaire se procure la clé publique de l'émetteur et l'utilise pour déchiffrer (« vérifier la signature ») le message. Un tel mécanisme offre alors les garanties suivantes : d'une part, le message ainsi « signé » l'a bel et bien été par la clé privée correspondant à la clé publique utilisée pour la vérification; d'autre part, le message n'a pu être modifié après la « signature », sinon la vérification aurait échoué. En pratique, les technologies de signature cryptographique nécessitent le déploiement d'infrastructures de gestion de clés (IGC) qui permettent entre autres de

²⁰ Wittfield Diffie and Martin E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory* 22 (1976). Pour une histoire de la cryptographie en général, voir David Kahn, *The Codebreakers. The Story of Secret Writing* (New York: Macmillan, 1967) ; pour une histoire de la cryptographie contemporaine, voir Steven Levy, *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age* (New York: Viking Books, 2000) ; Simon Singh, *The Code Book – The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (London: Fourth Estate Limited, 1999) ; Pour une introduction à la cryptographie contemporaine, voir Jacques Stern, *La Science du secret* (Paris: Editions Odile Jacob, 1998) ; pour un exposé vulgarisé des problèmes de la sécurité électronique, voir Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (New York: John Wiley and Sons, Inc, 2000).

²¹ Ronald L. Rivest, "Cryptography," in *Handbook of Theoretical Computer Science (Volume A: Algorithms and Complexity)*, ed. Jan van Leeuwen (Cambridge, Mass.: Elsevier and MIT Press, 1990), p. 6.

²² Cette impossibilité s'entend dans le contexte de la théorie de la complexité calculatoire, c'est-à-dire qu'on ne dispose pas d'algorithmes permettant d'accéder à la solution en un temps raisonnable.

distribuer les clés publiques sous forme de « certificats à clés publiques » garantissant l'identité du propriétaire de la clé privée associée.²³

L'invention de la cryptographie à clé publique a marqué un point tournant dans l'évolution de la discipline et donné lieu à un essor scientifique remarquable. Les conséquences pratiques de cette révolution sont nettement moins définies, et la cryptographie à clé publique sera, pendant les années 80 du moins, caractérisée comme « une solution à la recherche d'un problème ».²⁴ C'est l'explosion des technologies de l'Internet qui fournira, au milieu des années 1990, ce problème, la sécurisation du commerce électronique. La signature électronique, telle que modélisée par Diffie et Hellman va alors soudainement se retrouver au cœur d'une série d'initiatives internationales visant à définir un cadre juridique pour les transactions électroniques voie royale vers l'avènement supputée d'une société de l'information, où tant les relations commerciales que les relations entre l'Etat et le citoyen sont conduites par l'entremise de réseaux électroniques. Parmi les nombreux textes résultant de ces initiatives, il faut citer les *Digital Signature Guidelines* de l'American Bar Association,²⁵ les *Cryptography Guidelines* de l'OCDE²⁶, et la *Loi type sur le commerce électronique* de la CNUDCI²⁷.

Le texte législatif le plus important à contribuer à la définition du régime probatoire de la signature électronique est sans nul doute la Directive Européenne du 13 décembre 1999 « sur un cadre communautaire pour les signatures électroniques ». La Directive définit deux types de signature électroniques, et mande les Etats Membres de leur accorder une force probante distincte. La « signature électronique » y est définie 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)

²³ Pour plus de détails sur la signature cryptographique, voir Jean-François Blanchette, « Les Technologies de l'écrit électronique: Synthèse et évaluation critique, » in *Les actes authentiques électroniques. Réflexion juridique prospective*, ed. Isabelle de Lamberterie (Paris: La Documentation Française, 2001).

²⁴ Selon l'expression de Jim Bidos, ancien vice-président de RSA Security, lors d'une présentation à la conférence « Doing Business Securely on the Information Highway », Montréal, 30-31 août 1995.

²⁵ Les *Digital Signature Guideline* (ABA, 1996) définissent la signature électronique comme celle découlant des technologies de cryptographie à clé publique à l'exclusion de tout autre approche. Elles ont influencé un certain nombre de textes législatifs relatifs à la signature électronique, notamment ceux de l'Utah — voir Bradford C. Biddle, « Misplaced Priorities : The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure » *San Diego Law Review* 33 :1143-1193 (1996).

²⁶ Les *Cryptography Guidelines* de l'OCDE recommandent aux Etats Membres de distinguer entre l'utilisation de la cryptographie à des fins de chiffrement et son utilisation à des fins d'authentification des données, de façon à pouvoir dégager les technologies cryptographiques des réglementations qui en contraignent le commerce pour des raisons de sécurité nationale. Suite à ces recommandations, la France a considérablement relaxé son contrôle des technologies cryptographiques en 1999 — voir David Sobel, *Cryptography and Liberty 2000 : An International Survey of Encryption Policy*, EPIC 2000.

²⁷ La *Loi type de la CNUDCI sur le commerce électronique* (1996) énonce un certain nombre de principes aptes à faciliter la reconnaissance juridique des écrits électroniques, entre autres, la définition fonctionnelle de la signature (identification du signataire et consentement aux obligations contenues dans l'acte) et le principe de non-discrimination (un document électronique ne peut être écarté sous seul motif qu'il est sous forme électronique).

alors qu'une « signature électronique avancée » est définie comme

« une signature électronique qui satisfait aux exigences suivantes : (1) être liée uniquement au signataire; (2) permettre d'identifier le signataire; (3) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif; (4) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable; » (art. 2.2)

Malgré les aspirations de la Directive à une certaine « neutralité technologique »²⁸ cette définition décrit, sans la nommer, la signature cryptographique. En effet, on constate que la quatrième exigence énonce précisément cette caractéristique propre à la signature cryptographique de signaler si le message signé a subi une quelconque modification après la signature.

À ces deux types de signatures électroniques correspondent deux régimes d'admissibilité et de force probante. D'une part, dans le cas d'une signature électronique « simple », la Directive exige que les Etats Membres se conforment au principe de « non-discrimination » énoncé par la CNUDCI,²⁹ c'est-à-dire que ceux-ci

« ... 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; ... »³⁰

D'autre part, les signatures électroniques « avancées » sont non seulement recevables, mais les Etats membres doivent amender leurs droits nationaux respectifs de façon à ce que ces signatures

« répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier. »³¹

Ainsi, la Directive européenne impose aux Etats membres un régime probatoire où les signatures électroniques fondées sur les technologies de cryptographie à clé publique se voient accorder un régime préférentiel — valeur probante équivalente à celle d'une signature manuscrite — tout en leur aménageant une certaine marge de manœuvre, sous la forme d'une définition de signature électronique « simple », à la force probante indéterminée.

La jonction entre les exigences de la Directive et le processus de réforme du droit de la preuve amorcé au sein du système juridique français allait s'effectuer au sein d'un

²⁸ Par exemple, réctal 8 : « eu égard à la rapidité des progrès techniques et à la dimension mondiale d'Internet, il convient d'adopter une approche qui prenne en compte les diverses technologies et services permettant d'authentifier des données par la voie électronique. »

²⁹ CNUDCI, article 5 : « L'effet juridique, la validité ou la force exécutoire d'une information ne sont pas déniés au seul motif que cette information est sous forme d'un message de données. »

³⁰ Directive op. cit., art. 5.2.

³¹ Ibid., article 5.1.

groupe de travail constitué par le Conseil d'état à la requête du Premier Ministre, et chargé « d'analyser les questions juridiques liées au développement d'Internet et de mettre en lumière les adaptations nécessaires de notre droit. »³² Le groupe de travail allait énoncer un parti pris clair pour les technologies de signature basées sur la cryptographie, supputant son hégémonie prochaine :

« En pratique, les signatures électroniques sont aujourd'hui rendues fiables par un recours à des techniques cryptographiques similaires à celles utilisées pour le chiffrement. Parmi celles-ci, le procédé dit de la 'signature numérique à clé publique' est sans doute le mieux adapté à la signature de messages électronique et tout laisse penser que son usage devrait rapidement se généraliser au niveau mondial. »³³

Cette future généralisation, ainsi que le désir d'établir des conditions favorables à la naissance d'une industrie de services de certification de clés publiques,³⁴ va pousser le Conseil d'État à accorder à la signature électronique sécurisée une présomption simple de fiabilité, bouleversant ainsi le mécanisme de la charge de la preuve qui prévalait jusqu'alors pour les actes sous seings privés.³⁵ C'est ainsi qu'à la suite de la définition originale de la signature, telle que proposée dans l'avant-projet, apparaît dans le texte final la clause stipulant que

« la fiabilité de ce procédé est présumée, jusqu'à preuve du contraire, lorsque la signature est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'état »

Fameux décret, publié au Journal Officiel le 31 mars 2001,³⁶ dont l'architecture échevelée met à mal un droit de la preuve aux lignes élégantes et patinées par le temps.³⁷ Il a pour fonction de définir les caractéristiques techniques des procédés de signature électroni-

³² Conseil d'état, *Internet et les réseaux numériques*, p. 6.

³³ Ibid, p. 54. Ce parti pris semble fondé en parti sur un malentendu, puisque le groupe de travail semble imputer au processus de certification la capacité d'assurer la conservation de l'écrit électronique : « Ainsi, 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**. » (ibid. p. 56). Or, la certification, telle qu'on l'entend dans l'univers de la signature numérique et dans les décrets pris à cet effet, n'a rien à voir avec la conservation durable des écrits, mais à plutôt comme seul et unique objet d'assurer le lien entre l'identité du signataire et sa clé publique.

³⁴ Espoirs malheureusement non-avérés — voir Hervé Morin, « Pourquoi la signature électronique reste lettre morte », *Le Monde* 22 juin 2003.

³⁵ « La question du risque de la preuve qui détermine la perte du procès lorsque le juge se heurte à un doute irréductible, pour se poser rarement, n'en est pas moins déterminante de l'équilibre de toute règle de droit. En matière d'électronique, d'informatique, ou plus largement, de technologie avancée, la question prend une dimension emblématique parce qu'elle touche à celle de savoir qui supporte le risque de l'incertitude scientifique. » Jean Devèze, « Vive l'article 1322 ! Commentaire critique de l'article 1316-4 du Code civil » in *Le Droit Privé Français à la fin du XXIème Siècle. Études Offertes à Pierre Catala* (Litec, Paris : 2001).

³⁶ Décret no. 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil relatif à la signature électronique, *JO* (2001).

³⁷ De Lamberterie, I. et Blanchette, J.-F. (2001), « Le décret du 30 mars relatif à la signature électronique: Lecture critique, technique et juridique », *La Semaine Juridique --- Entreprises et affaires*, no. 30.

que susceptible de bénéficier de la présomption de fiabilité énoncée à l'article 1316-4. Après avoir défini, dans l'esprit de la Directive, deux types de signatures électronique — simple³⁸ et sécurisée³⁹ — le décret résume la complexité technique des signatures électroniques et des IGC en une seule présomption de fiabilité:

« La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve du contraire lorsque ce procédé met en oeuvre 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. »⁴⁰

La réforme de 2000 articule ainsi une double caractérisation du concept d'intégrité de l'écrit électronique. D'une part, cette intégrité est assurée par le recours à la signature « sécurisée » puisque celle-ci est « liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable ». D'autre part, les conditions de conservation déterminent l'intégrité de l'écrit et, par conséquent, son admissibilité (art. 1316-1).

La première caractérisation est celle communément adoptée par les cryptologues, c'est-à-dire que l'intégrité est définie comme « la propriété selon laquelle des données n'ont pas été altérées [par l'insertion, suppression, substitution de bits] d'une façon non autorisée depuis le moment où ces données ont été créées, transmises, ou entreposées par une source autorisée. »⁴¹ Ainsi définie au niveau de l'encodage binaire des données, l'intégrité est susceptible d'être quantifiée avec précision.

La seconde caractérisation fait référence à un ensemble de « conditions » de nature à garantir l'intégrité de l'écrit électronique. La loi n'explicite ni la notion d'intégrité utilisée ici, ni la relation entre ces « conditions » et l'utilisation de la signature électronique sécurisée du décret. Un éclairage supplémentaire est cependant apporté par une autre communauté professionnelle de la preuve documentaire, celle des archivistes, qui a exploré à fond la tension entre ces deux caractérisations de l'authenticité.

V — Les archivistes

Si la communauté scientifique a proposé que la signature cryptographique offre l'équivalent électronique de la signature manuscrite, si la communauté juridique lui a accordé un accueil chaleureux en définissant un cadre où, sous certaines conditions, elle acquiert une force probante équivalente à la signature manuscrite, la communauté archivistique n'a offert qu'un accueil réservé aux technologies de signature cryptographique. Cette réserve n'est pas simplement issue d'un atavisme professionnel mal placé,

³⁸ « Signature électronique': une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase de l'article 1316-4 ; »

³⁹ « 'Signature électronique sécurisée' : une signature électronique qui satisfait, en outre aux exigences suivantes: (1) être propre au signataire; (2) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif; (3) garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable ; »

⁴⁰ Décret, op. cit, art. 2.

⁴¹ Menezes, van Oorschot & Vanstone, *Handbook of Applied Cryptography* (CRC Press, 1996) p. 361.

mais plutôt d'une analyse cohérente des implications des technologies de l'information pour la conservation sur le long terme de documents électroniques authentiques.

La communauté archivistique a en effet déjà effectué un certain nombre de constats relatifs à la préservation de documents électroniques authentiques, notamment à travers les travaux du projet InterPARES, dont la première phase a eu lieu de 1998 à 2001.⁴² Ce projet a dégagé un ensemble de principes propres à sous-tendre toute politique, stratégie, ou norme de préservation de documents d'archive qui doit assurer les qualités d'authenticité des documents sur le long-terme.⁴³ Nous discutons ici trois de ces principes particulièrement pertinents à notre propos : (a) la relation entre intégrité physique et authenticité d'un document électronique, (b) la distinction entre « authenticité » et « *authentication* », et (c) la notion de cycle de vie du document.

(a) Intégrité physique

Dans l'univers du document papier, l'archivistique traditionnelle peut (en partie du moins) inférer l'authenticité d'un document à partir de l'intégrité de son support physique. Dans l'univers du document électronique, où le support physique d'un document correspond à son encodage binaire enregistré sur un support magnétique ou optique, ce repère disparaît, pour deux raisons :

- D'une part, cet encodage binaire n'entretient aucune relation particulière avec son support physique, qu'il soit optique, magnétique, ou électronique, pouvant être recopié à l'infini sans souffrir de dégradation ;
- D'autre part, la chaîne de bits qui forme cet encodage⁴⁴ est susceptible d'être modifié, au fil des migrations nécessaires pour préserver l'intelligibilité du document.⁴⁵

Or, si ces manipulations ont pour effet irrémédiable de modifier la chaîne de bits sous-tendant au document, elles n'ont pas nécessairement pour conséquence d'infirmen son authenticité : il faut plutôt pouvoir élaborer les critères permettant d'indiquer quelles manipulations sont compatibles avec la mission de l'archiviste. En contrepartie, il est absolument certain qu'un document dont on a scrupuleusement préservé l'intégrité physique, mais qui soit devenu illisible ne peut être qualifié d'authentique au sens archivistique du terme ! C'est ainsi que les chercheurs d'InterPARES en arrivent à la conclusion qu'

⁴² Le projet InterPARES vise à déterminer des principes archivistiques pertinents à la conservation de documents électroniques authentiques. Il regroupe des représentants de nombreuses archives nationales, incluant la Direction des archives de France. Voir Duranti, L. (1998). *Diplomatics : New uses for an old science*. Lanham, Md., Scarecrow Press et le site <http://www.interpares.org>.

⁴³ InterPARES

⁴⁴ En anglais, *bitstring*.

⁴⁵ Voir Ken Thibodeau « Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years », in *The State of Digital Preservation: An International Perspective* (Washington D.C. : Council on Library and Information Resources, 2002).

« il n'est pas possible de préserver un écrit électronique en tant qu'*objet physique entreposé*; il est uniquement possible de préserver *les moyens de rendre ce document manifeste*. »⁴⁶

Un certain nombre de conséquences importantes découlent de ce constat, non parmi les moindres, que l'exigence de préserver la signature cryptographique à des fins de preuve impose à l'archiviste un dilemme insoluble, entre préserver l'intégrité physique du document électronique signé, et préserver son intelligibilité! C'est ainsi que plusieurs archives nationales ont annoncé qu'elles n'avaient aucune intention de préserver les signatures attachées aux écrits électroniques sous leur responsabilité.⁴⁷

(b) Authenticité et « authentication »

Du point de vue de la communauté archivistique, la signature électronique fournit un service d'« *authentication* »⁴⁸ et non pas une mesure d'*authenticité*. En archivistique, l'*authentication* d'un document consiste en une attestation de son authenticité à un moment spécifique.⁴⁹ Dans l'univers électronique, cette attestation est généralement effectuée après une transmission du document dans l'espace. Cette attestation n'est équivalente ni à l'authenticité des archivistes (une qualité conférée à un document selon le mode, la forme et l'état de sa transmission et préservation dans l'espace et le temps),⁵⁰ ni au concept d'authenticité du droit civil, (la force probante résultant de l'exécution de certains formalismes par un officier public).⁵¹ Du point de vue des archivistes, la signature numérique ne constitue donc qu'un seul des éléments susceptibles de permettre d'inférer la force probante d'un écrit archivé.⁵²

⁴⁶ Voir Duranti et al., « Strategy Task Force Report », in *The Long-Term Preservation of Authentic Electronic Records : Findings of the InterPARES project*, p. 4.

⁴⁷ Voir à ce sujet mon rapport à la Direction des archives de France : *La conservation de la signature électronique : Perspectives archivistiques*, disponible à <http://www.archivesdefrance.culture.gouv.fr/fr/quoideneuf/index.html>.

⁴⁸ Il n'existe pas de traduction française satisfaisante du terme anglais « *authentication* ». En informatique, il se définit comme « le procédé matériel ou électronique visant à établir de façon formelle et intangible l'identification des parties à un échange ou une transaction électronique », de Lamberterie, *op. cit.*, p. 36.

⁴⁹ « In common usage, authentication is understood as a declaration of a record's authenticity at a specific point in time by a juridical person entrusted with the authority to make such a declaration. It takes the form of an authoritative statement (which may be in the form of words or symbols) that is added to or inserted in the record attesting that the record is authentic », MacNeil et al. (2002), « Authenticity Task Force Report », in *The Long-Term Preservation of Authentic Electronic Records : Findings of the InterPARES project*, p. 2.

⁵⁰ Voir Luciana Duranti et al., *Preservation of the Integrity of Electronic Records* (Dordrecht : Kluwer Academic Publishers, 2002), p. 110.

⁵¹ Jacques Flour, « Sur une notion nouvelle d'authenticité (Commentaire des articles 11 et 12 du décret no. 71-041 du 26 novembre 1971) (a) », *Desfrenois* 92: 977-1017 (1992).

⁵² « Digital signatures are an example of an authentication technology that has been developed to address the need for secure electronic communication across open networks such as the Internet. Digital signatures, which identify the sender of a data object and verify that it has not been altered in transmission, can support the authentication of electronic records, but they are not sufficient to establish the identity and demonstrate the integrity of an electronic record over the long term. » MacNeil, *op. cit.*, p. 2.

(c) La chaîne de préservation

L' *authentication* qui résulte de la validation d'une signature numérique n'est effectuée qu'à un moment précis de la vie du document. Les archivistes infèrent l'authenticité d'un écrit en se fondant sur le principe du respect de la « chaîne de préservation », c'est-à-dire, l'ensemble des contrôles et des procédures qui assurent l'identité et l'intégrité d'un document au travers la totalité de son cycle de vie. Alors que la Directive européenne (et le droit français qui en découle) confère à la validation de la signature une valeur prépondérante, presque exclusive, au sein de cette chaîne, les archivistes ne la considèrent que comme un maillon parmi d'autres de cette chaîne. Ainsi, le projet InterPARES offre-t-il deux ensembles de critères pour évaluer l'authenticité des documents électroniques, le premier à être utilisé pour jauger la capacité d'un système d'information à produire des documents d'archives authentiques, le second pour la production de copies conformes de documents d'archives, critères fondés sur la *documentation de l'ensemble du processus de préservation*.⁵³

VI – Conclusion

La formulation des exigences que doit rencontrer un écrit électronique pour préserver sa valeur probante est un des problèmes les plus importants à l'agenda de la communauté des professionnels de la preuve documentaire. En France, ces exigences ont été principalement formalisées par les juristes, de concert avec les spécialistes en informatique et sont articulées, comme nous l'avons décrit, autour des qualités des technologies de signatures cryptographiques, telles qu'entérinées par la loi du 13 mars 2000 et ses décrets d'application. Ce parti pris technologique s'explique en parti par l'engouement initial suscité par la signature cryptographique, un engouement qui en a entraîné plusieurs à vanter sa supériorité intrinsèque par rapport à l'écrit papier et la signature manuscrite.⁵⁴

On peut utilement évoquer une logique similaire à l'œuvre dans le contexte du droit criminel de la preuve. Alors que le profil ADN se voyait initialement dotée d'un statut de preuve d'identification irréfutable, « une signature — un autographe — qui l'emporte en crédibilité sur tout autre déclaration », elle connaîtra pourtant un échec retentissant au cours du célèbre procès d'O. J. Simpson en 1995. Comme le suggère une analyse issue de la sociologie des sciences,

« ... en suivant les échantillons de la scène du crime au laboratoire, puis du laboratoire au tribunal, on s'aperçoit que l'empreinte génétique joue le rôle d'un témoin compétent *si et seulement si* la succession des transactions au cours du prélèvement du transport, de la conservation, de la numérisation et de l'analyse de l'échantillon est attestée par des témoins, certifiée et dûment enregistrée par

⁵³ MacNeil, *ibid.*

⁵⁴ C'est ainsi que les auteurs d'un ouvrage de référence sur le commerce électronique expliquent que « Throughout history, lawmakers of both civil and commonlaw jurisdictions have sought rules that achieve the type and level of non-repudiation made possible by digital technology. Signatures, seals, notaries, recording offices, and certified mail are all examples of traditional mechanisms employed in efforts to supply and bolster non-repudiation. ... Explicit consciousness of this powerful issue has surfaced only very recently, as society has faced the challenge of first matching and then exceeding traditional legal protections in the emerging digital communications environment. » Warwick Ford & Michael Baum, *Secure Electronic Commerce : Building the Infrastructure for Digital Signatures and Encryption* (Prentice-Hall 2000), p. 564.

des fonctionnaires responsables. Pour être considérée comme telle, la vérité contenue dans la signature automatique (le code-barre génétique) se doit donc d'être accompagnée, entourée, par toute une série de traces bureaucratiques: signatures manuscrites sur des formulaires standards, véritables codes-barres collés sur les sacs contenant les échantillons, etc. »⁵⁵

Il en est de même pour l'écrit électronique : il ne peut être « témoin compétent » d'un fait juridique qui si toute une série de traces bureaucratiques l'accompagnent, traces qui documentent l'ensemble des opérations qu'un écrit est susceptible de subir — création, modifications, annotations, signature, sauvegarde, conversion, etc. Pour qu'elles soient crédibles, ces opérations se doivent d'être effectuées par des systèmes de traitement de l'information jugés fiables, c'est-à-dire conformes aux critères de la communauté archivistique pour la création, la gestion et la conservation des écrits électroniques.⁵⁶

Cet article a délibérément ignoré l'autre élément principal de la réforme de 2000 du droit de la preuve, l'introduction des actes authentiques électroniques, dont la loi se contente d'énoncer le principe et renvoie la définition des conditions matérielles à un décret d'application.⁵⁷ Quatre années et deux groupes de travail plus tard, le décret n'est toujours pas rédigé, son élaboration achoppant principalement sur les problèmes évoqués dans cet article, notamment celui de la conservation sur le long terme des documents électroniques signés. C'est que la volonté de préparer au 21^{ème} siècle une des institutions les plus vénérables du droit français, l'acte authentique, ne peut être uniquement motivée par le désir de la profession notariale de se parer des toutes dernières avancées technologiques afin « de ne pas affronter la concurrence sous des couleurs fanées. »⁵⁸

Alors même que de plus en plus de services administratifs et de transactions commerciales sont possibles par l'entremise de réseaux électroniques, la preuve documentaire demeure un instrument simple et durable, essentiels aux administrés et aux consommateurs pour faire valoir leurs droits et apporter la sérénité nécessaire aux échanges commerciaux. Il serait souhaitable que l'adaptation d'un outil aussi performant au contexte électronique implique l'ensemble des professions concernées par l'administration de la preuve documentaire — juristes, spécialistes de l'informatique, mais également, les archivistes. Une preuve documentaire dont la complexité technique la met hors de portée de ses usagers et des professions chargées de l'administrer, ne remplit plus les objectifs de stabilité juridique et sociale envisagés par les rédacteurs du Code Civil.

⁵⁵ Michael Lynch, Ruth McNally & Patrick Daly, « Le tribunal : Fragile espace de la preuve », *La Recherche*, n° 300, juillet-août 1997, p. 112-115.

⁵⁶ Ce sont de tels critères que le groupe InterPARES offre sous la forme de *benchmark* et *baseline requirements*. Voir MacNeil *et al.*, « Authenticity Task Force Report », in *The Long-term Preservation of Authentic Electronic Records*. InterPARES 2002.

⁵⁷ C.C., art. 1317 : « L'acte authentique est celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises. Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat. »

⁵⁸ Pierre Catala, « Le formalisme et les nouvelles technologies », *Defresnois* 15-16/00, p. 910.