Jean-François Blanchette

Théorie et pratique de la preuve documentaire à l´ère de l´électronique
Exposé aux Journées d´informatique juridique 2004 à Berne

Par sa plasticité, sa reproductibilité et sa libre circulation au travers de réseaux toujours plus étendus et interconnectés, l'information numérique semble remettre en question certaines des institutions les plus importantes du monde juridique, parmi elles, le droit de la preuve. La Directive Européenne de 1999 sur la signature électronique devait réagir à ce défi et exprimer la modernité du droit européen face à la nouvelle donne des échanges commerciaux électroniques. Dans cette présentation, nous suggérons que l´emphase de cette réforme sur la fonction de signature électronique a occulté le problème plus général de la preuve documentaire. 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 joue un rôle de plus en plus important dans la vie administrative et juridique des citoyens.

Tables des matières

I. Introduction

[Rz 1] Peut-être plus que tout autre développement technologique l'ayant précédée, l'explosion des nouvelles technologies de l'information et de la communication (TIC) 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.

[Rz 2] Cette apparente capacité à défier le droit a justifié en 1997 la commande par le Gouvernement d'une étude au Conseil d'Etat, dans le but d'identifier les moyens s'offrant à l'État pour réguler efficacement ces nouveaux médias. [1] Publié en 1998, le rapport a réaffirmé 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 la pertinence de la plupart des concepts généraux, parfaitement transposables à ce nouvel environnement, même si certaines adaptations sont nécessaires [2]».

[Rz 3] Cet article présente les conditions de ces «nécessaires adaptations» dans le contexte de la définition d'un nouveau cadre juridique du droit de la preuve en France. Du point de vue législatif, trois dates marquent à ce jour ce processus:

a) Le 13 décembre 1999, avec la publication de la Directive européenne «sur un cadre communautaire pour les signatures électroniques[3]»;
b) Le 13 mars 2000, avec la loi «portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique[4]»;
c) 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 électronique[5]».

[Rz 4] Ces dates fournissent une grille de lecture parallèle au contenu juridico-régulatoire des textes en question, encadrant le début et la fin de la fièvre spéculatoire sur les technologies Internet, fièvre qui exerça à l'époque une extraordinaire emprise sur le discours public en France et en Europe.

[Rz 5] Cet article propose par conséquent 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 processus distincts (et, jusqu'à tout récemment, indépendants): 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 régulatoires internationales [6] et introduit dans le droit français par le biais de la Directive de 1999.

[Rz 6] Si cette analyse ne permet pas de dégager de la réforme de 2000 une cohérence qu'elle n'a de toute façon jamais possédée, elle permettra d'en distinguer les logiques constitutives et de les contraster avec d'autres logiques, celles issues de la confrontation de la science archivistique avec les technologies de l'écrit électronique. Une telle analyse suggère que, loin d'un simple aménagement mécanique, les «nécessaires adaptations» sont synonymes de bouleversements profonds qui n'épargneront ni les principes qui sous-tendent, ni les pratiques qui entourent, le droit de la preuve français.

II. La réforme de 1980

[Rz 7] La confrontation du droit de la preuve français au nouvelles manifestations de l'écrit débute avec la réforme de 1980, 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). [7] Si ces nouvelles formes d'écrits posent à l'analyse doctrinale les mêmes défis conceptuels que ceux associés aux nouvelles technologies de l'information, ils ne s'inscrivent pas dans une mouvance sociale comparable à celle si puissamment symbolisée aujourd'hui par l'Internet. Le législateur se contentera ainsi stipuler que les règles du Code Civil (articles 1341 et suivants) exigeant la production d'un écrit papier

> «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 durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support.» (art. 1348)

[Rz 8] Bien que la valeur probante de telles reproductions ne soit 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 le déploiement 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 très fine, le professeur Jacques Larrieu propose un certain nombre principes qui, selon lui, seraient à même de d'affecter une transition harmonieuse à un univers de transactions électroniques. [9]

[Rz 9] J. 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 techniques.»[10] Suivant en cela l'analyse socio-historique d'Henri Levy-Bruhl, J. Larrieu affirme que la prééminence de l'écrit dans le droit de la preuve français n'est en aucun cas attribuable à ses qualités matérielles (en tant que support infalsifiable), mais n'est plutôt explicable que par son important capital symbolique, dû à sa longue présence historique dans la société française et la protection étendue que le législateur lui accorde. [11]

[Rz 10] J. Larrieu suggère plutôt que la valeur probante d'un document est facteur de trois conditions: (a) les qualités de son auteur (par exemple, sa compétence 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 accident. Il 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 J. Larrieu pourra surprendre. Il pose 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 pré-constitution 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]

[Rz 11] Il n'y a donc, selon J. Larrieu, aucun obstacle, juridique ou intellectuel, à la reconnaissance des 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 «accorder à ces nouvelles technologies 'la légitimation sociale' qui seule peut établir la confiance en ces moyens de preuve.» [14] En dernière analyse, le pouvoir de la preuve émane avant tout du tissu de conventions sociales sur laquelle cette preuve repose, tissu dont le droit positif ne forme qu'un élément. Dans l'optique de J. 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

[Rz 12] Néanmoins, les appels à une intervention législative se feront entendre de façon répétée au cours des années 1990. Le Ministère de la justice constituera alors en 1996 un groupe de travail, formé d'universitaires éminents, ayant 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. [15]

[Rz 13] 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 loi déposé au Sénat en septembre 1999 et adopté à l'unanimité par l'Assemblée nationale le 29 février 2000. Bien que 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.[16] Quatre articles du Code Civil 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 matériel

> «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 leur modalités de transmission.» (art. 1316)

[Rz 14] 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.» (art. 1316-1)

[Rz 15] Troisièmement, des règles indiquant à un juge la manière de trancher en cas de conflit entre des écrits sur différents supports:

> «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.» (art. 1316-2)

[Rz 16] 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.» (art. 1316-3)

[Rz 17] 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 J. 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. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.» (art. 1316-4)

[Rz 18] 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 […]» (art. 1316-4)

[Rz 19] La deuxième partie du second alinéa de l'article 1316-4 introduit un mécanisme qui permet 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 'Etat.» (art. 1316-4)

[Rz 20] 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. Parcours juridique de la signature électronique

[Rz 21] En 1976, deux chercheurs de l'Université de Stanford, Whitfield Diffie et 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.[17] Cette science, que Ronald Rivest définit comme celle de «la communication en présence d'adversaires»[18], 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.* Cependant, la nécessité pour les participants de s'entendre *au préalable* sur une telle clé commune réduit considérablement l'efficacité et la sécurité de tels systèmes de communication chiffrés. Dans leur article, Diffie et Hellman proposent un mécanisme mathématique inédit

permettant à deux individus d'échanger des données chiffrées, avec la propriété étonnante qu' *ils ne nécessitent pas de s'entendre au préalable sur une clé commune de chiffrement et de déchiffrement.* Le mécanisme étant 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, il est désigné sous le nom de *cryptographie à clé publique*, ou encore, *cryptographie asymétrique.*

[Rz 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, [19] simplement en inversant l'ordre des clés: la clé privée devient la *clé de signature*, et la clé publique, celle de *vérification*. Le mécanisme offre alors les assurances 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 modifiée après la «signature», sinon la vérification aurait échoué.[20]

[Rz 23] C'est l'explosion des technologies de l'Internet qui pose, au milieu des années 1990, le problème de la sécurisation du commerce électronique. La signature électronique, telle que proposée 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 suscitées par 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 textes ayant le plus contribué à définir ce cadre, il faut citer les *Digital Signature Guidelines* de l'American Bar Association, les *Cryptography Guidelines* de l'OCDE, et la *Loi type sur le commerce électronique* de la CNUDCI. Le texte législatif le plus important à reconnaître un rôle particulier à la signature cryptographique est cependant la Directive Européenne du 13 décembre 1999 *«sur un cadre communautaire pour les signatures électroniques».*

[Rz 24] Les Directives Européennes sont des instrument réglementaires complexes, dont l'objectif principal est d'obtenir une harmonisation des réglementations nationales de façon à éliminer les obstacles intérieurs au marché unique. Dans le cas de la signature électronique, cette harmonisation se voulait préventive, face à la reconnaissance prochainement attendue de la valeur de preuve de la signature électronique par les Etats Membres. Elle se voulait également proactive dans l'établissement d'un marché européen de la signature cryptographique et des services associés. A cette fin, la Directive définit une architecture réglementaire se fondant sur deux niveaux distincts de signatures électroniques, mandant les Etats Membres de leur accorder une valeur juridique distincte. L'article 2.1 définit une «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), 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)

[Rz 25] Cette seconde définition décrit, sans la nommer, la signature électronique fondée sur les technologies de cryptographie à clé publique, puisque la quatrième caractéristique est l'apanage de cette technologie, c'est-à-dire que la vérification de la signature échoue si le message signé subit une quelconque modification après la signature. [21]

[Rz 26] À ces deux types de signature électronique correspondent deux régimes d'admissibilité et de force probante. D'une part, dans le cas d'une signature électronique «générique», la Directive exige des Etats Membres que ceux-ci se conforment au principe de «non-discrimination» énoncé par la CNUDCI, [22] 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.» (art. 5.2) 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.»[23]

[Rz 27] 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 «générique», à la force probante indéterminée.

[Rz 28] La jonction entre les exigences de la Directive et le processus amorcé au sein du système juridique français allait s'effectuer au sein du groupe de travail constitué par le Conseil d'Etat à la demande du Premier Ministre [24], qui allait alors 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. Ce procédé permet de signer des messages électroniques dont l'origine et l'intégrité sont certifiées par un tiers dit de certification.» [25]

[Rz 29] C'est ainsi que, à la suite de la définition originale de la signature de l'avant-projet de loi, apparaît 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 'Etat» (Code Civil, art. 1316-4). Une fois retracée l'historique du modèle de la signature cryptographique, le texte du décret d'application du 30 mars 2001 prend tout son sens. [26] La première définition de la signature reprend la définition de signature générique de la Directive:

> «'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 ;» (art. 1.1)

[Rz 30] La seconde définition reprend presque mot pour mot la définition de signature avancée introduite par la Directive:

> «'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 ;» (art. 1.2)

[Rz 31] L'article 2 du décret résume la mécanique complexe des infrastructures à clés publiques en une seule finalité, celle d'accorder à la signature cryptographique une *présomption de fiabilité*, faisant ainsi porter le *risque de la preuve* sur celui qui en conteste la validité:

> «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.» (art. 2)

[Rz 32] Le tableau final de l'acte sous seing privé sur support électronique est donc celui-ci: d'une part, *l'écrit électronique* est admis, avec une force probante équivalente à celui sur support papier, en autant que l'identité de son auteur et sa conversation soit assurée. D'autre part, une technologie particulière de signature électronique, celle fondée sur la cryptographie asymétrique, bénéficie d'une présomption de fiabilité. Bien que tout procédé de signature électronique répondant à la définition de 1316-4 soit admissible, le mode de démonstration de sa fiabilité n'est pas spécifié. D'autre part, les faiblesses de la Directive se retrouvent à l'identique dans le décret, c'est-à-dire que le processus de vérification n'est nullement régulé, [27] et que la conservation dans le temps des signatures «sécurisées» n'est nulle part abordée. [28]

V. Les archivistes

[Rz 33] La réforme de 2000, telle qu'articulée par les juristes et les informaticiens, ne fait pas appel à la réflexion collective entamée depuis plusieurs années par la profession archivistique sur la meilleure façon d'assurer

l'authenticité des documents électroniques et de préserver leur fonction de mémoire et de preuve. La place croissante occupée par l'écrit électronique au sein des sociétés industrielles a forcé la communauté archivistique à interroger la pertinence des approches traditionnelles à la préservation de la preuve documentaire. En effet, la perte du lien entre le contenu informationnel du document et son support, de même que l'obsolescence accélérée affligeant les éléments matériels et logiques nécessaire à l'intelligibilité de l'écrit électronique, exigent d'interroger la pérennité des grands principes archivistiques ou la nécessité de leur reformulation.

[Rz 34] Cette interrogation s'est en partie déroulée par l'entremise de projets de recherche pluridisciplinaires, notamment le projet InterPARES,[29] qui réunit des représentants des Archives nationales sur quatre continents et dont la première phase s'est conclue en 2001. Le projet a dégagé un ensemble de principes susceptibles de sous-tendre toute politique, stratégie, ou norme visant à assurer la préservation des qualités d'authenticité des documents d'archive,[30] principes offrent une alternative à ceux qui ont menés à la loi du 13 mars 2000. Cinq de ces principes sont particulièrement pertinents à notre propos:

[Rz 35] **1. – Reconnaître que la préservation de documents d'archive électroniques authentiques est un processus continu, qui débute au moment de la création du document, et dont la finalité est la transmission de documents d'archive authentiques à travers l'espace et le temps.**

[Rz 36] L'archivistique ne s'est traditionnellement préoccupée du document qu'à partir du moment où celui-ci est susceptible d'être transféré à des archives. Ce n'est qu'à partir de ce moment que l'archiviste va évaluer la pertinence du transfert, pour ensuite (a) assurer les conditions matérielles de conservation du document (bâtiments spécialisés, locaux d'archivage, conditionnement des documents); (b) effectuer la description du document, selon des conventions qui permettent au document de prendre sens, en le replaçant dans son contexte de production; [31] (c) spécifier les modalités de communication des documents, c.-à-d. sécurité, règles de communication, et délivrance de copies.

[Rz 37] Dans le contexte de l'écrit électronique, ce processus ne suffit plus à assurer l'authenticité des documents. Il faut plutôt mettre en place un système cohérent de contrôles – la «chaîne de préservation» – s'appliquant sur *l'ensemble du cycle de vie* des documents, contrôles qui assurent leur identité et leur intégrité à travers toute manipulation qui affecte la façon dont les documents sont représentés pour le stockage ou présentés lors de leur utilisation.[32]

[Rz 38] Pour évaluer la qualité de ces contrôles, InterPARES propose deux listes de critères s'appliquant à deux phases distinctes du cycle de vie des documents:

- les *benchmark requirements* définissent les exigences relatives à la création et à la préservation des documents alors qu'ils sont sous le contrôle de leur créateur; [33]

- Les *baselines requirements* définissent les exigences relatives au transfert et la préservation des documents sous le contrôle de l'archiviste, de façon à ce que la chaîne de préservation demeure intacte; ces exigences permettent de définir les conditions nécessaires à la production de copies authentiques des documents d'archives;[34]

[Rz 39] Seule la conformité à ces deux ensembles d'exigences permet d'inférer la qualité d'authenticité d'un document d'archive électronique.

[Rz 40] **2.** – *Enoncer explicitement que le mécanisme principal permettant de protéger et d'établir sur le long terme l'authenticité des documents est* ***la documentation exhaustive de la totalité du processus de préservation*** .

[Rz 41] 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 la chaîne de préservation.

[Rz 42] **3.** – *Etre fondé sur le principe qu'il est impossible de préserver un document d'archive électronique en tant qu'objet physique entreposé;* ***il est uniquement possible de préserver la capacité de rendre un document intelligible.***

[Rz 43] 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, pouvant être recopié à l'infini sans souffrir de dégradation ;

- D'autre part, la chaîne de bits qui forme cet encodage [35] est susceptible d'être modifiée, au fil des migrations nécessaires pour préserver l'intelligibilité du document. [36]

[Rz 44] 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'infirmer 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!

[Rz 45] **4.** – *Etablir une distinction claire entre la* ***préservation de l'authenticité*** *des documents et leur «authentication».*

[Rz 46] Du point de vue de la communauté archivistique, la signature électronique fournit un service d' « *authentication»*[37] 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. [38] Dans l'univers électronique, cette attestation est généralement effectuée après une transmission du document dans l'espace. Elle 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), [39] ni au concept d'authenticité du droit civil, (la force probante résultant de l'exécution de certains formalismes par un officier public). [40] 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.

VI. Conclusion et pistes

[Rz 47] Le savoir-faire et le fondement du métier de l'archiviste ont permis de renouveler et d'enrichir la réflexion sur le droit de la preuve dans l'environnement électronique. Si le cadre législatif de la réforme de 2000, fondé sur la signature électronique, demeure, il est d'ores et déjà apparent que cette technologie ne peut servir de panacée au problème de l'authenticité des documents électroniques. Nous conclurons donc en évoquant deux pistes de réflexion particulièrement prometteuses, la première issue de la sociologie des sciences, la seconde fruit des méthodes ethnographiques utilisées par des chercheurs du domaine de l'interaction homme-machine.

[Rz 48] La réforme du droit de la preuve français a été principalement conduite sous l'égide des juristes, en consultation avec des experts informatiques. Elles sont axées, comme nous l'avons indiqué, sur les qualités des technologies de signatures cryptographiques, telles qu'entérinées par la loi du 13 mars 2000 et ses décrets d'application. Alors que, comme Jacques Larrieu l'a souligné, le droit n'avait jamais auparavant particulièrement présumé des qualités matérielles du support de la preuve, on a cru bon d'accorder à la signature électronique une présomption de fiabilité. Selon cette logique, l'utilisation de la signature cryptographique assurerait l'authenticité de l'écrit électronique – son origine et son intégrité – avec un niveau de sécurité dépassant largement ce qui était possible dans l'univers papier.[41]

[Rz 49] Une première piste est offerte par l'analyse de trois sociologues des sciences qui observent 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 toute autre déclaration», cette technologie connaîtra un échec retentissant au cours du célèbre procès d'O. J. Simpson. C'est 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 des fonctionnaires responsables. Pour être considérée comme telle, la vérité contenue dans la signature automatique (le code à barre génétique) se doit donc d'être accompagnée, entourée, par toute une série de traces bureaucratiques: signatures manuscrites sur des formulaires standards, véritables codes à barres collés sur les sacs contenant les échantillons, etc.» [42]

[Rz 50] 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 que cet écrit est susceptible de subir – création, modifications, annotations, signature, sauvegarde, conversion, etc. Pour être 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. En entourant l'écrit électronique d'un faisceau serré de preuves concordantes, ces traces en garantissent l'authenticité et l'intégrité, même si cette notion n'est plus assimilable à *l'intégrité physique* du document.

[Rz 51] Une seconde piste est offerte par des chercheurs qui se sont intéressés à l'utilisation du papier comme outil permettant d'accomplir des tâches de traitement de l'information – lecture, correction, classement, communication, etc. – au sein des organisations. La première observation résultant de cette démarche est que si, dans certains contextes, le papier semble «résister» à l'informatisation, ce n'est pas dû aux difficultés liées au «changement des mentalités», mais bien parce que le papier demeure l'instrument principal par lequel les membres d'un groupe organisent leurs activités individuelles et coordonnent leurs activités collectives.

[Rz 52] Il en découle, comme l'ont observé deux auteurs d'une importante série d'études sur la question, [43] que si le processus d'informatisation est motivé par le désir d' *éliminer* le papier (et la symbolique afférente de bureaucratie poussiéreuse et inefficace), cette informatisation est vouée à rencontrer des difficultés importantes – une observation qui s'applique tout à fait au processus de réforme du droit de la preuve que nous avons décrit dans cet article. En fait, il est beaucoup plus profitable de considérer que le papier et l'électronique sont voués à une relation durable et synergétique, où *l'un supplémente, plutôt que supplante l'autre,* (comme est à même de le constater, d'un simple coup d'œil à son bureau, n'importe que travailleur moderne de l'information). [44] Ainsi, même à l'ère de l'administration moderne et transparente — dématérialisée, rien de moins ! – il n'est pas inutile de considérer la pertinence d'un certain conservatisme et du développement de stratégies de conservation mariant l'électronique à des supports plus durables, comme la technologie COM et le microfilm.

[Rz 53] 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. 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. Il est donc essentiel 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, specialistes des technologies de l'information, mais également, archivistes.

Jean-François Blanchette, Assistant Professor, Department of Information Studies, Graduate School of Education & Information Studies, University of California, Los Angeles.

Eine deutschsprachige Zusammenfassung des Vortrags von Jean-François Blanchette an der Tagung für Informatik und Recht 2004 in Bern wurde publiziert als: Eva Schmid, Theorie und Praxis des Dokumentenbeweises im Internetzeitalter, in: Jusletter 8. November 2004.

[1] Conseil d'Etat, *Internet et les réseaux numériques* , Paris, La Documentation Française, 1998.

[2] Conseil d'Etat, *op. cit*., p. 12.

[3] «Directive 1999/93/EC du Parlement Européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques», *OJEC* L13, 2000.

[4] «Loi n°. 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique», *JORF,* n° 62, 14 mars 2000, p. 396*8*.

[5] «Décret n° 2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du Code civil et relatif à la signature électronique», *JORF*, n°77, 31 mars 2001, p. 5070.

[6] Par exemple, *Loi type de la CNUDCI sur le commerce électronique* , Commission des Nations Unies pour le Droit Commercial International 1997; *OECD Cryptography Policy Guidelines*, OCDE/GD(97) 204 , 1997; *Digital Signature Guidelines*, American Bar Association, 1995.

[7] Voir Michel Vion, «Les modifications apportées au droit de la preuve par la loi du 12 juillet 1980», *Desfrenois,* no. 32470, 1980.

[8] Vion, *op. cit*, p. 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. Cette analyse a aussi fortement inspiré celle de Xavier Lagarde: voir Xavier Lagarde, *Réflexion critique sur le droit de la preuve*, Paris, Librairie générale de droit et de jurisprudence, 1994; et Xavier Lagarde, «Vérité et légitimité dans le droit de la preuve», *Droits*, no. 23, p. 31-40, 1996.

[12] Larrieu, *op. cit.*, p. 14.

[13] Ibid., p. 15.

[14] Ibid., p. 10.

[15] Groupe composé de Pierre Catala, Pierre-Yves Gautier, Jérôme Huet, Isabelle de Lamberterie, Xavier Linant de Bellefonds, André Lucas, Lucas de Leyssac, et Michel Vivant.

[16] 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, et 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* , (s.l.d. Camille Jauffret-Spinosi et Isabelle de Lamberterie), Paris, Société de législation comparée, 1999, ainsi que Isabelle de Lamberterie «Preuve et Signature: Les innovations du droit français», *Cahiers Lamy droit de l'informatique et des réseaux* K, no. 123 (2000).

[17] Wittfield Diffie et 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. Egalement, 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, Wiley, 2000.

[18] Ronald R. Rivest, «Cryptography», in *Handbook of Theoretical and Computer Science (Volume A: Algorithms and Complexity)*, Cambridge, Mass.: Elsevier and MIT Press, 1990, p. 6.

[19] Diffie & Hellman *op. cit.*, p. 644.

[20]

Pour autant que les hypothèses mathématiques sur lesquelles la sécurité d'un tel système est fondé demeurent valables. 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* (s.l.d. Isabelle de Lamberterie), Paris, La Documentation Française, 2001.

[21] Et ce, malgré les prétentions de la Directive à une approche fondée sur la «neutralité technologique»: par exemple, préambule 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.»

[22] CNUDCI, *op. cit.*, art. 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.»

[23] Directive, *op. cit*., art. 5.2.

[24] Voir *supra*, note 1.

[25] Conseil d'Etat, *op. cit*.

[26] «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», *JORF* (2001).

[27] Isabelle de Lamberterie et Jean-François Blanchette, «Le décret du 30 mars relatif à la signature électronique: lecture critique, technique et juridique», *La Semaine Juridique – Entreprises et affaires* , no. 30, 2001., p. 1269-1275.

[28] Jean-François Blanchette, «The Digital Signature Dilemma: To Preserve or Not to Preserve ?» in *Proceedings, IS&T's 2004 Archiving Conference*, April 20-23, 2004, pp. 221-226. Springfield, Virginia: The Society for Imaging Science and Technology.

[29] «**I**nternational **R**esearch on **P**ermanent **A**uthentic **R**ecords in **E**lectronic **S**ystems». Voir http://www.interpares.org.

[30] Luciana Duranti *et al.*, «Strategy Task Force Report», in *The Long-term Preservation of Authentic Electronic Records – Findings of the InterPARES Project*, Vancouver, 2004.

[31] Leur valeur étant conditionnée à l'action qui a présidé à leur élaboration, de même qu'aux missions et attributions de l'institution qui a produit ou reçu ces documents.

[32] Duranti, *ibid.*

[33] MacNeil *et al*, «Requirements for Assessing and Maintaining the Authenticity of Electronic Records», in *The Long-term Preservation of Authentic Electronic Records – Findings of the InterPARES Project* , Vancouver 2004.

[34] MacNeil, *ibid.*

[35] En anglais, *bitstring.*

[36] Voir Thibodeau, *op. cit.*

[37] 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.

[38] «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.

[39] Voir Duranti, *ibid*.; Duranti, L., T. Eastwood, et al. (2002). *Preservation of the Integrity of Electronic Records* . Dordrecht, Kluwer Academic Publishers., p. 110

[40] Flour, J. (1972), «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.

[41] Voir Armant Roth, «L'acte dématérialisé existe: je l'ai rencontré», *La Semaine Juridique Notariale et Immobilière*, No. 29, 21 juillet 2000, pp. 1186-1187.

[42] Michael Lynch, Ruch McNally et Patrick Daly, «Le tribunal, fragile espace de la preuve», *La Recherche*, n° 300, juillet-août 1997, p. 113.

[43] Abigail J. Selen et Richard H. R. Harper, *The Myth of the Paperless Office* , Cambridge, Mass., MIT Press, 2002.

[44] Voir Ziming Liu et David G. Stork «Is Paperless Really More? Rethinking the Role of Paper in the Digital Age» *Communications of the ACM* 43:11(94-97).

Rechtsgebiet:	Informatikrecht
Erschienen in:	Jusletter 8. November 2004
Zitiervorschlag:	Jean-François Blanchette, Théorie et pratique de la preuve documentaire à l´ère de l´électronique, in: Jusletter 8. November 2004
Internetadresse:	http://www.weblaw.ch/jusletter/Artikel.asp?ArticleNr=3467