

**Citation** : Eric A. Caprioli, *Traçabilité et droit de la preuve électronique*, <http://www.caprioli-avocats.com>

**Première publication** : *Droit & Patrimoine*, mai 2001

---

## TRAÇABILITE ET DROIT DE LA PREUVE ELECTRONIQUE

[Eric A. Caprioli](#)

email : [contact@caprioli-avocats.com](mailto:contact@caprioli-avocats.com)

---

### Plan

#### INTRODUCTION

##### I/ La trace électronique, moyen d'identification

###### A) Identification et authentification électroniques

###### B) Délivrance et vérification de l'identité électronique

##### II/ Etablissement et conservation des traces électroniques intègres

###### A) La trace intègre

###### B) Restitution de la trace probante

#### Notes

---

### INTRODUCTION :

Alors que la "trace" est définie comme " *une suite d'empreintes ou de marques que laisse le passage d'un être ou d'un objet ; marque laissée par une action quelconque ; ce à quoi on reconnaît que quelque chose a existé ; ce qui subsiste d'une chose passée.*" ([1]), la « traçabilité » est un vocable entré dans le langage moderne qui ne fait l'objet d'aucune acception classique. Afin de saisir la signification que recouvre ce terme, la définition de la « trace » peut être exploitée comme point de départ. En outre, en informatique, le mot « traçabilité » existe et peut avoir plusieurs sens : « 1) *Aptitude à retrouver l'historique, l'utilisation ou la localisation d'un article ou d'une activité au moyen d'un identifiant enregistré.* 2) *Opération qui consiste, au fil des étapes de raffinement de la modélisation d'un système ou d'un logiciel en construction, à suivre toutes les exigences de la spécification et à vérifier qu'elles se retrouvent dans les constituants du modèle* » ([2]). Par ailleurs, la doctrine s'est souciée depuis longtemps des marques laissées dans le temps et de leur importance dans le droit. Ainsi, citant Locré, « *Si tous les hommes étaient justes et sincères, on n'aurait pas besoin sans doute de tant de règles. Mais outre que l'expérience n'a que trop appris tout ce que l'on doit redouter du vice ou de la faiblesse, ce qui seul justifierait les mesures que la loi prend pour constater les conventions, nous devons aussi reconnaître que les hommes se succédant sur la terre et les obligations se transmettant d'âge en âge, il est indispensable de fixer les formes qui seules peuvent faire retrouver les traces des obligations et des preuves de la libération.* », Messieurs Gautier et Linant de Bellefonds estiment que la « "trace", c'était déjà du langage informatique. » ([3])

Cette première réflexion nous invite à centrer notre étude sur la seule traçabilité liée aux technologies de l'information. Au préalable et d'une façon générale, il convient de relever que certaines traces informatiques sont laissées à l'insu des personnes, surtout lorsque l'on navigue dans les eaux numériques (données de connexion, adresse IP, ...). Ceci explique sans doute pourquoi les individus utilisateurs des réseaux invoquent de plus en plus le droit à l'anonymat voire plus généralement le respect de leur vie privée ([4]). En matière de droit de la preuve, la traçabilité couvre une sphère d'application très large : droit privé, droit public, droit comptable, fiscal, pénal, commercial (preuve libre), etc. Selon le domaine concerné, on peut distinguer les preuves ou traces volontairement préconstituées et les preuves non volontaires ([5]). Il est évident que la traçabilité a une incidence majeure en matière pénale pour les délits réalisés sur les réseaux numériques. En effet, en matière de preuve pénale, le juge et la police recherchent principalement deux choses : localiser et identifier l'auteur de l'infraction et préserver les éléments de preuve pour matérialiser l'infraction. Mais, ces éléments peuvent se trouver sur le territoire d'un autre état. Dans cette optique, la conservation des données de connexion aux réseaux qui constituent, le cas échéant, une preuve matérielle contribuera à la poursuite des délinquants. Or, sur les réseaux numériques, trois contraintes existent : l'**anonymat** (personne qui se connecte sur l'Internet à partir d'un ordinateur sans s'identifier) ; la **volatilité des informations** (possibilité de modifier et de supprimer des éléments de preuve quasi-instantanément) ; leur **caractère international**. Le projet de convention du conseil de l'Europe se propose d'apporter des réponses juridiques aptes à concilier ces différentes données ([6]). De même, lors de la conférence du G8 de Paris des 15-17 mai 2000, le sujet des débats était justement la cybercriminalité dans le cyberspace ([7]). L'acuité du sujet est forte après les attaques de février 2000 contre les principaux sites de commerce électronique (Yahoo.com, Amazon.com, e-bay ...) et suite aux virus MELISSA et I LOVE YOU. En outre, la création de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication ([8]) devrait permettre l'organisation d'un procédé efficace de lutte contre les « *cyberdélinquants* », et ce, notamment compte tenu de la coopération internationale dont l'office a la charge. Enfin, le régime de responsabilité civile et pénale des intermédiaires de la société de l'information (fournisseurs d'accès, fournisseurs d'hébergement) répond également au souci de traçabilité des acteurs de l'internet ([9]).

En matière probatoire, les fonctions de la traçabilité sont différentes. En effet, si la preuve est le reflet de l'existence de droits et de situations juridiques, sa finalité, comme l'enseignant Planiol, est de convaincre le juge ([10]). En ce sens, la preuve est une pierre essentielle du fonctionnement de la plupart des systèmes juridiques, notamment ceux de tradition romano-germanique. Plus précisément, en droit civil, il est important de savoir à qui l'acte qui a laissé une marque dans le temps est imputable et s'il est l'exacte restitution du contenu de l'acte à la date à laquelle il a été passé ([11]). A ce titre, comme le soulignait Monsieur Jérôme Huet, " *De fait, pour ceux qui concluent des opérations par le biais des réseaux de communication, il est essentiel de savoir que, s'ils en conservent la trace dans des mémoires d'ordinateur, ils pourront en faire état, en cas de litige devant un tribunal.*" ([12]). Dans la société de l'information, la question de la traçabilité au regard du droit de la preuve se trouve au cœur du débat sur la réforme du code civil. Les conditions d'une traçabilité probatoire résident ainsi dans la garantie de l'intégrité de l'écrit de son établissement à sa restitution. Sous cet angle, la traçabilité doit permettre l'identification des personnes dont l'acte émane, quand et à quel contenu les parties ont consenti.

La traçabilité vient de recevoir une consécration dans le cadre de l'adoption de la loi du 13 mars 2000 ([13]) portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique. Dans la présente étude, nous prendrons le parti de nous centrer sur la seule preuve des actes juridiques au regard de ce texte législatif, voté le 29 février 2000 par l'Assemblée nationale en première lecture en des termes identiques à ceux adoptés par le Sénat le 8 février 2000. Tous les modes de preuve qui relèvent de la preuve par tous moyens seront par conséquent exclus (faits juridiques, preuve entre commerçants, commencement de preuve par écrit notamment). De même, l'incidence de la loi selon qu'il s'agit d'écrit ad

probationem ou ad validitatem ([14]) ne sera pas étudiée dans la mesure où l'analyse de la traçabilité peut se faire indépendamment de cette préoccupation. Avec la loi nouvelle, le code civil s'affranchit du monopole « papier » et, "libéralisme" oblige, notre système probatoire s'est ouvert à d'autres supports, d'autres médias. Si l'on se penche sur la question de la traçabilité dans une perspective de droit de la preuve des actes juridiques, l'écrit appréhendé à l'article 1316-1 c. civ., comme le répète d'ailleurs selon nous de façon superflue l'article 1316-3 c. civ. ([15]), est une preuve parfaite. C'est donc à la lumière de l'article 1316-1 c. civ. que la trace entendue comme une marque ou une empreinte laissée par une action volontaire et qui subsiste d'une chose passée guidera notre réflexion ; étant précisé que l'écrit sous forme électronique doit correspondre à des exigences techniques. Cet article énonce en effet : " *l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité*". Dans cette logique, la trace électronique apparaît comme un moyen d'identification (I) et son établissement et sa conservation devront être réalisés dans des conditions de nature à en garantir l'intégrité (II) ; étant noté que ces caractéristiques exigées des écrits sous forme électronique pour valoir preuve conduisent nécessairement à examiner les signatures électroniques telles qu'elles ont été retenues tant par la directive du 13 décembre 1999 ([16]) que par le système français ([17]).

### **I/ La trace électronique, moyen d'identification**

Compte tenu de la définition large donnée par l'article 1316 c. civ. à la preuve littérale ([18]), nombreuses seront les traces concrètes qui pourront être qualifiées de preuve par écrit, indépendamment du support utilisé et des modalités de leur transmission. Si cette définition respecte le principe de neutralité technique en ne visant aucun support ni média particulier, pour admettre l'écrit sous forme électronique en preuve au même titre que l'écrit sur support papier, le juge doit néanmoins avoir la plus grande certitude possible que l'acte juridique en cause émane de celui auquel on l'oppose ([19]). Cette approche conduit à deux exigences : l'origine de cet échange électronique doit être sécurisée et sa non-falsification garantie. Ceci implique l'identification de la personne du signataire (A) ainsi que des garanties quant à la possibilité de vérifier ladite identification (B). La signature électronique basée sur la cryptologie à clé publique qui est le procédé retenu de façon implicite par la directive du 13 décembre 1999 et par le projet de décret français établit ce lien avec la personne signataire grâce à un certificat numérique d'identification émis par une autorité de certification (le Prestataire de service de certification, ci-après désigné par « P.S.C. »).

#### **A) Identification et authentification électroniques**

Préalablement à tout développement plus avant, une distinction importante tant sur le plan technique que sur le plan juridique mérite d'être présentée. En effet, les procédés relatifs à l'identification d'un système de signature doivent être appréciés et analysés distinctement des procédés relatifs à l'identification du titulaire d'un dispositif de signature électronique ([20]). L'illustration la plus parlante pour comprendre cette différence est celle des numéros d'identification personnels (P.I.N.) à quatre chiffres liés à l'utilisation de cartes à puce (téléphone portable, carte bancaire, ...) ou des certificats de signature quelque soit leur support (matériels ou logiciels) qui constituent un procédé n'identifiant pas directement la personne dont l'acte émane, mais identifiant la personne à laquelle il sera imputé ([21]). Comme nous l'avons déjà indiqué dans nos propos introductifs, la jurisprudence exigeait pour que l'écrit sous forme électronique (en l'espèce une télécopie) vaille preuve, en sus de l'intégrité de l'acte, que l'imputabilité de son contenu à son auteur désigné ait été vérifiée ou ne soit pas contestée ([22]). Avec la loi du 13 mars 2000, la notion d'imputabilité qui résulte de la formulation retenue à l'article 1316-1 c. civ., est appréhendée sous un nouvel angle. Ce texte reconnaît notamment la force probante d'un écrit sous forme électronique au même titre que l'écrit papier, « *sous réserve que puisse être dûment identifiée la personne dont il émane (...)* ». L'emploi du terme "dûment" avant le mot "identifiée"

implique que l'identification de la personne dont l'écrit émane doit faire l'objet d'une vérification. En ce sens, la première condition posée par l'article 1316-1 c. civ. pour que les écrits électroniques soient probants recouvre un double aspect : l'imputabilité de l'acte à la personne qui l'a signé et la vérification de l'identification du signataire. Dès lors, cette acception est plus large que la seule notion d'imputabilité traditionnellement retenue par la jurisprudence et la doctrine. Mais, l'article 1316-1 c. civ. ne renvoie pas directement à un décret en Conseil d'Etat pour prévoir les modalités relatives au respect de l'exigence d'identification (ainsi qu'à celle d'intégrité !). C'est donc indirectement que le régime probatoire institué pour les écrits électroniques impose un lien évident entre l'écrit et la signature qui sont pourtant deux notions juridiques distinctes. Cette exigence d'identification dûment constatée pour l'acte peut surprendre puisqu'il s'agit en réalité d'une fonction propre à la signature et non à l'écrit lui-même. Néanmoins, force est de constater que l'on exige des écrits électroniques, pour leur reconnaître la même force probante que les écrits papier, qu'ils soient signés. De la sorte, l'écrit s'inspire étroitement de la notion d'acte sous seing privé original (art. 1325 c. civ.). Le procédé de signature électronique basé sur la cryptologie à clé publique (signature numérique) offre la garantie d'identification telle qu'exigée des écrits sous forme électronique pour qu'ils valent preuve grâce au certificat à clé publique qui est l'un de ses composants fondamentaux. Avec la signature numérique, l'identification du signataire correspond au nom de la personne inscrite dans le certificat en qualité de signataire lié à une paire de clé asymétrique. Bien entendu, en pratique, la personne figurant sur le certificat peut mettre à disposition temporairement sa clé privée, son code ou son mot de passe à une personne de son choix (un proche, un collaborateur, ...). Dans ces hypothèses, l'acte n'émane pas directement de la personne qui est identifiée, mais d'une autre et ce, sans que l'on puisse le savoir justement parce que le code d'activation de la clé privée du signataire est parfaitement correct. Seul le recours à des procédés biométriques tels que l'empreinte digitale ou oculaire, permettra d'être certain que c'est effectivement le signataire qui a activé la clé privée avec les données de création de la signature (directive art. 2). Pour l'heure, le procédé de signature électronique tel que retenu par la directive européenne sur les signatures comme par le projet de décret français ne garantit que l'identification du signataire qui est la personne inscrite dans le certificat afférent au bi-clé activé et non pas l'identité du signataire en tant que personne. Ainsi, le projet de décret définit le signataire comme : "*toute personne qui détient un dispositif de création de signature électronique*" ([23]).

Il convient de noter au demeurant que l'authentification au sens juridique revêt deux significations. Soit elle correspond à "*l'opération (contemporaine de la rédaction d'un acte) consistant à conférer l'authenticité à cet acte (spécialement à observer les formes dont dépend celle-ci)*" étant noté que l'authenticité est ici entendue comme la "*qualité (spécialement force probante) dont est revêtu un acte du fait qu'il est reçu, ou au moins, dressé par un officier public compétent, suivant les formalités requises*" ([24]). Soit, elle est définie comme l'opération "*consistant (après coup) à vérifier l'authenticité d'un objet ou d'un document.*", l'authenticité étant cette fois-ci la "*qualité de l'objet ou du document (œuvre, écrit, et c.) dont l'auteur ou l'origine sont attestés, notamment sur la foi d'un certificat*". Dans le cadre de notre étude, c'est cette seconde définition qui nous intéresse puisqu'elle recouvre bien la notion d'identification. D'un point de vue technique, l'opération d'authentifier consiste à vérifier l'origine du message ; ce qui implique une identification de l'émetteur - signataire garantie par un tiers indépendant et qui peut être vérifiée par le destinataire. Notons en cet endroit que le P.S.C. n'authentifie jamais le contenu des actes, dont il ne connaît d'ailleurs en principe ni le nombre, ni la nature, ni la teneur, ni les noms des destinataires. Ce tiers a pour seule fonction d'identifier le signataire auquel il a octroyé un certificat numérique d'identité unique. Ainsi, le P.S.C. ne certifie à aucun moment l'écrit sous forme électronique mais seulement le dispositif de création de signature (bi clé) sous le contrôle du signataire, étant noté au demeurant que le certificat émis par le P.S.C. n'établit que le lien qui existe entre une personne et un bi-clé. Par suite, si le P.S.C. participe indirectement à l'écrit électronique en étant l'un des rouages du processus de la signature électronique, il n'a ni les moyens ni pour fonction de garantir les écrits électroniques. En revanche, son rôle est primordial dans l'opération d'identification électronique.

## B) Délivrance et vérification de l'identité électronique

Les signatures électroniques dite « avancées » ([25]) telles que visées par le projet de décret français pris en application de l'article 1316-4 c. civ. doivent satisfaire à 4 exigences. Ainsi, le procédé retenu qui correspond concrètement aux signatures numériques impose que la signature soit liée uniquement au signataire, qu'elle permette de l'identifier, qu'elle soit créée par des moyens que le signataire puisse garder sous son contrôle exclusif et enfin qu'elle soit liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable ([26]). Ceci étant précisé, dans le cadre des procédés d'identification numériques, la délivrance de l'identité s'effectue au moyen d'un certificat électronique qui est émis par le P.S.C.. Selon le niveau de sécurité juridique souhaité, les conditions d'enregistrement de ses abonnés par le P.S.C. peuvent varier. Ainsi, l'enregistrement peut s'effectuer directement et seulement en ligne. Dans ce cas, la certitude de l'identité déclarée par l'abonné n'est pas totale ; il s'agit donc d'une identification correspondant à un niveau de sécurité minimum. L'enregistrement peut également se faire en ligne et sur envoi par voie postale de pièces justifiant de l'identité des personnes morales et/ou physiques déclarée par le titulaire du certificat. Le P.S.C. peut aussi prévoir que ses abonnés s'inscrivent en ligne et procèdent au retrait du certificat (et des données d'activation) sur présentation des pièces justificatives en face à face, c'est à dire à un guichet organisé dans un lieu physique par le P.S.C.. L'enregistrement peut enfin être réalisé en dehors de toute inscription en ligne et exclusivement sur présentation d'un certain nombre de pièces justifiant de l'identité de la personne inscrite dans le certificat. Ce dernier est émis sous la responsabilité du P.S.C. ([27]). En pratique, ce certificat qui contient la clé publique de l'abonné est le plus souvent joint au message que la partie entend signer à l'aide de sa clé privée, mais il peut également être mis à disposition dans une base contenant les certificats émis par le P.S.C.. Dès lors, le récepteur du message ou du fichier signé (partie qui se fie) doit s'assurer que le certificat qui contient la clé publique correspondant à la clé privée ayant servi à signer est en cours de validité et qu'il n'est pas révoqué. Pour ce faire, il devra consulter la liste de révocation des certificats sur un annuaire publié et mis à jour par le P.S.C. émetteur du certificat. Le destinataire devra également vérifier la signature que le prestataire aura apposé sur le certificat jusqu'à l'autorité de certification racine c'est à dire celle qui se trouve au sommet de la pyramide hiérarchique (Infrastructure à Clé Publique ou I.C.P.) ([28]). Avec ce procédé de signature électronique, l'exigence d'identification est ainsi honorée.

Ceci étant posé, les traces de l'écrit sous forme électronique doivent également garantir son intégrité.

### II/ Établissement et conservation des traces électroniques intégrées

L'écrit doit être établi et conservé sans qu'aucune altération, ni changement ne soit intervenu depuis la manifestation de volonté d'adhésion au contenu de l'acte jusqu'au moment où il devra faire foi, apporter la certitude de son contenu au juge. Dans l'univers numérique, « virtuel », le système juridique a besoin de s'appuyer sur des éléments de preuve matérialisés sous forme de traces électroniques préconstituées. De sorte que si la loi sur la preuve prescrit que la trace électronique soit établie et conservée encore convient-il d'en assurer l'intégrité (A) ; toutefois, cette obligation probatoire a pour but de garantir la restitution de la trace par la conservation (B).

#### A) La trace intègre

Avec le support papier, la notion de trace intègre était caractérisée par « l'original ». L'intégrité de l'écrit, c'est à dire la certitude que l'écrit est demeuré intact dans le temps, correspond à une fonction juridique fondamentale ([29]). Cette notion facilement perceptible dans le monde matériel pouvait poser un problème particulier dans le monde numérique. En effet, l'informatique et d'une façon plus générale les échanges électroniques ne permettent pas une transposition parfaite de la notion d'original telle qu'appréhendue dans le

monde matériel. En informatique, il n'y a point d'original (sauf sur le système d'information utilisé), mais des copies. De la sorte, l'analyse menée par les parlementaires luxembourgeois lors du projet de loi sur le commerce électronique doit, selon nous, être partagée. Ainsi, il est exact que « *Classiquement, la distinction original-copie s'appuie sur une différenciation relative à la nature du support. A cette différenciation correspond un traitement juridique différent. L'information contenue sur le support original se voit reconnaître une force probante supérieure à celle apparaissant sur la copie.* » ([30]). Apparaît alors justifié l'article 7 de la loi luxembourgeoise du 14 août 2000 qui ajoute un article 1322-1 dans le code civil rédigé de la façon suivante : « *L'acte sous seing privé électronique vaut comme original lorsqu'il présente des garanties fiables quant au maintien de son intégrité à compter du moment où il a été créé pour la première fois sous sa forme définitive.* ». C'est dans le même sens que la loi-type de la C.N.U.D.C.I. ([31]) a intégré la fonction d'intégrité dans la notion de forme originale. Le législateur français lors des premiers textes spéciaux qui traitaient de la dématérialisation des factures et des déclarations administratives par voie électronique ([32]) n'avait pas procédé à une totale assimilation, se contentant d'énoncer un principe d'équivalence fonctionnelle. Néanmoins, l'emploi des termes « intégrité » et « fidélité » ([33]) constituent deux notions qui permettent de transposer l'exigence du caractère intact de l'écrit dans le monde électronique. En revanche, la notion de fiabilité ne répondait pas au besoin de sécurité juridique dans la mesure où ce terme s'applique, selon nous, exclusivement aux procédés et autres processus techniques, ainsi qu'aux systèmes informatiques qui produisent des documents, des écrits. Or, ce sont les écrits qui doivent être intègres voire fidèles ([34]), les moyens utilisés devant être fiables. A l'heure actuelle, seule la signature électronique basée sur un certificat à clé publique permet de garantir cette fonction d'intégrité. En effet, ce procédé opère de façon automatique un condensé (abrégé) du message signé qu'il chiffre au moyen d'un algorithme de cryptographie (par une fonction dite « *hasch* » ou « *contrôle* »). Le message signé est alors accompagné de l'« empreinte » obtenue qui garantit que le document envoyé est identique au message reçu. Dès lors, le destinataire d'un message ou un fichier signé qui entend s'y fier, doit vérifier que la signature est valable c'est à dire qu'il doit comparer le résultat du calcul numérique (suite de chiffres) de l'abrégé du message chiffré à l'émission avec le résultat du calcul obtenu lors de réception. Cette opération permet de s'assurer que le message est bien intègre. Aussi, est-il permis d'affirmer que le fait qu'un écrit sous forme électronique soit signé lui confère la qualité d'un écrit tenant lieu d'original. Par conséquent, non seulement la formulation de l'article 1316-1 c. civ. semble avoir été judicieusement choisie, mais au surplus, le procédé de signature numérique répond aux attentes juridiques en matière de traces intègres. Cette solution permet ainsi d'établir de façon certaine une assimilation parfaite entre la force probante des écrits papier et celle des actes sous forme électronique dès lors qu'ils sont signés. A contrario, rappelons que les juges demeurent rigoureux sur l'appréciation de la valeur probante des photocopies et des télécopies au regard de l'intégrité des originaux supposés reproduits. Ainsi, récemment, la jurisprudence a considéré que dans la mesure où l'existence même de l'original n'était pas établie et qu'elle était contestée par le destinataire de la télécopie litigieuse, la preuve de l'acte juridique n'était pas rapportée ([35]). En outre, dans l'hypothèse des photocopies certifiées conformes, c'est à dire des copies dont la conformité à l'original est certifiée par une personne digne de foi et ayant procédé à la vérification entre le contenu de l'original et la copie, on peut penser que la condition de « fidélité » est respectée. Dans ce cadre, les photocopies certifiées conformes peuvent être considérées comme des traces intègres de l'acte juridique ([36]).

Par ailleurs, l'exigence d'un écrit sous forme électronique établi et conservé dans des conditions de nature à garantir l'intégrité permet d'appréhender l'écrit de la création de l'enregistrement informatique jusqu'à l'expiration de son délai de conservation et parfois sa destruction. Dès lors, la fonction intrinsèque d'intégrité de l'acte sous forme électronique est assurée pendant tout son cycle de vie. Cette approche fait de l'écrit électronique un document indépendant du support utilisé. Est ainsi juridiquement reconnue la possibilité de changer de support durant la vie de l'écrit électronique pour autant que son intégrité soit préservée et que les moyens et procédures de sécurité utilisés soient idoines.

## B) Restitution de la trace probante

Souvent le contrat électronique résulte d'une succession de messages signés électroniquement (une offre, son acceptation). Cependant un même fichier peut être signé électroniquement par les parties. La restitution est la finalité essentielle de la conservation. Elle doit être intelligible (1) et accessible ultérieurement (2).

### 1) Intelligibilité et lisibilité

Depuis longtemps, la jurisprudence française considère que l'écrit peut être appréhendé de façon autonome vis à vis de l'instrument et de la matière qui ont permis de le réaliser ([37]). La loi du 13 mars 2000 a consacré cette approche. Toutefois, il résulte de l'article 1316 c. civ. que pour être une preuve par écrit, la suite " *de lettres, de caractères, de chiffres ou de tous autres signes ou symboles* " doit être dotée d'une signification intelligible. Ceci signifie selon nous que l'écrit exprimé, même sous une forme chiffrée (ce qui vise directement les messages cryptés) ou de code informatique ne vaudront preuve que si leur contenu informationnel peut être produit de façon lisible et compréhensible par l'homme. En conséquence, pour que le juge puisse retenir un écrit sous forme électronique à titre de preuve, il devra pouvoir le comprendre. La condition de l'intelligibilité qui concerne tous les écrits - qu'ils soient notamment sous forme électronique ou sur support papier - implique que le contenu informationnel de l'écrit puisse être restitué en langage clair au juge, par exemple sous la forme d'une sortie imprimée sur papier. Il convient de noter en cet endroit que l'intelligibilité de l'écrit induit qu'il soit conservé de telle sorte que cette condition soit respectée, c'est à dire que la restitution de l'écrit à plus ou moins long terme garantisse que l'homme pourra avoir accès au contenu de l'écrit de telle sorte qu'il soit intelligible par lui.

### 2) Accessibilité ultérieure

L'article 6 de la loi-type de la CNUDCI relatif à l'écrit intègre l'idée d'accessibilité ultérieure de l'écrit électronique. Malheureusement, contrairement au projet de loi initial, la loi du 13 mars 2000 n'a pas repris cette notion à l'article 1316 c. civ. dans le cadre de la définition de la preuve littérale. Or, le souci d'accessibilité ultérieure de l'écrit touche à la durabilité de l'écrit c'est à dire comme l'appréhende l'article 1348 alinéa 2 c. civ. à l'intégrité du document dans le temps. Néanmoins, l'absence de référence à cette notion dans le cadre de l'article 1316 c. civ. est corrigée par les termes de l'article suivant. En effet, l'article 1316 -1 qui prescrit une trace identifiable de la personne dont l'acte émane impose également que l'acte soit conservé dans des conditions qui garantissent son intégrité. Dès lors, la notion de conservation ainsi exigée par ce texte renvoie à celle d'accessibilité ultérieure du document étant donné que l'intégrité demeure une fonction intrinsèque de l'écrit électronique pour qu'il vaille en preuve. Qui plus est, le législateur a posé le seul principe de la conservation de l'intégrité de l'écrit électronique mais ne traite pas, à juste titre selon nous des modalités d'une telle conservation. Cette matière relève en effet du domaine réglementaire. Ainsi, pour les écrits papier, aucun texte de loi général ne précise quelles méthodes utilisées pour protéger ce support pourtant altérable par nature au fil du temps (du fait des bactéries, des insectes, de l'humidité voire des incendies notamment). Il aurait été peut-être souhaitable que le législateur prévoit explicitement l'intervention d'un décret en Conseil d'Etat sur ce point, à l'instar de ce qui a été décidé pour les signatures électroniques (art. 1316 -4, al. 2 c. civ.) et pour les actes authentiques électroniques (art. 1316-4, al. 1 c. civ. *in fine* et art. 1317 c. civ.) ([38]). Le gouvernement devra se pencher sur cette question fondamentale de la conservation des écrits sous forme électroniques. Pour l'heure, la doctrine comme les acteurs de la société de l'information concernés par cette préoccupation primordiale ont réfléchi sur ce sujet. La question est importante sur le fond et correspond à un réel besoin de la pratique. Car à quoi peut servir l'admissibilité de la preuve électronique si la conservation y afférente n'est pas résolue ? ([39]). L'instauration de nouveaux prestataires de services d'archivage permettra de garantir la conservation de l'intégrité des écrits électroniques. Une telle solution serait intéressante dans la mesure où ces

prestataires de services contribueraient utilement à assurer la traçabilité des actes juridiques électroniques au moment où le code civil a tourné une page pour s'adapter à l'ère du numérique.

En tout état de cause, pour répondre à l'obligation d'intelligibilité de l'acte et d'accessibilité ultérieure de la trace probante, la conservation sera nécessairement « active ». Ainsi, afin que les écrits électroniques soient admis en preuve, elle devra permettre une migration des écrits sur différents supports sans qu'il soit porté atteinte à l'intégrité de l'acte. Cette caractéristique nous semble fondamentale dans la mesure où l'évolution des technologies est susceptible à plus ou moins brève échéance de rendre techniquement possible la réalisation de faux indétectables en cassant la clé de signature conservée avec l'écrit électronique.

Effectivement, il n'est pas exclu que dans quelques années la clé privée de signature (actuellement d'une longueur de 512 bits sur la plupart des navigateurs) puisse être déduite ou recalculée à partir de la clé publique dont on dispose ([40]). De la sorte, il est envisageable que les progrès technologiques permettent de refaire un faux intègre et re-signer avec la « vraie clé » privée l'écrit conservé sous forme électronique.

Il ressort de ces développements que l'acte devra pouvoir être suivi à la trace, de son enregistrement d'origine jusqu'à sa destruction, dans des conditions de sécurité juridique et techniques fixées ; c'est à ce prix que l'on disposera d'une preuve écrite « tracée ».

#### Notes :

[1] Dictionnaire Robert, entrée " Trace".

[2] Dictionnaire Informatique, Larousse, entrée : " Traçabilité".

[3] P.-Y. Gautier, et X. Linant de Bellefonds, *De l'écrit électronique et des signatures qui s'y attachent*, JCP 2000, éd. G, I 236, v. n° 31. Locré, t.XII, p.505.

[4] V. à titre d'illustration du " traçage" qui peut se faire à l'insu des internautes, l'expérience proposée sur le site de la CNIL, [www.cnil.fr](http://www.cnil.fr) (traces) ; pour des réflexions sur ce thème : v. C.N.I.L., 17ème rapport d'activité 1996, Paris, La documentation française, 1997, p. 99 et s. ; N. Mallet -Poujol, *Nouvelles technologies de l'information et libertés individuelles*, Problèmes politiques et sociaux, n° 805, Paris, La Documentation Française, 3 juillet 1998 ; J. Frayssinet, *Internet et protection des données personnelles*, Expertises 1998, n° 214, p. 99.

[5] M.-T. Calais-Auloy, *L'importance de la volonté en droit*, Les petites affiches, 7 décembre 1999, n°243, p. 14 et s.

[6] V. le site du Conseil de l'Europe : [www.coe.fr](http://www.coe.fr). Ce projet a été communiqué à la fin du mois d'avril 2000.

[7] Rev. Droit bancaire et financier, Mai -Juin 2000, n°3, p.167, chronique d'actualité de E. Caprioli et A. Prüm.

[8] Créé par le décret n°2000-405 du 15 mai 2000 (J.O. 16 mai 2000, p. 7338).

[9] La loi n° 2000-719 du 1<sup>er</sup> août 2000 (J.O. du 2 août 2000) modifiant la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication dispose en son article 43-9, « Les personnes mentionnées aux articles 43-7 et 43-8 (fournisseurs d'accès et d'hébergement) sont tenus **de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elles sont prestataires.** » De plus, aux termes de l'article 43-10, « I - Les personnes

dont l'activité est d'éditer un service de communication en ligne autre que de correspondance privée tiennent à la disposition du public : - s'il s'agit de personnes physiques, leurs noms, prénom et domicile, - s'il s'agit de personnes morales, leur dénomination ou leur raison sociale et leur siège social ; - le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction au sens de l'article 93 -2 de la loi n°82-652 du 29 juillet 1982 sur la communication audiovisuelle ; - le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné à l'article 43-8 (fournisseur d'hébergement). » Les personnes qui publient des contenus sur les réseaux devront donc respecter les règles applicables au droit de la presse.

[110] Planiol : « On appelle "preuves" les divers procédés employés pour convaincre le juge. », Traité élémentaire de droit civil, t. 2, 3<sup>ème</sup> éd., Paris LGDJ, p.1.

[111] V. sur ce point à titre d'illustration : Cass. com., 2 décembre 1997, à propos d'un bordereau Dailly communiqué par télécopie les juges considérant que « l'écrit constituant, ..., l'acte d'acceptation de la cession ou de nantissement d'une créance professionnelle peut être établi et conservé sur tout support t, y compris par télécopies, dès lors que son intégrité, et l'imputabilité de son contenu à son auteur désigné ont été vérifiées, ou ne sont pas contestées. », Cass. com., 2 décembre 1997, D. 1998, p.192, note Didier Martin.

[112] Jérôme Huet, *Preuve et sécurité juridique en cause dans l'immatériel*, Arch. Phil. Droit 1999, p. 164.

[113] JO du 14 mars 2000, p. 3968 ; pour des commentaires sur ce texte, V. : Michel Vivant, *Un projet de loi sur la preuve pour la "société de l'information"*, Cah. Lamy Droit de l'informatique, Bull. n°117, 1999, E, p.1 ; Pierre Catala, *Ecriture électronique et actes juridiques*, in *Mélanges Michel Cabrillac*, Paris, Litec, 1999, p.91 s. ; Eric Caprioli, *Le juge et la preuve électronique*, publié sur le site :

<http://www.iuriscom.net/universite/doctrine/article7.htm> et *Ecrit et preuve électroniques dans la loi n°2000-230 du 13 mars 2000*, JCP 2000, éd. E., n°2, p.1 et s. ; Valérie Sédallian, *Preuve et signature électronique*, <http://www.iuriscom.net/chronique/2/fr0509.htm> ; Jérôme Huet, *Vers une consécration de la preuve et de la signature électroniques*, D. 2000, chr., p.6 ; Pierre-Yves Gautier, *Le bouleversement du droit de la preuve : vers un mode alternatif de conclusion des conventions*, Petites affiches, 7 février 2000, n°26, p.10, n°16 et *Révolution internet : le dédoublement de l'écrit juridique*, D. 2000, n°12, Actualité, p.V -VI.

[114] J. Flour, *Sur une notion nouvelle de l'authenticité*, Défr. 1972, art. 30159, n°5, p.981 ; *Quelques remarques sur l'évolution du formalisme*, in *Etudes Georges Ripert*, T. 1, 1950, p.93 s. ; X. Lagarde, *Observations critiques sur la renaissance du formalisme*, J.C.P. éd. G, 1999, I, 170 et *Vérité et légitimité dans le droit de la preuve*, Droits, n°23, 1996, p.31 s. ; Luc Grynbaum, *Loi du 13 mars 2000 : la consécration de l'écrit et de la preuve électroniques au prix de la chute de l'acte authentique*, Commun. Comm. Electr. Avril 2000, p.14 ; Christian Pisani, *L'acte dématérialisé*, Arch. Phil. Droit 1999, p.153-161.

[115] L'article 1316-3 c. civ. dispose : "l'écrit sur support électronique a la même force probante que l'écrit sur support papier." ; v. pour un commentaire : Eric Caprioli, *Ecrit et preuve électroniques dans la loi n°2000-230 du 13 mars 2000*, JCP 2000, éd. E., n°2, p. 7.

[116] Directive 1999/93/CE du Parlement européen et du Conseil, sur un cadre communautaire pour les signatures électroniques (J.O.C.E. n° L 13, 19 janvier 2000, p. 12 et s.) ; pour un commentaire, v. E. A. Caprioli, *La loi française sur la preuve et la signature électronique dans la perspective européenne*, JCP 2000, éd. G, I 224.

[117] C'est à dire la loi du 13 mars 2000 et le projet de décret pris en application de l'article 1316-4, al. 2 du code civil qui dispose : « Lorsqu'elle (la signature) est électronique, elle consiste en l'usage d'un procédé fiable

d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat . » Pour le projet et les commentaires V. <http://www.internet.gouv.fr>

[18] Art. 1316 c. civ. : « 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. ».

[19] Pierre Catala et Pierre-Yves Gautier, *L'audace technologique de la Cour de cassation*, J.C.P. 1998, éd. E, p.884-885.

[20] A. Raynouard, *Adaptation du droit de la preuve aux technologies de l'information et à la signature électronique*, Defrénois 2000, p.595 ; J. Larrieu, *Identification et authentification*, in *Une société sans papier ?*, sous la direction de Mme Gallouédec -Genuys, La Documentation française, Paris, 1990, p.211 et s. ; S. Martin et A. Tessalonikos, *Informatique – La signature électronique*, Gazette du Palais 19 – 20 juillet 2000, p. 4 et s.

[21] Etienne Davio, *Preuve et certification sur Internet*, Rev. Droit Com. (Belge), 1997, p.666.

[22] Cass. com., 2 décembre 1997, cf. note n°11.

[23] La définition du signataire donnée à l'article 2 §3 de la directive est quant à elle la suivante : « »

[24] Définitions données in *Vocabulaire juridique*, sous la direction de G. Cornu, Association Henri Capitant, PUF, 1987.

[25] Article 2-2 de la directive du 13 décembre 1999.

[26] Eric A. Caprioli, *La loi française sur la preuve et la signature électroniques dans la perspective européenne – Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999*, JCP G, 2000, I, 224.

[27] Article 6 § 1 de la directive européenne du 13 décembre 1999, article 6 § 2 du projet de décret français.

[28] V. E. A. Caprioli, *Sécurité et confiance dans le commerce électronique - signature numérique et autorité de certification*, JCP 1998, éd. G., I, 223 ; *Preuve et signature dans le commerce électronique*, Droit et Patrimoine, n° 55, décembre 1997, p. 56 et s.

[29] V. la remarquable étude de M. Jacques Larrieu, *Les nouveaux moyens de preuve : pour ou contre l'identification des documents informatiques à des écrits sous seing privés ? (Contribution à l'étude des notions d'écriture et de signature)*, Lamy, Cah. dr. de l'informatique, nov. 1988, fasc. H, p.8 -19 (1ère partie) et déc. 1988, fasc. I, p.26-34 (2ème partie). V. également J.-M. Breton, *Intégrité de l'information*, in *Une société sans papier ?*, sous la direction de Mme Gallouédec -Genuys, La Documentation française, Paris, 1990, p.225 et s. ; Théo Hassler, *Preuve et documents stockés sur disque optique*, R.J.com. 1996, p.265 s.

[30] Le commentaire du projet de loi précisait d'ailleurs : « L'avènement de l'informatique remet en question la notion même de support, du moins de support matériel. Il n'en reste pas moins que la notion d'originalité d'un document reste primordiale. Cette originalité ne se ramène pas, comme par le passé, à une absence de modification du support, mais cette originalité découle de ce que l'intégrité d'une information puisse être établie

de son origine à nos jours. L'article 8 de la loi type de la CNUDCI sur le commerce électronique préconise cette approche (...). De la sorte on adopte une vue élargie de l'originalité (par opposition à une vision qui ramenait la question de l'originalité à la nature du support). Cette approche permet de rendre compte de ce que la technique informatique autorise la reproduction d'un document tout en assurant l'originalité de l'information contenue. Tel est le cas par exemple pour la technique de signature digitale qui permet de figer le document et d'assurer ainsi son intégrité.»

[31] Article 8 «Original» de la loi-type de la C.N.U.D.C.I. : « 1) Lorsque la loi exige qu'une information soit présentée ou conservée sous sa forme originale, un message de données satisfait à cette exigence : a) S'il existe une garantie fiable quant à l'intégrité de l'information à compter du moment où elle a été créée pour la première fois sous sa forme définitive en tant que message de données ou autre ; et b) Si, lorsqu'il est exigé qu'une information soit présentée, cette information peut être montrée à la personne à laquelle elle doit être présentée. (...) »

[32] Rappr. le terme original de l'expression qui figure à l'article 47 de la Loi de Finances rectificative pour 1990, n°90-1169 : "les factures transmises par voie télématique constituent, ..., des documents **tenant lieu** de factures d'origine" (J.O. du 30 décembre 1990, p.16469), v. Eric A. Caprioli , *La dématérialisation de la facture commerciale au regard de sa polyvalence juridique*, J.C.P. éd. E, 1993, Cah. de dr. de l'entr., n°1, p.34, ainsi qu'à l'article 4 de la loi n°94-126 du 11 février 1994 : " la réception d'un message transmis conformément aux dispositions du présent article **tient lieu** de la production d'une déclaration écrite ayant le même objet" (J.O. du 13 février 1994, p.2493 s.).

[33] Ce terme étant classiquement retenu pour les copies qui doivent être « fidèles » pour revêtir une force probante égale à celle reconnue aux originaux lorsque ces derniers n'existent plus. V. en ce sens : l'art. 1348 al. 2 c. civ. et à titre d'illustration, l'art. 13 de la loi du 14 août 2000 relative au commerce électronique, Mémorial, J. O. du Grand-Duché du Luxembourg, Recueil de législation A - n° 96, 8 septembre 2000, p. 2175 et s.

[34] En ce sens, v. C.R.I.D. (Mireille Antoine, Marc Eloy, Jean-François Brakeland), *Le droit de la preuve face aux nouvelles technologies de l'information*, Story scientia et C.R.I.D., Namur, 1992, p.35.

[35] Cass. 1<sup>ère</sup> Civ., 28 mars 2000, n° 654 P, Sté Lazard c/ Mme Thurin, Contrats, conc., consom 2000., comm. n° 107, note L. Leveneur. Sur le droit probatoire général, v. *Lamy Droit de l'informatique et des réseaux* éd. 2000, sous la direction de M. Vivant et de C. Le Stanc, n° 2826 et s. et sur la télécopie v. plus spécialement n° 2841.

[36] V. Cass. 1<sup>ère</sup> Civ., 6 octobre 1998, Contrats, conc., consom. 1999, comm. n° 5, note L. Leveneur.

[37] Aix-en-Provence, 27 janvier 1846, D.P. 1846, 2, 230 ; et plus récemment : Versailles, 12 octobre 1995, R.T.D.civ. 1996, p.172, obs. Jacques Mestre ; sur l'usage d'un crayon à papier lors de la rédaction d'un acte sous seing privé Cass. com., 8 octobre 1996, R.T.D.civ. 1997, p.137, obs. Jacques Mestre ; Dalloz Affaires 1996, p.1254.

[38] S'agissant de l'art. 1317 c. civ., actuellement un groupe de travail interdisciplinaire du GIP « *Droit et Justice* » auprès de la Chancellerie a été chargé « *de rechercher les conditions d'un nouveau formalisme électronique venant se substituer aux actuelles exigences liées au support papier* » en vue de l'élaboration de ce décret.

[39] Sur la conservation, v. Xavier Linant de Bellefonds, *Les résistances des droits comptables et fiscaux européens au développement des échanges de données informatisées*, R.I.D.C. 1995, 1, p.77 s. ; E. A. Caprioli, *Variations sur le thème du droit de l'archivage dans le commerce électronique*, Les Petites Affiches, 1<sup>ère</sup> partie, n° 164, 18 août 1999, p. 4 s., 2<sup>ème</sup> partie, n° 165, 19 août 1999, p.7 s. ; Ordre des Experts Comptables, *L'archivage électronique*, Paris, 1998.

[40] V. sur le site [www.industrie.gouv.fr](http://www.industrie.gouv.fr), la note du Secrétariat d'État à l'industrie qui mentionne des questions se trouvant à la fin de la présentation du projet : l'horodatage et la re-signature comme étant des conditions de sécurité susceptibles d'être introduites dans le décret sur les signatures électroniques. A notre avis, ces deux questions n'ayant pas encore fait l'objet d'une réflexion suffisamment poussée, il serait opportun de différer tout aspect réglementaire sur ces sujets.