

## COMMERCE ELECTRONIQUE

Citation : Eric A. CAPRIOLI & Anne CANTERO, Aspects légaux et réglementaires de la signature électronique, www.caprioli-avocats.com

### Aspects légaux et réglementaires de la signature électronique

Par Eric A. Caprioli et Anne Cantéro  
contact@caprioli-avocats.com

---

#### Plan

##### Introduction

##### I / DE L'ECRIT ET DE LA PREUVE ELECTRONIQUE

##### II / DE LA SIGNATURE ELECTRONIQUE A LA SIGNATURE ELECTRONIQUE SECURISEE

---

#### Introduction

L'écrit sur support papier sur lequel est apposée une signature manuscrite a été gravé dans le marbre du code civil en 1804. Il a fallu, cependant, attendre près de deux siècles pour que le législateur abroge ce quasi monopole de fait, né de la prééminence de l'écrit (papier) dans le domaine de la preuve ; en effet, l'article 1333 du code civil (" *des tailles* ") faisait déjà référence à d'autres modes de preuve : aux entailles faites sur des morceaux de bois lors des foires et des marchés d'autrefois.

L'entrée de la France dans la société de l'information est prise en compte dans le cadre du Programme d'Action Gouvernemental pour l'entrée de la France dans la Société de l'Information (PAGSI). Les ambitions de cette action sont à la mesure des enjeux économiques, sociaux, politiques et juridiques. Au niveau international, les Nations Unies (CNUDCI) adoptaient en 1996 une loi-type qui reconnaissait notamment la valeur juridique d'un écrit et d'une signature sous forme électronique. Une nouvelle loi-type sur les signatures électroniques a été adoptée en juillet 2001 [1]. Outre les textes législatifs et réglementaires applicables de ces dernières années (sur la preuve et sur la signature électronique la loi du 13 mars 2000 [2] et le décret du 30 mars 2001 [3], et les dispositions relatives à la cryptologie dans la loi relative à la sécurité quotidienne du 15 novembre 2001 [4]), deux projets de lois devraient bientôt être discutés au Parlement : la Loi pour la confiance dans l'économie numérique (LEN)[5] et la Loi sur la protection des personnes physiques à l'égard des traitements de données à caractère personnel[6]. Ces textes résultent de transpositions de directives européennes : directive sur les données à caractère personnel du 24 octobre 1995, directive 1999/93/CE du 13 décembre 1999 pour un cadre commun sur les signatures électroniques [7] et directive du 8 juin 2000, " commerce électronique ". En outre, la prise en considération des relations entre les administrations, les collectivités locales et les citoyens constitue un point fort de l'action gouvernementale. En effet, confiance et sécurité sont les maîtres mots de tous les échanges en ligne et de leur conservation.

Nous préciserons dans un premier temps les notions d'écrit et de preuve électronique (I), puis nous nous pencherons, dans un second temps, sur les conditions d'admissibilité et de validité des signatures électroniques telles qu'elles découlent des nouveaux textes en vigueur (II).

##### I / DE L'ECRIT A LA PREUVE ELECTRONIQUE

Par la définition donnée (art. 1316 code civil), la loi du 13 mars 2000 étend la notion de preuve littérale ou par écrit à tous les écrits (lettres, caractères, chiffres, signes, symboles) qu'ils soient papier, électronique ou autres et elle énonce que la preuve littérale ne dépend ni du support ni des modalités de transmission. Cette définition légale de l'écrit respecte ainsi le principe de neutralité technologique et médiatique. La nature de l'écrit ne dépend donc pas de ses modalités de transmission. L'écrit pour valoir preuve doit être intelligible.

La loi reconnaît désormais la validité des conventions sur la preuve comme le faisait déjà la jurisprudence fondée sur le caractère non impératif des règles sur la preuve [8]. La rédaction de ces conventions ne peut pas se faire n'importe comment, elle doit s'opérer en fonction du contexte dans lequel elles s'inscrivent pour pouvoir être considérées comme valables en cas de contentieux.

Par la situation des articles introduits par la loi dans le code civil, tous les écrits sont a priori visés par la réforme. De plus, l'article 1316-3 c. civ. prescrit : "*l'écrit sur support électronique a la même force probante que l'écrit sur support papier.*" Mais dans le même temps, cet article sous-entend que les conditions requises

pour certains écrits "papier" sont également requises des écrits électroniques pour leur conférer la même force probante. Qui plus est, il faut distinguer l'exigence d'un écrit *ad probationem et ad validitatem* [9]. Ainsi, les seconds doivent honorer certaines formalités pour être valables, c'est à dire pour exister en droit. Certains contrats doivent encore être rédigés par écrit papier et de façon manuscrite tant que la directive commerce électronique n'aura pas été transposée sur ce point (ex: cautionnement, contrat de travail à durée déterminée,...). Par suite, il faudra veiller à la faisabilité de la dématérialisation des conditions exigées pour les actes où l'écrit est exigé *ad validitatem*. Tel était le cas par exemple des formalités du double exemplaire qui dans l'univers électronique ne sont pas *ipso facto* transposables. La loi a d'ores et déjà modifié l'art. 1326 c. civ. en remplaçant les termes relatifs aux mentions " *de sa main*" par les termes " *par lui-même*".

En outre, la loi française a complété l'article 1317 c. civ. de telle sorte qu'elle pose le principe de la possible " dématérialisation " des actes authentiques (actes notariés, actes de l'état civil et jugements), y compris donc certains actes des collectivités locales. Un décret d'application est attendu. 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 vertu de l'article 1316-1 c. civ. " *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.* " En conséquence, ce qui compte, c'est la certitude que l'écrit émane bien de celui auquel il pourrait être opposé et que ni son origine, ni son contenu n'ont été modifiés ou falsifiés. Si pour l'établissement de l'acte, le texte ne renvoie pas à un décret en Conseil d'Etat pour apprécier les modalités de respect de ces conditions, il convient de se reporter au nouvel article 1316-4 c. civ. relatif à la signature électronique. D'un autre côté, l'archivage électronique doit garantir la conservation des " traces " probantes intègres selon des procédures de sécurité élaborées sur la base de la norme de l'AFNOR NF Z 42-013 relative à l'archivage électronique.

## II/ DE LA SIGNATURE ELECTRONIQUE A LA SIGNATURE ELECTRONIQUE SECURISEE

L'art. 1316-4 al. 1 c. civ. donne une définition fonctionnelle de la signature en général. La signature électronique (ou manuscrite) remplit deux fonctions juridiques de base : l'identification de l'auteur de l'acte et l'expression du consentement du signataire au contenu de l'acte. La définition des signatures électroniques et surtout les conditions légales posées pour cette catégorie de signature sont données à l'article 1316-4, al. 2 c. civ. qui dispose : " *Lorsqu'elle est électronique, elle (la signature) 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.* " Le procédé de signature électronique doit donc identifier le signataire, garantir le lien entre l'acte et la personne dont il émane et assurer l'intégrité de l'écrit signé. A l'heure actuelle, seules les signatures électroniques basées sur la cryptologie à clé publique (à savoir les signatures numériques) répondent aux exigences légales et plus particulièrement à la garantie de la solidité du lien entre la signature et le message. En effet, ce procédé assure l'intégrité du message signé grâce à la fonction " *hash*" ou " *contrôle*" qui consiste à faire à l'aide d'un logiciel intégré dans le dispositif de signature un abrégé du message (" *condensé*") que l'on chiffre à l'aide de la clé privée de signature (connue du seul signataire) et qui est logiquement lié au message électronique e. L'identification du signataire s'effectue par le biais d'un certificat électronique d'identification, émis par un tiers mais ce dernier doit, à notre avis, être indépendant des parties en cause dans la transaction. D'où l'on en déduit la notion de tiers qui participe à la confiance. La demande de certificat, l'enregistrement du titulaire et sa délivrance permettent son identification. La vérification de l'identité en face-à-face (rencontre physique contre, notamment, la présentation d'une pièce d'identité) est une condition essentielle pour assurer la sécurité qui va découler ultérieurement des actes signés.

C'est le Prestataire de Services de Certification électronique (P.S.C.E.) ou " *autorité de certification*" qui délivre un certificat électronique établissant le lien entre le signataire et un bi-clé de signature. Ce certificat servira au destinataire à vérifier que c'est la personne qui dit avoir signé qui sera réputée avoir signé le document électronique et que le message (acte) est intègre (non modifié depuis le moment de sa signature). Ces fonctions juridiques sont permises par les clés de cryptographie asymétriques (bi-clés). Les techniques de cryptographie peuvent également être utilisées à des fins de confidentialité des échanges, de sorte que le message soit inintelligible à toute personne non autorisée. Cela permet de préserver les secrets d'entreprise ou les données confidentielles ou sensibles (voire les informations classifiées dans le domaine de la défense). Mais pour ce faire, il est fortement recommandé d'utiliser des bi-clés différents de celui que l'on utilise à des fins de signature des messages.

Le décret d'application n° 2001-272 du 30 mars 2001 de la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information vient préciser les contours de la " *Signature électronique sécurisée* " qui bénéficie de la présomption légale de fiabilité. Cette disposition établit un renversement de la charge de la preuve au bénéfice de celui qui utilise une telle signature ; celui qui conteste la preuve de l'acte électronique en cause conserve néanmoins la possibilité de prouver que le procédé de signature n'était pas fiable [10].

On peut, toutefois, distinguer les signatures électroniques que nous qualifierons de "simples" dont l'utilisateur

doit démontrer qu'elles sont fiables et les **signatures électroniques sécurisées** pour lesquelles la loi pose une présomption de fiabilité du procédé dès lors qu'elles répondent aux exigences juridiques et techniques découlant du décret d'application du 30 mars 2001. Pour bénéficier de la présomption de fiabilité, le décret fixe un niveau de sécurité relativement élevé avec des exigences techniques et juridiques. A ce titre, on observera que la clé de signature doit être gardée sous le contrôle exclusif du signataire, ce qui exclut sa garde par un tiers qui au surplus n'a pas le droit de conserver une copie de ladite clé s'il l'a émise au profit de l'un de ses clients conformément à l'article 6-II, e) du décret.

D'une part, la mise en œuvre d'une signature électronique sécurisée devra être établie au moyen d'un dispositif sécurisé de création de signature dont la certification s'effectuera sur la base de normes européennes à paraître. D'autre part, la vérification de cette signature devra reposer sur l'utilisation d'un certificat électronique qualifié [11]. Le certificat est un document sous forme électronique qui atteste du lien entre une personne et un bi-clé de signature (clés asymétriques) : l'une privée qui sert à signer, l'autre publique qui sert à vérifier l'identité du signataire ; les deux étant indissociables.

A ce jour, sur le plan juridique, les signatures électroniques sont d'ores et déjà parfaitement valables depuis la loi du 13 mars 2000. Encore faut-il, devant le juge, rapporter la preuve de leur fiabilité technique et de leur lien avec l'acte qu'elles sont censées signer comme vient de nous le rappeler la Cour d'appel de Besançon dans une décision du 20 octobre 2000 (refus d'admettre la validité d'une signature scannérisée)[12].

Finalement, l'utilisation des technologies de l'information et de la communication va jouer un rôle majeur quant aux échanges des entreprises, des particuliers et des administrations. Néanmoins, il conviendra d'avoir recours à des moyens sécurisés et à des tiers prestataires de services afin de remplir le besoin de confiance du marché.

## Notes

[1] Voir nos commentaires publiés dans la revue Communication Commerce Electronique, décembre 2001.

[2] Loi n° 2000-230 du 13 mars 2000, JO n° 62 du 14 mars 2000, p. 3968.

[3] Décret n° 2001-272 du 30 mars 2001, J.O. n° 77 du 31 mars 2001, p. 5070, ainsi que le décret n° 2002-535 du 18 avril 2002 et l'arrêté du 31 mai 2002. V. à cet égard, l'article ci-joint sur les PSCE. De plus, le décret n° 2002-1436 du 3 décembre 2002 sur les questions de l'adaptation du droit de la preuve aux technologies de l'information (art. 9 du décret introduisant dans le nouveau code de procédure civile l'article 288-1), JO du 12 décembre 2002, p. 20482 s.

[4] Loi n° 2001-1062 du 15 novembre 2001, JO n° 266 du 16 novembre 2001, p. 18215.

[5] Projet de loi disponible sur le site de l'Assemblée nationale (<http://www.assemblee-nationale.fr>)

[6] Le projet de loi a été déposé à l'Assemblée Nationale le 18 juillet 2001, v. <http://www.assemblee-nationale.fr/projets/p13250.asp>

[7] JOCE n° L 13, 19 janvier 2000, p.12 s.

[8] Par exemple, Cass. civ. 16 novembre 1977 et Cass. civ. 8 novembre 1989.

[9] V. les dispositions de l'article 14 du projet de loi pour la confiance dans l'économie numérique qui introduira dans le code civil les articles 1108-1 et 1108-2 relative à l'écrit ad validitatem.

[10] V. les dispositions de l'article 9 du décret du 3 décembre 2002 introduisant dans le nouveau code de procédure civile l'article 288-1 précisant que " lorsque la signature électronique bénéficie d'une présomption de fiabilité, il appartient au juge de dire si les éléments dont il dispose justifient le renversement de cette présomption. "

[11] V. à cet égard, l'article ci-joint sur les P.S.C.E.

[12] V. E. A. Caprioli et P. Agosti, La signature manuscrite scannérisée sur la déclaration d'appel par le conseil d'une des parties rend cet appel irrecevable, JCP G, 2001, n° 41, p. 1890 s .