SIGNATURE ET CONFIANCE DANS LES COMMUNICATIONS ÉLECTRONIQUES EN DROITS FRANÇAIS ET EUROPÉEN

par Éric A. CAPRIOLI
Docteur en droit, expert aux Nations unies,
avocat à la cour de Paris, spécialiste en droit de la propriété intellectuelle

Depuis l'adoption de la loi pour la confiance dans l'économie numérique (LCEN) en juin 2004 [1], on peut considérer que la confiance constitue l'un des piliers fondateurs à la fois de la banalisation et de l'essor des échanges numériques dans tous les domaines de la vie en société [2]. Les relations peuvent être locales ou internationales, porter sur des biens corporels ou incorporels, relever du droit privé ou du droit public [3]. On est en présence d'une mutation

1. L. nº 2004-575, 21 juin 2004, pour la confiance dans l'économie numérique (*JO* 22 juin, p. 11168 s.). É. A. Caprioli et P. Agosti, « La confiance dans l'économie numérique », *LPA* 3 juin 2005, p. 4 s.

2. Le ministre français de l'Économie et des Finances l'avait d'ailleurs souligné en précisant que « le commerce électronique ne pourra se développer massivement si les consommateurs n'ont pas une entière confiance dans les procédures électroniques associées. » La loi pour la confiance dans l'économie numérique concrétise cette réflexion. V. également sur le manque de confiance des consommateurs, C. Huard, « Le consommateur et l'électronique », *Rev. conc. consom.* 2001. 123. 22. Ou encore dans un autre domaine Ch. Caron, « Le consommateur en droit d'auteur », in *Liber amicorum J. Calais-Auloy*, Paris, Dalloz, 2003, p. 245 s.

3. V. sur ce sujet : A. Cantero, *Des actes unilatéraux des communes dans le contexte électronique. Vers la dématérialisation des actes administratifs*, PUAM, coll. « Collectivités locales », 2002. Les lois françaises nº 2003-591, 2 juill. 2003, habilitant le gouvernement à simplifier le droit

sociétale, de laquelle est né ce que l'on peut appeler le « marché électronique » [4] ou numérique. La régulation de ce nouveau marché par les pouvoirs publics était nécessaire pour rassurer ses acteurs : consommateurs/citoyens, entreprises, administrations, collectivités locales et établissements publics. D'ailleurs, on ne compte plus les lois nationales ou fédérales et les règles régionales ou internationales qui ont été adoptées depuis une dizaine d'années [5].

Le mot « confiance » vient du latin *confidentia*. Si l'on en cherche la définition juridique, on trouve plusieurs significations dans le *Vocabulaire juridique* de Gérard Cornu [6] :

- croyance en la bonne foi, loyauté, sincérité et fidélité d'autrui (un tiers, un cocontractant) ou en ses capacités, compétences et qualifications professionnelles (ex. : la confiance en un professionnel du droit ou de la médecine) ;

- action de se fier à autrui, ou plus précisément de lui confier une mission (mandat, dépôt,...). À l'opposé, le droit sanctionne son abus (l'abus de confiance par le Code pénal ou les abus de domination par le droit de la concurrence) ou la perte de confiance en droit du travail ;

- manifestation de cette confiance, déclaration d'approbation (engagement de la responsabilité du gouvernement devant l'Assemblée nationale, art. 49 Const.).

Dans le monde numérique, la confiance se construit principalement autour de la notion de sécurité, qu'elle soit juridique, technique ou organisationnelle [7]. Pour que le commerce électronique se développe, la sécurité prêtée aux écrits sous forme papier doit être transposée dans un environnement électronique : les écrits établis sous forme électronique devaient disposer de la même force probante et de la même valeur juridique. Or, la prééminence de l'écrit papier qui caractérisait la plupart des systèmes probatoires européens, dont le système français, constituait un obstacle majeur à l'admission de la

(*JO* 3 juill., p. 1192) et n° 2004-1343, 9 déc. 2004, de simplification du droit (*JO* 10 déc., p. 20857) et les ordonnances prises en application de ces textes s'inscrivent dans le droit fil de la reconnaissance juridique des relations électroniques entre administrations et usagers et entre administrations elles-mêmes. Ord. 8 déc. 2005, *JO* 9 déc., p. 18896 et s. ; É. A. Caprioli, commentaire de l'ordonnance, *JCP* Adm. 2006. 1079. 432.

4. V. en ce sens, le remarquable travail de O. Cachard, *La régulation internationale du marché électronique*, préf. P. Fouchard, Paris, LGDJ, coll. « Bibliothèque de droit privé », Tome 365, 2002.

5. É. A. Caprioli, « Aperçus sur le droit du commerce électronique (international) », in *Souveraineté étatique et marchés internationaux à la fin du XXe siècle. Mélanges en l'honneur de Ph. Kahn*, Litec, 2000, p. 247 s. Égal. É. A. Caprioli, *Droit international de l'économie numérique*, Litec, 2007.

6. G. Cornu (dir.), *Vocabulaire juridique*, Paris, PUF, 1987, V° « Confiance ».

7. V. not. Ph. le Tourneau, « La notion de contrat électronique », *in* É. A. Caprioli (dir.), *Les deuxièmes journées internationales du commerce électronique*, préf. J. Huet, Paris, Litec, coll. « Actualités de droit de l'entreprise », 2005, t. 22, p. 1 s., not. p. 7.

force probante et de la validité des écrits électroniques ainsi qu'un frein à la confiance attendue par les acteurs de la société de l'information. La confiance est devenue le maître mot dans différents domaines législatifs [8].

S'agissant des communications électroniques, l'article L. 32-1° du Code des postes et des communications électroniques les définit comme étant « les émissions, transmissions ou réceptions de signes, signaux, d'écrits, d'images ou de sons, par voie électromagnétique ». Cette définition des communications électroniques est très large, un peu à l'image de la définition de la preuve littérale ou par écrit figurant à l'article 1316 du Code civil [9], mais elle s'inscrit dans le cadre des échanges et non dans celui de la constatation des actes juridiques ou des contrats.

L'initiative de la reconnaissance des écrits électroniques a été prise au niveau international par la Commission des Nations unies pour le droit du commerce international (CNUDCI) qui adoptait en 1996 une loi-type sur le commerce électronique [10] puis, pour préciser le régime juridique des signatures électroniques, une autre loi-type en juillet 2001 [11]. Reprenant les développements de la CNUDCI, le Parlement et le Conseil européens ont adopté une directive pour un cadre commun sur les signatures électroniques [12] réglementant l'usage des signatures électroniques tout en consacrant leur reconnaissance juridique. En France, le cadre juridique de la preuve et la signature électroniques a été posé par la loi du 13 mars 2000 [13] complétée par les décrets n° 2001-272 du 30 mars 2001 [14] et n° 2002-535 du 18 avril 2002 [15] ainsi que l'arrêté du 31 mai 2002 [16]. Ce dernier arrêté a d'ailleurs été abrogé par un arrêté du 26 juillet 2004 [17] relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation. Si ce dernier arrêté

8. V. en ce sens, L. n° 2005-67, 28 janv. 2005, tendant à conforter la confiance et la protection du consommateur, *JO* 1er févr., p. 1648 s. ou L. n° 2005-842, 26 juill. 2005, pour la confiance et la modernisation de l'économie, *JO* 27 juill., p. 12160 s.

9. « 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 ».

10. V., É. A. Caprioli et R. Sorieul, « Commerce international électronique : vers l'émergence de règles juridiques transnationales », *JDI* 1997. 2. 323-393.

11. V., É. A. Caprioli, « La loi-type de la CNUDCI sur les signatures électroniques », *CCE* déc. 2001. 9-10.

12. Dir. 1999/93/CE, 13 déc. 1999, *JOCE* 19 janv. 2000, L. 13, p. 12 s.

13. V. not. É. A. Caprioli, « La loi française sur la preuve et la signature électroniques dans la perspective européenne », *JCP* 2000. I. 224 ; « Écrit et preuve électroniques dans la loi n° 2000-230 du 13 mars 2000 », *Cah. dr. entr.* 2000. 2, suppl. 30. 1-11.

14. *JO* 31 mars, p. 5070.

15. *JO* 19 avr., p. 6944. V. à cet égard, *Dr. et patr.* févr. 2003. 116, obs. É. A. Caprioli.

16. *JO* 8 juin, p. 10223.

17. *JO* 7 août, p. 14104.

semble plus en adéquation avec les attentes du marché de la certification, il reste que l'on a longtemps attendu sa mise en œuvre.

Tous ces dispositifs légaux qu'ils soient nationaux, communautaires ou internationaux font la part belle à la signature. En effet, en tant qu'instrument juridique, elle se retrouve dans les échanges juridiques sous des formes diverses (sceau, manuscrite, code PIN « *Personnal Identification Number* », biométrique, scannée [18], clé cryptographique,...). Toutefois, son importance s'est considérablement développée avec la reconnaissance des écrits sous forme électronique.

Lorsque l'on examine la question de la confiance dans les communications électroniques en droit, une première entame consisterait à l'associer à la sécurité technique en ce domaine [19]. Ainsi, on pourrait également se pencher sur les contours juridiques de ce que l'on appelle « les tiers de confiance » [20], aussi bien en partant de leur typologie par catégorie pour en tracer le régime juridique, qu'en se référant à l'incidence des services à valeur ajoutée qu'ils fournissent au marché de la confiance, si tant est que ces services puissent être définis précisément. Une personne à qui l'on se fie doit être fiable, sûre et pérenne. Or, ce sont justement les exigences juridiques et techniques pesant sur une catégorie particulière de tiers (les prestataires de services de certification électronique) et les responsabilités y associées que fixent en France les lois et règlements applicables aux écrits et aux signatures électroniques [21] et en Europe la directive 1999/93/CE du 13 décembre 1999 [22].

Pourtant la confiance ne se décrète pas car elle relève de la psychologie collective des utilisateurs des technologies et des réseaux numériques. Elle doit, en effet, s'entendre du *sentiment de sécurité* dans le marché numérique ou électronique. Les métiers de la confiance ont une incidence sur toutes les activités de l'économie numérique en terme de sécurité informatique en général, que ce soit au niveau de l'infrastructure (les réseaux, les sites et les

18. Besançon, 20 oct. 2000, *JCP* 2001. II. 10606, note É. A. Caprioli et P. Agosti ; confirmé par Civ. 2e, 30 avr. 2003, *Bull. civ.* II, n° 118.

19. É. A. Caprioli, « Sécurité et confiance dans le commerce électronique (signature numérique et autorité de certification) », *JCP* 1998. I. 123.

20. É. A. Caprioli, « Les tiers de confiance dans l'archivage électronique : une institution juridique en voie de formation », *in* E. Mackaay (dir.), *Les incertitudes du droit*, Montréal, éd. Thémis, 1999, p. 25 s.

21. P.-Y. Gautier et X. Linant de Bellefonds, « De l'écrit électronique et des signatures qui s'y attachent », *JCP* 2001. I. 236, 1113 s. ; É. A. Caprioli, « Écrit et preuve électroniques dans la loi n° 2000-230 du 13 mars 2000 », *préc.* ; P. Catala, « Le formalisme et les nouvelles technologies », *Defrénois* 2000. 37210 ; J. Huet, « Vers une consécration de la preuve et de la signature électroniques », *D.* 2000. Chron. 95 s. ; P. Leclercq, « Le Nouveau droit civil et commercial de la preuve et le rôle du juge », *CCE* 2000. chron. 9 ; Ph. le Tourneau, *Contrats informatiques et électroniques*, 3e éd., Dalloz, coll. « Dalloz Référence », 2004, p. 24 s.

22. É. A. Caprioli, « La directive européenne n° 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques », *Gaz. Pal.* 29-31 oct. 2000. 5 s.

serveurs) ou au niveau des échanges électroniques entre les sujets de droit. Les communications électroniques sont principalement concernées par certaines fonctionnalités comme la confidentialité (chiffrement/déchiffrement des messages), l'authentification et l'identification des auteurs des messages (signatures électroniques), la traçabilité ou la garantie d'intégrité des données transmises. Mais il ne faut pas arrêter la liste à ces fonctions; il faudrait y ajouter la datation électronique des envois et des réceptions et l'archivage électronique des messages de manière intègre en vue de leur restitution en tant que preuves ou pour leur validité juridique.

Ici, les règles de droit et les règles techniques s'enchevêtrent; les pré-requis techniques permettent l'application des règles de droit, le droit devant prendre en compte l'état de l'art technique du moment (la normalisation en matières de signature électronique et de dispositif sécurisé de création et/ou de vérification de signature électronique, par exemple...). Le système juridique a fixé un cadre réglementant les évaluations et le contrôle de la sécurité des systèmes d'information notamment pour ce qui concerne le schéma d'accréditation des prestataires de certification électronique (PSCE) émettant des certificats qualifiés.

Ainsi pour mettre en lumière la constitution des éléments juridiques contribuant à la confiance dans les échanges électroniques, et avant d'aborder les questions liées au schéma d'accréditation des PSCE (II) et au régime juridique applicable à ceux-ci (III), il conviendra de rappeler les principales règles juridiques régissant les signatures électroniques dans l'expression de leur diversité (I). Les développements s'appuieront uniquement sur la directive européenne et le droit français relatif aux signatures électroniques.

I. - Signatures, signatures électroniques et signature électronique avancée, qualifiée ou sécurisée

Le cadre juridique de la signature électronique est fondé sur une hiérarchie de fiabilité par rapport à des exigences techniques, juridiques et organisationnelles, qu'il s'agisse du cadre communautaire (A) comme du cadre national (B). Toutefois, d'un strict point de vue juridique, il appartiendra au juge de déterminer si telle ou telle signature électronique doit être considérée comme valable ou non, quelle que soit l'application en cause et si le procédé bénéficie ou non de la présomption de fiabilité (réfragable) tirée de l'article 1316-4 du Code civil (art. 287 et 288-1 NCPC) [23]. Ainsi, tous les types

23. J. Devèze, « *Perseverare diabolicum* : À propos de l'adaptation du droit de la preuve aux technologies de l'information par le décret nº 2002-1436 du 3 décembre 2002 », *CCE* 2003. chron. 8. 13.

de signatures peuvent être recevables en justice dès lors que leur fiabilité est démontrée devant les tribunaux (signature électronique simple) ou présumée du fait du respect de certaines exigences (signature électronique sécurisée). Aucun texte n'exige une signature électronique sécurisée ou un certificat qualifié pour les actes sous seing privé, contrairement aux actes authentiques électroniques prévus à l'article 1317 du Code civil [24].

A. - *Le cadre communautaire*

La directive communautaire doit assurer la libre circulation des produits et services de signature électronique et la liberté d'établissement des prestataires, d'une part, et attribuer un minimum d'effets juridiques aux signatures électroniques dans le marché intérieur, d'autre part. Il s'agit d'éviter que le fonctionnement du marché intérieur ne soit gravement entravé par des initiatives divergentes entre États, en créant de graves distorsions de concurrence ; d'encourager l'utilisation des signatures électroniques et de renforcer la confiance dans les nouvelles technologies. À cette fin, la directive poursuit deux objectifs majeurs. Le premier est de créer un cadre légal pour l'activité des prestataires de services de certification (PSC) [25]. Le second est la reconnaissance juridique des signatures électroniques comme le souligne l'article 5 de la directive.

1° Éléments de définitions

L'article 2-1 de la directive définit la « 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 ». L'approche retenue n'est ni juridique (équivalent fonctionnel), ni technique [26].

---

24. Sur la question, v., B. Reynis, « Cliquer c'est signer », *JCP* N 2000. 49. 1747 ; « Vers l'authenticité électronique », X[e] rencontres notariat université, *LPA* 2 avr. 2001, p. 65 ; « Signature électronique et acte authentique, le devoir d'inventer », *JCP* N 2001. 1494. V. Décr. n° 2005-972, 10 août 2005, modifiant Décr. n° 56-222, 29 févr. 1956, pris pour l'application de l'ord. 2 nov. 1945 relative au statut des huissiers de justice et le Décr. n° 2005-973, 10 août 2005, modifiant le Décr. n° 71-941, 26 nov. 1971, relatif aux actes établis par les notaires (*JO* 11 août, p. 13055 et s.).

25. En droit français, les PSC sont devenus les prestataires de services de certification électronique (PSCE) en raison de l'utilisation du terme certification dans le Code de la consommation pour les services et produits autres qu'alimentaires (L. n° 94-2, 3 janv. 1994).

26. Selon la norme ISO 7498-2 de 1998, par « signature numérique » on entend : « données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon ».

De plus, la méthode d'authentification, qui n'est mentionnée qu'à l'occasion du considérant nº 21, n'est pas précisée, ce qui peut prêter à confusion et être source d'interprétation non uniforme dans les États de l'Union. En effet, de telles méthodes d'authentification ont une couverture plus large que la signature des actes juridiques puisqu'elles ont pour but de vérifier l'identité d'une personne ou d'un objet quelconque. À notre avis, la signature a pour but d'assurer les deux fonctions juridiques figurant à l'article 7 de la loi-type de la CNUDCI (identification et consentement). À la vérité, il résulte de cette définition que la signature électronique couvre à la fois les actes juridiques ainsi que d'autres formes « d'authentification » qui existent dans les pratiques des échanges électroniques, à savoir, les certificats de serveurs *web* (on est sûr que le site Internet est le bon et permet d'endiguer certaines formes de « *phishing* »), d'appareils tels que les routeurs ou les certificats d'éditeurs (ex. : logiciels, produits multimédias). C'est avec ces nouveaux moyens d'authentification que les tiers peuvent vérifier l'identité de ces objets et connaître l'entité juridique à laquelle ils sont attachés à l'aide d'un certificat numérique émis par un PSC. Ces certificats doivent être distingués de la labellisation des sites *web* qui tend à se développer et qui contribue également à la confiance nécessaire au développement du commerce électronique [27]. Par ailleurs, il existe également des certificats d'attributs qui servent à attester d'un rôle ou d'une qualité et qui sont associés à une personne, telle que la capacité à exercer une profession ou la délégation de pouvoir au sein d'une organisation. Mais ces certificats ne sont jamais considérés comme des signatures *stricto sensu*, dans la mesure où ils sont inclus dans une signature numérique et protégés par cette dernière [28].

Mais à l'heure actuelle, le certificat d'attribut n'est plus considéré comme une solution pertinente. De nombreux projets ont pour objet la gestion et la fédération d'identités entendues comme le fait de permettre à une personne de recourir à un identifiant unique pour accéder à différents services (ex. Liberty Alliance).

---

27. M. Antoine, D. Gobert et A. Salaün, « Le développement du commerce électronique : les nouveaux métiers de la confiance », *in* É. Montero (dir.), *Droits des technologies de l'information, Regards prospectifs*, Bruxelles, Bruylant, 1999, spéc. p. 11-21. Ces auteurs estiment que « la labellisation est le résultat de la combinaison de la technologie et de l'audit. Elle poursuit essentiellement l'objectif de donner une meilleure visibilité à un site Web et aux pratiques que celui-ci applique dans les relations avec ses clients » (p. 11).

28. Selon D. Pinkas, « alors qu'un certificat de clé publique associe une clé publique à un identifiant d'utilisateur, un certificat associe un ou plusieurs rôles à un identifiant de certificat. [...] Le certificat d'attribut n'est pas nécessairement émis par la même autorité que celle qui a émis le certificat de clé publique », in *Comprendre la différence entre signature électronique et signature numérique*, Conférence *Trusting Electronic Trade'99*, 7-9 juin 1999, Marseille.

En l'état actuel, la signature ne peut émaner que d'une personne physique, voire morale dans certains pays européens, qui s'identifie et qui manifeste son approbation au contenu de l'acte. Un objet ou un système d'information ne peut pas être assimilé à une personne [29]. Ainsi, le signataire est la « personne qui détient un dispositif de création de signature et qui agit soit pour son compte soit pour celui d'une entité ou personne physique ou morale qu'elle représente » (art. 2-3 Dir.). L'intention de signer (*animus signandi*) s'exprime par l'acte volontaire d'activation de la clé privée de signature lorsque le signataire entre ses données d'activation confidentielles. Le stylo ou la plume (l'outil qui permet de laisser une « *trace* » ou une marque personnelle) est remplacé par un dispositif de création de signature utilisant des prestations de cryptologie à clé publique. Cette définition semble donc reconnaître la signature des personnes morales, à l'instar de ce qui est prévu au Royaume-Uni ou au Luxembourg. Impensable avec les signatures manuscrites où seule une personne physique pouvait instrumenter la personne morale, il nous semble que l'adoption d'une telle disposition en droit français s'inscrirait dans le prolongement d'un mouvement de fond dont les manifestations les plus visibles sont la responsabilité pénale des personnes morales [30] et les textes fiscaux applicables à la facture électronique qui consacrent cette possibilité nouvelle [31]. Dans ce prolongement, il convient de préciser que la manifestation du consentement programmé par une machine ou un agent électronique est parfaitement valable [32].

La directive poursuit l'objectif de neutralité technique, non sans quelques difficultés car les pratiques s'appuient pour l'essentiel sur les signatures numériques à clé publique. Si les signatures numériques constituent un sous-ensemble des signatures électroniques, elles incarnent celles dont la technique permet le plus fort niveau de sécurité. Aussi, il était impossible de ne pas faire

29. É. A. Caprioli, « Consentement et système d'information », *RRJ* 1999. 1075 s.

30. V. l'analyse de M. Antoine et D. Gobert, « La directive européenne sur la signature électronique. Vers la sécurisation des transactions sur l'Internet? », *JTDE* avr. 2000, n° 68, v. n° 9.

31. Dir. 2001/115/CE, 20 déc. 2001 (*JOCE* 17 janv. 2001, L. 15, p. 24 s.), modifiant la Dir. 77/388/CEE, 17 mai 1977, en matière d'harmonisation des législations des États membres relative aux taxes sur le chiffre d'affaires — système commun de taxe sur la valeur ajoutée : assiette uniforme, dite « sixième directive », *JOCE* 13 juin 1977, L. 145, p. 1 s. ; L. n° 2002-1576, 30 déc. 2002, *JO* 31 déc., n° 304, p. 22070 ; Décr. relatif aux obligations de facturation en matière de taxe sur la valeur ajoutée et modifiant l'annexe II au CGI et la deuxième partie du Livre des procédures fiscales, *JO* 9 juill., p. 11617 ; Décr. pris pour l'application de l'art. 17 de la loi de finances rectificative pour 2002 du 30 déc. 2002, *JO* 20 juill., p. 12272 ; art. 96-F, annexe III CGI ; instruction fiscale, 7 août 2003, sur la TVA précisant les obligations des assujettis concernant l'établissement des factures (*BOI* 7 août 2003, n° 136). V. également É. A. Caprioli, *Cadre juridique et fonctionnement de la facture électronique*, disponible sur le site www.caprioli-avocats.com.

32. É. A. Caprioli, « L'agent électronique et le contrat », *in* É. A. Caprioli (dir.), *Les deuxièmes journées internationales du commerce électronique*, *op. cit.*, p. 213 s.

état des utilisations de « certificat », de « certificat qualifié » (art. 2-9 et 2-10 Dir.) et des « prestataires de services de certification » (art. 2-11). Avec cette technologie, les clés étant asymétriques, l'une ne marche pas sans l'autre (clé privée et clé publique). Le certificat qui contient la clé publique peut être envoyé avec le message signé ou publié lorsqu'il est révoqué dans une base de données (annuaire) tenue par un PSC [33]. L'intervention de ce tiers est indispensable; il garantit le lien qui existe entre une personne identifiée dans le certificat numérique qu'il émet sous sa responsabilité et une paire de clé unique à la personne. Cette personne, l'abonné/client du prestataire, doit avoir préalablement été enregistrée. Cette clé publique permet au destinataire de vérifier que la signature émane bien de la personne qui s'est identifiée avec sa clé privée. De même, les définitions qui traitent des données afférentes à la création (art. 2-4) et à la vérification de signature (art. 2-7) mentionnent que ces données peuvent être des codes ou des clés cryptographiques. En réalité, ce sont les clés privée et publique qui sont implicitement visées par la directive.

2° Effets juridiques des signatures électroniques

Lorsque l'on utilise les réseaux numériques, tels l'Internet, les relations s'effectuent en milieu ouvert — c'est-à-dire sans contrat préalable entre les parties, sans convention sur la preuve — et peuvent donner lieu indifféremment à des contrats domestiques ou internationaux [34]. La directive n'apporte aucune définition déterminant ce qu'il faut entendre par la notion de « réseau fermé ».

Par ailleurs, à la lecture du considérant n° 16, on constate que l'autonomie des parties et la liberté contractuelle doivent être préservées. Ceci explique pourquoi les cocontractants peuvent consentir entre eux les termes et conditions d'acceptation des signatures électroniques, le niveau de sécurité qu'ils estiment adéquat, mais dans les limites fixées par le droit national et sans s'appuyer sur les signatures électroniques avancées visées par la directive. Sur ce point, la loi française a introduit dans le Code civil la validité des

---

33. Toutefois, dans un intranet ou un extranet, on peut envisager que l'administrateur de l'infrastructure à clé publique établisse et gère lui-même l'annuaire où seront publiés les certificats de signature numérique ainsi que les certificats de confidentialité des membres. Cette hypothèse se conçoit également pour les groupes de sociétés ou pour les réseaux intégrés tels qu'ils existent dans les échanges de données informatisés (EDI).

34. V. not. sur le contrat international, la célèbre affaire des *Messageries Maritimes*, Civ. 21 juin 1950, *in* B. Ancel et Y. Lequette, *Grands arrêts de la jurisprudence française de droit international privé*, 3e éd., Paris, Dalloz, 1998, n° 22, p. 171 s. ; J.-M. Jacquet, *Le contrat international*, 2e éd., Paris, Dalloz, coll. « Connaissance du droit », 1999.